

Documento di ePolicy I.C. CASTELDACCIA

VIA CARLO CATTANEO N. 80 - 90014 - CASTELDACCIA

Palermo (PA) - Sicilia

Data di approvazione: 30/06/2025 - 09:28

Cap 1 - Lo scopo della ePolicy

1.1 Scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

1. Scopo dell'ePolicy
2. Ruoli e responsabilità nell'implementazione dell'ePolicy
3. Integrazione dell'ePolicy con regolamenti e normativa generale esistenti
4. Condivisione e comunicazione dell'ePolicy all'intera comunità educante
5. I piani di Azione dell'ePolicy

Capitolo 2 - Sensibilizzazione e prevenzione

1. Sensibilizzazione e prevenzione
2. Il Curricolo Digitale
3. IL KIT DIDATTICO

Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola

1. Protezione dei dati personali e GDPR
2. Accesso ad Internet
3. Strumenti di comunicazione online (PUA)
4. Strumentazione personale (BYOD)

Capitolo 4 - Segnalazione e gestione dei casi

1. Cosa segnalare
2. Come segnalare: quali strumenti e a chi
3. Gli attori sul territorio per intervenire
4. Allegati con le procedure

1.1 Scopo dell'ePolicy

(Questo paragrafo illustra lo scopo e gli obiettivi di questo documento programmatico per la cittadinanza digitale)

L' E-Policy ha come obiettivo principale quello di promuovere le competenze digitali per un uso delle tecnologie digitali positivo, critico e consapevole, da parte degli studenti e delle studentesse guidati dagli adulti coinvolti nel processo didattico-educativo.

La competenza digitale è una competenza chiave del cittadino europeo come indicato dal Consiglio Europeo

(Raccomandazione del 2018) che permette ad ogni cittadino di esercitare i propri diritti all'interno degli ambienti digitali (ONU - [Commento Generale 25](#): I diritti dei minori negli ambienti digitali).

L'ePolicy è un documento programmatico che permette di lavorare su quattro obiettivi:

1. Il piano di azioni triennale per promuovere nell'intera comunità scolastica l'uso sicuro responsabile e positivo della rete;
2. le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
3. le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
4. le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

Gli strumenti informatici, infatti, oltre a fornire una enorme opportunità espongono gli utenti, in particolar modo i minori ed i soggetti con limitate competenze informatiche, ad alti rischi che sono tanto più elevati quanto più è alto il grado di inconsapevolezza dei modi legittimi di usare la rete stessa. E' proprio per aumentare il grado di consapevolezza dell'uso legittimo della rete e per far sì che internet possa solo avvantaggiare i giovani che il nostro Istituto ha deciso di partecipare al progetto "Generazioni Connesse" e di fornirsi di un documento di riferimento che si integrasse con il Regolamento interno di Istituto allo scopo di promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti. L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali.

Nello specifico costituisce il riferimento per tutta la comunità educante per quanto attiene:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on- line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

1.2 - ePolicy: ruoli e responsabilità nell'implementazione dell'ePolicy

- (In questo paragrafo vengono dettagliati ruoli e responsabilità nell'implementazione del documento all'interno dei contesti scolastici ivi inclusi rappresentanti genitori e studenti per secondaria II grado).

Affinché l'ePolicy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, s'impegni nell'attuazione e promozione di essa.

È opportuno che nel documento vengano definiti con chiarezza ruoli, compiti e responsabilità di ciascuna delle figure all'interno dell'Istituto.

In questo paragrafo dell'ePolicy è importante specificare le figure professionali che, a vario titolo, si occupano di gestione e programmazione delle attività formative, didattiche ed educative dell'Istituto e tutte quelle figure appartenenti alla comunità educante.

IL DIRIGENTE SCOLASTICO

Il ruolo del Dirigente Scolastico nel promuovere l'uso consentito delle tecnologie digitali e di internet include i seguenti compiti:

- promuovere la cultura della sicurezza online e garantirla a tutti i membri della comunità scolastica, in linea con il quadro normativo di riferimento, le indicazioni del MIM, delle sue agenzie e attraverso il documento di ePolicy;
- promuovere la cultura della sicurezza online – anche attraverso il documento di ePolicy - integrandola ed inserendola nelle misure di sicurezza più generali dell'intero Istituto;
- ha la responsabilità di fornire sistemi per un uso sicuro delle TIC, internet, i suoi strumenti ed ambienti e deve garantire alla popolazione scolastica la sicurezza di navigazione tramite internet utilizzando adeguati sistemi informatici e filtri;
- ha la responsabilità della gestione dei dati e della sicurezza delle informazioni e garantisce che l'Istituto segue le pratiche migliori possibili nella gestione dei dati stessi;
- deve tutelare la scuola e garantire agli utenti la sicurezza di navigazione utilizzando adeguati sistemi informatici e servizi di filtri Internet;
- ha il compito di garantire a tutto il personale una formazione adeguata sulla sicurezza online per essere tutelato nell'esercizio del proprio ruolo educativo e non;
- deve essere a conoscenza delle procedure da seguire in caso di un grave incidente di sicurezza online;
- deve garantire adeguate valutazioni di rischio nell'usare strumenti e TIC, effettuate in modo che comunque quanto programmato possa soddisfare le istanze educative e didattiche dichiarate nel PTOF di Istituto;
- deve garantire l'esistenza di un sistema che assicuri il monitoraggio e il controllo interno della sicurezza online in collaborazione con le figure di sistema;
- deve essere a conoscenza ed attuare le procedure necessarie in caso di grave incidente di sicurezza online.

L'ANIMATORE DIGITALE E IL TEAM PER L'INNOVAZIONE DIGITALE

L'animatore digitale e il Team per l'Innovazione digitale sono co-responsabili, con il referente ePolicy, dell'attuazione dei piani di azione in particolare in riferimento alla formazione dei docenti. Sono inoltre responsabili del controllo all'accesso da parte degli studenti delle Tic

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

Il referente cyberbullismo è co-responsabile, con il team ePolicy, dell'attuazione dei piani di azione e coordina le iniziative di prevenzione e contrasto del cyberbullismo.

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

In coerenza con le Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo del Ministero dell'Istruzione (D.M. n. 18 del 13/1/2021, agg. 2021 - nota prot. 482 del 18-02-2021), il Team ha le funzioni di coadiuvare il Dirigente Scolastico, coordinatore del Team nella scuola, nella definizione degli interventi di prevenzione e nella gestione dei casi di bullismo e cyberbullismo che si possono presentare. Promuove inoltre la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale e comunica ad alunni, famiglie e tutto il personale scolastico dell'esistenza del team, a cui poter fare riferimento per segnalazioni o richieste di informazioni sul tema.

Il Team ha il compito di:

- coadiuvare il Dirigente scolastico, coordinatore del Team, nella definizione degli interventi di prevenzione del bullismo (per questa funzione partecipano anche il presidente del Consiglio d'Istituto e i Rappresentanti degli studenti).
- Intervenire (come gruppo ristretto, composto da Dirigente e referente o referenti per il bullismo e il cyberbullismo, psicologo o pedagogo, se presente) nelle situazioni acute di bullismo.
- Promuovere la redazione e l'applicazione della ePolicy e monitorare le segnalazioni.

I/LE DOCENTI

I/le docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Possono, innanzitutto, integrare la propria disciplina con approfondimenti, promuovendo l'uso delle tecnologie digitali nella didattica. I docenti devono accompagnare e supportare gli/le studenti nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete. Inoltre, educano gli studenti alla prudenza, a non fornire dati ed informazioni personali, ad abbandonare un sito dai contenuti che possono turbare o spaventare e a non incontrare persone conosciute in Rete senza averne prima parlato con i genitori. Informano gli alunni sui rischi presenti in Rete, senza demonizzarla, ma sollecitandone un uso consapevole, in modo che Internet possa rimanere per bambini/e e ragazzi/e una fonte di divertimento e uno strumento di apprendimento.

I/le docenti osservano altresì regolarmente i comportamenti a rischio (sia dei potenziali bulli, sia delle potenziali vittime) e hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che veda coinvolti studenti e studentesse dandone tempestiva comunicazione al Dirigente Scolastico, al Referente per il Cyberbullismo e Bullismo e al Consiglio di Classe per definire strategie di intervento condivise.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Responsabile della protezione dei dati (RPD o DPO) conosce l'ePolicy di Istituto, fornisce la propria consulenza in merito agli obblighi derivanti dal GDPR e sorveglia sull'esatta osservanza della normativa in materia di tutela dei dati personali ed è

co-responsabile delle azioni di informazione e formazione nell'Istituto sulla protezione dei dati personali

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

Il personale ATA, all'interno dei singoli regolamenti d'Istituto, è coinvolto nelle pratiche di prevenzione - ivi incluso il processo di definizione e implementazione dell'ePolicy di Istituto - ed è tenuto alla segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.

GLI STUDENTI E LE STUDENTESSE

Gli studenti e le studentesse devono, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti. Con il supporto della scuola dovrebbero imparare a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le. Affinché questo accada devono partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

I rappresentanti degli/delle studenti sono informati del documento di ePolicy e invitati a costruire i piani di azione, a partire dal secondo anno della secondaria di II grado,

I GENITORI/ADULTI DI RIFERIMENTO

I Genitori, in continuità con l'Istituto scolastico, sono attori partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile degli strumenti personali (pc, smartphone, etc). Come parte della comunità educante sono tenuti a relazionarsi in modo costruttivo con i/le docenti sulle linee educative che riguardano le TIC e la Rete e - ivi incluso il documento di ePolicy - comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet.

È estremamente importante che accettino e condividano quanto scritto nell'ePolicy d'Istituto e nel patto di corresponsabilità in un'ottica di collaborazione reciproca. Si promuove il coinvolgimento dei rappresentanti di genitori/adulti di riferimento all'interno del percorso di definizione e implementazione dell'ePolicy.

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

Enti esterni pubblici e privati, il mondo dell'associazionismo dovranno conformarsi alla politica della scuola riguardo all'uso consapevole delle TIC e della rete per la realizzazione di iniziative nelle scuole, finalizzate a promuovere un uso positivo e consapevole delle Tecnologie Digitali da parte dei più giovani, e/o finalizzate a prevenire e contrastare situazioni di rischio online e valutare la rispondenza delle proposte di attività di sensibilizzazione/formazione alle esigenze di qualità contenute nel documento di ePolicy. Dovranno inoltre promuovere comportamenti sicuri durante le attività che si svolgono con gli/le studenti e verificare di aver implementato una serie di misure volte a garantire la tutela dei minori nel caso di insorgenza di problematiche e ad assicurarne la tempestiva individuazione e presa in carico.

La Funzione strumentale per le nuove tecnologie e i Responsabili delle tecnologie di ciascun plesso

Coadiuvare il DSGA nella redazione dell'inventario della dotazione tecnologia scolastica;

Coadiuvare il DS nelle comunicazioni con il MIUR inerenti il monitoraggio dei beni inventariati a servizio delle aule laboratoriali;

Si interfaccia con il DS e il DSGA per la gestione/manutenzione degli strumenti in dotazione alla didattica, individuando le soluzioni utili a garantire un uso adeguato da parte degli utenti della scuola;

Riportare al DS e al DSGA e alla figura di riferimento per il Pronto Soccorso Tecnico eventuali comunicazioni di danneggiamento/furto/malfunzionamento delle attrezzature;

Redigere la procedura di utilizzo degli strumenti in dotazione alle aule e vigila sulla mancata osservazione della stessa;

Eseguire interventi formativi per i docenti all'uso delle aule informatiche e della strumentazione esistente;

Comunicare ai docenti e agli studenti le procedure per il corretto utilizzo degli strumenti;

Referente Privacy

Supporta il DS e la segreteria nel diffondere e mettere in atto quanto previsto dalla normativa sulla privacy

Responsabile della gestione documentale per ciascuna Area Omogenea (AOO)

Redige il manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici nel rispetto della normativa in materia di trattamento dati personali ed in coerenza con quanto previsto dal manuale di conservazione:

Gesitisce in modo unico e coordinato i flussi documentali e gli archivi di tutte le unità organizzative responsabili;

Coordinatore della gestione documentale

opera d'intesa con il Responsabile del trattamento dei dati e con il responsabile protocollo informatico, della gestione dei flussi documentali e degli archivi

svolge i compiti definiti dal cap. 4 par.5 delle Linee Guida AgID avvalendosi del supporto di soggetti esterni appositamente nominati

Amministratore Firewall

Mettere in atto norme, procedure e regolamenti per il corretto uso delle tecnologie al servizio della didattica;

Gestione del firewall dell'IC Casteldaccia e dei permessi di accesso alla rete didattica e amministrativa

Amministratore registro elettronico

Gestire le funzioni del registro e supporta i docenti e i genitori nella compilazione dello stesso

Amministratore Google Workspace Istituto

Gestire le funzioni della Google Workspace di Istituto e supporta docenti e studenti nell'uso della piattaforma

Amministratore sito web di Istituto

Gestire il sito web curandone i contenuti a supporto dell'utenza scolastica in accordo con il DS, il DSGA

1.3 Integrazione ePolicy nei documenti scolastici

(Il paragrafo spiega in che modo integrare il documento nel Regolamento dell'Istituto Scolastico da aggiornare con specifici riferimenti all'E-policy, così come nel RAV e all'interno del Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto).

La trasversalità dell'ePolicy rende necessaria una sua integrazione nell'ambito dei documenti che disciplinano il funzionamento dell'Istituto Scolastico.

Il Regolamento dell'Istituto scolastico, che rappresenta il principale punto di riferimento normativo, dovrà essere aggiornato in modo tale da dare contezza dell'adozione dell'ePolicy, e richiamare le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione in ambiente scolastico.

Anche il **Patto di Corresponsabilità educativa** tra scuola e famiglia dovrà essere integrato con gli opportuni riferimenti all'ePolicy, puntualizzando, da un lato l'impegno dell'Istituto ad organizzare eventi formativi/informativi a beneficio dei genitori, e dall'altro l'impegno di questi ultimi a partecipare in maniera proattiva a tali eventi.

Il **Piano Triennale dell'Offerta Formativa**, per la sua funzione di carta d'identità culturale e progettuale delle istituzioni scolastiche, nel quale si esplicita la progettazione curricolare, extracurricolare, educativa e organizzativa che le singole scuole adottano nell'ambito della loro autonomia, deve contenere anche le progettualità relative ad azioni media educative legate al percorso di ePolicy.

Così come il PTOF è il risultato di una consapevole concertazione fra le componenti delle istituzioni scolastiche (Dirigente Scolastico, docenti, alunni, genitori) e fra queste e il territorio, il patto di corresponsabilità rappresenta l'assunzione di responsabilità da parte di tutti coloro che svolgono un ruolo attivo nella Comunità educante.

L'e-policy viene aggiornata periodicamente (minimo ogni 3 anni) e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento verranno apportate dal Referente del progetto Generazioni Connesse e dal Team di Supporto per il Bullismo e Cyberbullismo che operano al progetto. A tale scopo saranno raccolte e discusse le necessità da parte dei diversi utenti ed elaborate le modifiche al documento. Le modifiche una volta apportate vengono discusse con tutti i membri del personale docente riuniti in Collegio ed approvate. Il documento, come ogni regolamento, passa quindi alla valutazione del Consiglio di Istituto che lo approva e ne valida l'entrata in vigore.

Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

1. il curriculum sulle competenze digitali per la comunità educante (il DigComp2.2);
2. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative;
3. Come comunicare e condividere l'ePolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

1. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative;

L'efficacia dell'ePolicy è direttamente proporzionale a livello di conoscenza e diffusione all'interno della comunità scolastica ivi comprese le famiglie. Il documento rappresenta il canale interno privilegiato per informare, responsabilizzare e collaborare sui temi della rete e delle tecnologie a scuola con l'intera comunità scolastica.

In tal senso, il documento è accompagnato da versioni, allegate e sintetiche, all'interno delle quali sono individuati gli elementi principali del documento; una versione è diretta agli studenti ed una è diretta alle famiglie con un linguaggio e una presentazione dei contenuti adeguata, flessibile e chiara. La versione sintetica rivolta agli studenti è inserita all'interno delle attività didattiche dell'educazione alla cittadinanza mentre la versione per le famiglie è consegnata nel corso dei colloqui scuola-famiglia.

Il documento è altresì pubblicato sul sito della scuola ed inserito nel Patto di corresponsabilità.

2. Come comunicare e condividere l'ePolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

La presenza dell'ePolicy nell'Istituto scolastico è garanzia, per il territorio, della presenza di un presidio informato, sensibile e attento sulla rete e le tecnologie in relazione con i più giovani.

In questo senso l'Istituto può rappresentare per le Istituzioni del territorio, le aziende, e le realtà del Terzo Settore un luogo di confronto privilegiato e di sperimentazione per tutti coloro che intendono costruire progetti di cittadinanza digitale rivolte ai più giovani.

A tal fine l'adozione dell'ePolicy è comunicata all'USR di riferimento e al Municipio (servizi istruzione e servizi sociali) attraverso gli allegati sintetici progettati che indicano gli elementi del documento e le prospettive per la comunità.

1.5 - I Piani di Azione dell'ePolicy

I piani di azione rappresentano il **programma triennale** di obiettivi che la scuola intende realizzare per promuovere la

conoscenza delle regole e dei protocolli di intervento che sono stati adottati con il documento di ePolicy nella comunità scolastica.

Nei Piani di Azione sono riportati **gli impegni e le responsabilità** che la scuola si assume per promuovere sui temi dell'educazione civica digitale e dell'utilizzo sicuro e consapevole delle tecnologie e della rete:

- la rilevazione dei bisogni
- le iniziative informative e formative,
- la formazione di docenti, studenti e studentesse, e famiglie,
- il monitoraggio e la valutazione delle azioni (laddove possibile, anche all'interno del RAV);

I Piani di Azione si distinguono tra standard, comuni ad ogni scuola che ha adottato l'ePolicy, e autoprodotti ovvero definiti dalla scuola sulla base del proprio contesto territoriale e delle collaborazioni in essere con Istituzioni, associazioni e aziende.

1° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

- Realizzare un evento di presentazione dell'ePolicy ai docenti dell'Istituto;
- Realizzare un evento di diffusione dell'ePolicy in occasione degli Open Day e/o in occasione del SID dell'Istituto dedicato alle famiglie ed a studenti/esse;
- Diffondere l'ePolicy negli ambienti scolastici, a studenti e studentesse, docenti e famiglie attraverso le versioni friendly dell'ePolicy;

MODULO II

- Effettuare una rilevazione del fabbisogno formativo dei docenti sui temi dell'educazione civica digitale;
- Effettuare una rilevazione di interessi, bisogni e comportamenti delle famiglie sull'uso positivo del digitale;
- Avviare l'introduzione del kit didattico come metodo e risorsa di lavoro in alcune classi pilota;

MODULO III

- Integrare l'ePolicy (norme, regolamenti e procedure) nei documenti dell'Istituto;
- Aggiornare la Politica d'Uso Accettabile (PUA) della scuola ed il regolamento BYOD dell'Istituto;

MODULO IV

- Definizione, a partire da quanto definito nell'ePolicy, delle procedure di segnalazione anche con linguaggio child/youth friendly perché possano essere accessibili a studenti e studentesse;
- Realizzare una reportistica delle segnalazioni ricevute e dei relativi esiti.

2° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

- Realizzare una formazione rivolta ai docenti dell'Istituto, sulla base dei risultati della rilevazione svolta nel corso del primo anno, anche attraverso il supporto di esperti/associazioni esterne o avvalendosi del percorso disponibile sul sito di Generazioni Connesse. La formazione deve coprire almeno il 60% del corpo docente.

MODULO II

- L'Istituto utilizza il kit didattico come pratica metodologica e risorse a disposizione dei docenti per i percorsi di ECD attraverso la formazione specifica sviluppata per i docenti attraverso il sito di Generazioni Connesse;
- Effettuare una rilevazione di interessi, bisogni, comportamenti, abitudini di studenti e studentesse sui temi dell'educazione civica digitale;
- Realizzare una formazione rivolta agli studenti e alle studentesse attraverso il percorso previsto sulla piattaforma di Generazioni Connesse;
- Realizzare una formazione rivolta alle famiglie attraverso il percorso previsto sulla piattaforma di Generazioni Connesse

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

- [Kit Didattico](#)
- Area formazione (per docenti, famiglie, studenti/sse con ePolicy)
- Canale [Youtube](#) (webinar, video-stimolo, serie per target differenti)
- Canale [TikTok](#)
- Canale [Instagram](#)
- Canale [Facebook](#)

Un'ulteriore integrazione di tali risorse ed eventi con quanto messo in atto da altre Agenzie educative per la sensibilizzazione ad un uso responsabile delle tic e per il contrasto ai fenomeni di bullismo e cyberbullismo sarà resa disponibile sul sito curato dall'AD e dal team digitale disponibile sulla pagina del sito internet dell'Istituto (sites.google.com/istitutocomprensivocasteldaccia.net/didattica-innovativa/sicurezza-in-rete-cyberbullismo) e/o attraverso circolari.

Cap 2 - Sensibilizzazione e prevenzione

2.1 - Sensibilizzazione e prevenzione

(Il capitolo raccoglie indicazioni su azioni formative per studenti/esse, famiglie e docenti con obiettivi a breve e lungo termine e riferimenti normativi (es legge 92 2019 su ECD). I rischi online andranno in appendice come glossario, sul sito come approfondimenti, sul kit didattico come attività.

La quotidianità in rete di ciascuno dei componenti della comunità scolastica - docenti, studenti e famiglie - deve essere caratterizzata da una consapevolezza critica delle caratteristiche degli ambienti e dei servizi online affiancata alle competenze per vivere al meglio il mondo connesso.

In questa direzione l'ePolicy è un documento che sviluppa azioni e interventi con l'obiettivo di raggiungere l'intera comunità scolastica e promuovere, ciascuno secondo il proprio ruolo, una cittadinanza digitale composta dalla conoscenza dei diritti in rete, dei rischi e delle opportunità per una partecipazione attiva e responsabile nella rete.

Il rischio online si configura come la possibilità per il minore di:

- commettere azioni online che possano danneggiare se stessi o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e/o contenerli, ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. Ciò è possibile lavorando su aspetti di ampio raggio che possano permettere una riduzione dei fattori di rischio e di conseguenza una minore probabilità che i ragazzi si trovino in situazioni non piacevoli. È importante che abbiano gli strumenti idonei per riconoscere le possibili situazioni di rischio e segnalarle ad un adulto di riferimento.

Gli strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio si configurano come interventi di sensibilizzazione e prevenzione.

- Nel caso della sensibilizzazione si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.
- Nel caso della prevenzione si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.

In particolare il presente documento intende essere un riferimento non solo quindi per le azioni che contravvengono alle regole interne della scuola per un uso responsabile delle tic, ma soprattutto per quelle azioni che possono avere ripercussioni sul piano educativo e dello sviluppo della persona o che si possono configurare come reato ai sensi della normativa vigente: Cyberbullismo, Hate speech, Dipendenza da Internet e gioco online, Sexting, Adescamento online, Pedopornografia.

2.2 - Il Curricolo Digitale

Per realizzare questo obiettivo l'istituto utilizza le risorse messe a disposizione a livello nazionale e internazionale.

Il DigComp 2.2, framework europeo sulle competenze digitali, permette di costruire una cornice precisa in cui inquadrare i temi e le corrispondenti competenze da proporre nell'Istituto non solo per gli studenti.

Al suo interno vengono identificati alcuni temi sui quali è costruita una proposta specifica per le famiglie e gli studenti (formazione). Tale cornice trova poi sviluppo specifico, per gli studenti, nel curriculum di educazione alla Cittadinanza Digitale previsto dalla L. 92/2019. Il curriculum prende forma attorno all'ePolicy e le attività didattiche sono legate al documento ed alle scelte dell'Istituto al suo interno.

Nel curriculum va previsto in ogni classe un appuntamento didattico specifico, calibrato sull'età degli alunni, e l'utilizzo dei kit didattici per favorire da parte degli studenti una maggiore conoscenza e consapevolezza delle finalità del presente documento.

I regolamenti e le attività sviluppate sul tema della prevenzione presenti nell'ePolicy sono parte, costante ma non esclusiva, delle azioni di disseminazione e sensibilizzazione descritte ed attuate dall'Istituto.

Il presupposto dal quale si parte è la considerazione che i ragazzi usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali". Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla Cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico" (["Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente"](#), C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avviene attraverso l'attuazione e l'implementazione del curriculum digitale che è stato redatto e approvato dal Collegio dei docenti nel corso dell'a.s. 2020-21 e che viene riportato in allegato (<https://www.iccasteldaccia.edu.it/documento/piano-triennale-offerta-formativa-triennio-2022-2025/>). Alcuni aspetti formativi sono inoltre inerenti il curriculum di ed. civica, anch'esso condiviso e approvato dal collegio dei docenti nell'a.s. 2020-21. In particolare rientrano tra le competenze di ed. civica le competenze digitali che riguardano il comunicare e l'uso in sicurezza di strumenti digitali. Il curriculum viene periodicamente aggiornato anche alla luce di eventuali indicazioni messe a punto dal Ministero dell'Istruzione e del Merito.

2.3 - Il Kit Didattico

L'e-Policy prevede, a livello macro, un lavoro di lettura e d'intenti condivisi dall'intera comunità scolastica, a livello micro, invece, immagina che la singola classe lavori anche su tematiche direttamente collegate alla sicurezza in rete, ma complesse e di non immediata ricaduta nelle programmazioni scolastiche (etica e digitale, algoritmi, datafication). A tal fine si è progettato e predisposto del materiale che possa funzionare sia da attivatore, sia d'accompagnamento ai docenti e agli studenti nella fase più delicata ed incisiva del processo di prevenzione: la lezione in classe.

Pertanto, il progetto Generazioni Connesse, a supporto del lavoro dell'e-Policy ha previsto per i docenti e studenti di ogni segmento scolare un nuovo [Kit Didattico](#) che contiene materiali per le lezioni e per il proprio aggiornamento, a partire dalla scuola d'infanzia fino alla secondaria di secondo grado. Il Kit può essere usato nella sua interezza oppure può essere oggetto di selezione e scelta, sulla base di quanto fatto dal docente.

Sarà cura dei docenti del Consiglio di Classe progettare gli interventi necessari secondo quanto previsto dal curriculum di ed. civica e dal curriculum digitale o sulla base di esigenze educative emerse nel corso dell'a.s., individuando metodologie e strumenti adeguati al gruppo classe sul quale si interviene. Tali interventi rientreranno nel monte ore di ed. civica e/o all'interno delle proprie attività disciplinari quando previsto (ad. es. per i docenti di tecnologia o matematica).

Cap 3 - Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola

3.1 - Protezione dei dati personali e GDPR

La protezione dei dati personali delle persone fisiche costituisce un diritto fondamentale. L'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea e l'art. 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Le principali normative di riferimento sono il Regolamento Generale sulla Protezione dei Dati 2016/679 noto anche come GDPR, e il Dlgs 196/2003 conosciuto come Codice Privacy.

Il settore dell'istruzione è particolarmente impattato dalla tematica privacy in considerazione del fatto che gli Istituti Scolastici sono chiamati, necessariamente, a trattare un'enorme mole di dati personali.

Con l'entrata in vigore del GDPR è stato introdotto l'obbligo per ciascun Istituto scolastico di provvedere alla designazione di un Responsabile della protezione dei dati personali (RPD o DPO).

I principali obblighi in materia di protezione dei dati personali consistono nella definizione di un "organigramma privacy", nel rilascio dell'informativa al momento della raccolta dei dati e nella tenuta di un registro dei trattamenti.

"Le scuole sono chiamate ogni giorno ad affrontare la sfida più difficile, quella di educare le nuove generazioni non solo alla conoscenza di nozioni basilari e alla trasmissione del sapere, ma soprattutto al rispetto dei valori fondanti di una società. Nell'era di Internet e in presenza di nuove forme di comunicazione questo compito diventa ancora più cruciale. È importante riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino". (cfr. <http://www.garanteprivacy.it/scuola>).

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il "corretto trattamento dei dati personali" a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni.

In questo paragrafo dell'e-Policy affrontiamo tale problematica, con particolare riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori. A tal fine, l'Istituto allega alla presente e-Policy i modelli di autorizzazione al trattamento dei dati personali con la relativa informativa da utilizzare, conformemente alla normativa vigente, in materia di protezione dei dati personali insieme al modello organizzativo consultabile sul sito della scuola nell'area dedicata al regolamento (<https://www.iccasteldaccia.edu.it/documento/regolamento-distituto-2/>).

Si ribadisce che rientrano all'interno della norma tutti quei dati che contribuiscono ad identificare un soggetto e le sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc.:

- i dati che permettono l'identificazione diretta di una persona, come i dati anagrafici (ad es. nome e cognome);
- i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad es. il codice fiscale, l'indirizzo IP, il numero di targa);
- i dati rientranti in particolari categorie: si tratta dei dati cosiddetti sensibili, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale di una persona. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;
- i dati relativi a condanne penali e reati: si tratta dei dati cosiddetti giudiziari, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad es. i provvedimenti penali di condanna definitiva, la liberazione condizionale, il divieto o obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Personale ATA di Segreteria

Le anagrafiche degli studenti e i loro documenti sono trattati dal personale di segreteria incaricato che ne cura l'archiviazione secondo le norme di riferimento. I dati vengono gestiti dal sistema Argo che ne garantisce la tutela ai sensi della norma vigente.

Personale Docente

I docenti curano l'archiviazione della documentazione a supporto dell'attività didattica all'interno del Registro elettronico, coordinandosi con le figure di riferimento (DS, Resp. GOSP-GLH-GLI, segreteria scolastica). Ogni docente è responsabile della tutela dei dati personali degli studenti e pertanto avrà cura di conservare in modo adeguato documenti che possono contenere dati sensibili degli alunni (verbali, programmazioni, relazioni etc...). Riferimenti anagrafici o che comunque rientrano all'interno della norma sulla tutela della privacy possono essere inseriti solo all'interno di documenti il cui accesso è possibile esclusivamente al personale interno alla scuola (docenti/personale ATA di Segreteria). Sarà responsabilità del docente archiviare all'interno di Argo e depositare in Segreteria documenti di riferimento della classe che potrebbero contenere dati sensibili (programmazioni, verbali etc...). Nel caso in cui i documenti fossero archiviati su Argo la visualizzazione sarà esclusiva dei docenti della classe.

Per le categorie sopracitate il Dirigente Scolastico pubblica su Argo gli atti di "Autorizzazione e istruzioni al trattamento dei dati" (allegato). Tali documenti firmati per presa visione da ciascuno verranno conservati agli atti presso la Segreteria Scolastica:

- Allegato 2: Autorizzazione e istruzioni al trattamento dei dati - assistenti amministrativi;
- Allegato 3: Autorizzazione e istruzioni al trattamento dei dati - docenti;
- Allegato 4: Autorizzazione e istruzioni al trattamento dei dati collaboratori scolastici;
- Allegato 5: Autorizzazione e istruzioni al trattamento dei dati - AD e team digitale;

Famiglie

I dati degli studenti vengono gestiti dal personale scolastico e dai sistemi informativi della scuola (sistema Argo, piattaforme didattiche) garantendo la tutela ai sensi della norma vigente. I genitori prendono visione delle relative informative tramite Argo apponendo il flag presa visione e autorizzazione (Allegato6 - Informativa per il trattamento dati personali - alunni e loro famiglie).

Personale esterno

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio dell'interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa. Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza. Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network). A tale scopo si ricorda che è severamente vietato da parte di esterni scattare foto/video di minori durante le attività svolte a scuola (meeting, incontri formativi, eventi, iniziative di divulgazione/sensibilizzazione) senza avere preventivamente raccolto il consenso esplicito da parte dei tutori/genitori degli stessi per lo specifico intervento tenuto da personale esterno, anche se per motivi didattici. Il personale esterno che presta servizio a scuola su contratto specifico o gratuitamente devono firmare una informativa nella quale sono sintetizzate le regole della scuola e gli obblighi da parte degli stessi in relazione alla sicurezza e alla prevenzione di situazioni di rischio (Allegato 1 - Informativa privacy personale esterno e Dichiarazione presa visione e adesione). Per quanto attiene la gestione di documenti che potrebbero contenere dati sensibili personale esterno è tenuto a conservare in modo adeguato tali documenti consegnandoli al docente di riferimento dell'attività condotta che a sua volta ne curerà l'archiviazione secondo quanto previsto per i docenti.

3.2 - Strumenti di comunicazione online (PUA)

La Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) è un documento che racchiude una serie di regole legate all'utilizzo della rete a scuola e a casa da parte di studenti e di tutto il personale (compresi i professionisti esterni che lavorano in contesto scolastico), integrante il DPS (Documento programmatico sulla Sicurezza). Il documento, che funge da raccordo, si compone di punti strategici riguardanti non solo i vantaggi di internet a scuola ma anche i rischi connessi all'online, nella valutazione di quei contenuti presenti in rete e di quelle azioni negative che possono comprometterne l'uso positivo. Fra queste attività: ricercare materiale non consono allo stile educativo della scuola; produrre vere e proprie azioni illecite; giocare online con la rete scolastica; violare la privacy e i diritti d'autore, etc... Nella Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) vengono definite, dunque, le regole di utilizzo fra tutti gli attori in gioco, nel rispetto dei dati sensibili di ciascuno, in particolar modo degli alunni e delle alunne.

Di seguito vengono dettagliate le regole di utilizzo che la scuola si è data in riferimento all'uso della rete scolastica, degli strumenti digitali scolastici (tablet, pc, monitor, LIM etc...) incluse le piattaforme didattiche (Google Workspace for education

e sue estensioni, piattaforme per la didattica esterne a Google Workspaces).

3.2.1 - Accesso ad Internet

"L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale. Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale. Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete. L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.

Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale, tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità" (fonte: art. 2 Dichiarazione dei diritti di Internet, 27 ottobre 2014 - Commissione per i diritti e i doveri in Internet).

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola". Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola. Allo scopo di garantire in sicurezza il "diritto ad internet" la scuola mette in atto tutte le azioni necessarie per garantire agli studenti l'accesso ai motori di ricerca adottando tutti i sistemi di sicurezza conosciuti per diminuire le possibilità di rischio durante la navigazione.

Resta fermo che non è possibile garantire una navigazione totalmente priva di rischi e che la Scuola e gli insegnanti non possono assumersi le responsabilità conseguenti all'accesso accidentale e/o improprio a siti illeciti.

Accesso ad internet: filtri, antivirus e sulla navigazione

L'Istituto dispone di 5 plessi. La sede centrale della scuola secondaria dispone di un dominio su rete locale (rete segreteria) al quale accedono esclusivamente i computer dell'amministrazione.

La rete della Segreteria scolastica e quella della didattica sono protette da Firewall, le due reti sono separate ed accessibili ad uso esclusivo della segreteria la prima e dei docenti e degli studenti la seconda.

Rete segreteria e strumenti della segreteria

L'accesso alla rete della segreteria è consentito esclusivamente dalle postazioni fisse assegnate al personale e collegate attraverso sistema LAN in rete. Ogni postazione della segreteria è accessibile esclusivamente con user e password personali in modo da tutelare l'eventuale accesso ai dati personali. Tutte le postazioni della Segreteria al termine della giornata lavorativa vengono spente dai rispettivi utenti. L'accesso alla rete di ciascuna postazione è automatico e protetto da firewall. Tutti i pc della segreteria sono collegati al server della segreteria del quale il DSGA effettua periodicamente il backup dei dati.

Rete didattica

La rete è gestita da Firewall che ne garantisce la tutela dei dati e blocca l'accesso a siti non consentiti. Attraverso il firewall è possibile controllare gli accessi dei singoli utenti rilevando i tempi di navigazione e i siti utilizzati. L'aggiornamento dei siti da escludere alla navigazione viene gestito dalla ditta che ha in carico la manutenzione periodica del firewall.

L'accesso ai docenti è possibile previo inserimento di una user name e password di accesso alla rete scolastica. Tale password è comunicata ai docenti che avranno cura di custodirla garantendone la segretezza. La gestione degli accessi è effettuata dalla funzione delegata dal DS e dal DSGA che cura la profilazione degli utenti assegnando a ciascun docente le

proprie credenziali di accesso sul firewall e/o attraverso le credenziali di Google Workspace inserite sullo stesso sistema. Tali credenziali vengono periodicamente modificate direttamente dagli utenti. Il proprietario delle credenziali è l'unico responsabile delle operazioni svolte con esse. Il docente verificherà la disconnessione del dispositivo utilizzato in aula dalla rete al termine della sua ora di lezione.

Gli studenti potranno avere accesso alla rete internet attraverso credenziali che vengono assegnate su richiesta dalla funzione delegata, tali credenziali (voucher di accesso) hanno durata momentanea e scadono al termine della giornata di utilizzo. I docenti che per le proprie attività necessitano di voucher devono farne richiesta alla funzione strumentale che le fornirà. Attraverso il firewall è possibile controllare gli accessi dei singoli utenti rilevando i tempi di navigazione e i siti utilizzati. L'aggiornamento dei siti da escludere alla navigazione viene gestito dalla ditta che ha in carico la manutenzione periodica del firewall.

3.2.2 - Strumenti didattici - Gestione accessi (password, backup ecc)

Le disposizioni riguardanti la fruizione dei Laboratori e degli strumenti digitali, con il trattamento delle relative infrazioni, sono riportate in specifiche procedure contenute nel Regolamento di Istituto. Le istruzioni contenute nel Regolamento vanno sostituite e/o integrate con le norme contenute all'interno del Regolamento Covid che è stato approvato dal Consiglio di Istituto, valido a partire dall'a.s. 2020-21 fino ad ulteriori modifiche e/o integrazioni.

Gli strumenti sono protetti da antivirus che vengono aggiornati annualmente dal personale incaricato. Si raccomanda di limitare l'uso di dispositivi di archiviazione mobile per ridurre al massimo la possibilità di trasmissione di virus, malware.

Tutti gli strumenti della scuola sono dotati di pw e us con funzioni di amministratore utilizzata dalla funzione strumentale per le nuove tecnologie e dal personale incaricato a supporto per i diversi plessi. Grazie a tale account sarà possibile scaricare gli applicativi indispensabili per la didattica per i quali è necessario fare richiesta alla funzione strumentale.

Ogni aula ha in dotazione un proprio pc con doppio account amministratore/studente. I pc sono utilizzabili ricorrendo all'account "studente/alunno", è un account base con limiti nella gestione del pc. L'accesso ad internet del pc dell'aula è possibile solo attraverso credenziali del docente. Gli strumenti assegnati alle classi ad inizio anno non possono essere utilizzati in altre aule. I docenti che hanno accesso all'aula sono responsabili di un uso corretto degli strumenti che non devono essere mai lasciati incustoditi.

Gli strumenti delle aule laboratorio (notebook e tablet del laboratorio informatico, del lab. linguistico, del lab. multifunzione e delle aule laboratorio pnrr) vengono assegnati per la loro gestione a docenti incaricati e hanno l'accesso ad internet diretto. I docenti sono responsabili della sorveglianza degli studenti durante il loro utilizzo. Sarà cura del docente assicurarsi che nessun documento contenente dati sensibili sia condiviso e rimanga disponibile sullo strumento utilizzato.

L'utilizzo delle aule laboratorio ad eccezione di quelle pnrr è garantito attraverso un sistema di prenotazione gestito attraverso google calendar. I docenti devono prenotarsi entro la fine della settimana precedente inserendo il proprio nome, quello della classe e l'orario di fruizione dello stesso.

Tutti gli utenti che utilizzano gli strumenti delle aule laboratorio accedono con account denominato "studente/alunno" che impedisce di apportare alla macchina qualunque modifica alla configurazione. Ogni utente è responsabile della corretta archiviazione del materiale prodotto. Periodicamente la funzione incaricata effettua un controllo degli strumenti e l'aggiornamento dei file di sistema. Annualmente la funzione incaricata pulisce gli strumenti dai file prodotti nel corso dell'ultimo anno. La salvaguardia del materiale didattico elaborato da studenti e docenti è a carico del docente che lo ha prodotto. Qualunque segnalazione inerente il malfunzionamento o danni alla strumentazione deve essere effettuata per email indirizzata all'email della scuola all'attenzione della funzione incaricata e del DSGA.

3.2.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli

più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

E-mail

Gli studenti, profilati all'interno dell'area Google Workspace dell'IC Casteldaccia e formalmente autorizzati dai propri genitori, possono utilizzare i servizi mail accedendo ai relativi account generati dall'Amministratore di Google Workspace di Istituto e comunicati ai genitori.

3.2.4 - Piattaforme didattiche Google Workspace

A partire dall'anno scolastico 2020/21 il nostro Istituto ha attivato la G Suite for Education, oggi "Google Workspace for Education", un insieme di applicativi messi a disposizione da Google per le scuole, al fine di facilitare, sostenere e motivare l'apprendimento attraverso le nuove tecnologie. "Google Workspace for education" è costituita da un insieme di applicazioni. Le principali sono: la posta elettronica (Gmail), i documenti condivisi (Google Drive), il Calendario (Google Calendar), le classi virtuali (Google Classroom), la piattaforma per le videolezioni (Google Meet). Le funzionalità sono le stesse, praticamente identiche a quelle degli account Gmail di tipo privato (a parte Google Classroom), ma la grande differenza è nelle condizioni d'uso: per le Google Workspace for education la proprietà dei dati rimane in capo all'utente, con totale protezione della privacy e priva di pubblicità, mentre per gli account privati le possibilità di "intromissione" da parte di Google sono numerose.

In accordo con le linee guida del Piano Nazionale per Scuola Digitale, il nostro Istituto ha creato un dominio @istitutocomprensivocasteldaccia.net associato alla piattaforma Google Workspace for Education.

L'account Google Workspace for education è attivato per tutti i docenti e gli studenti dell'IC Casteldaccia i quali riceveranno un account personale gratuito con nome utente e password per l'accesso ai servizi di base di Google di cui potranno usufruire fino al termine del loro percorso scolastico nel nostro Istituto.

Tra gli applicativi di Google Workspace rientra anche Google Classroom, grazie al quale vengono create classi virtuali e gli studenti e i docenti possono comunicare in modo sicuro e protetto.

All'interno di Google drive sono state create cartelle - repository per lo scambio di materiali e documenti da parte dei docenti della scuola. La cura di tali materiali è assegnata al gruppo di docenti che ne ha accesso secondo la modalità di condivisione "editor/visualizzatore".

Per quanto attiene nello specifico l'utilizzo di Google Workspace for education l'Istituto ha redatto uno specifico regolamento al quale tutti gli utenti profilati dalla scuola devono fare riferimento e riportato in allegato alla E-policy: Allegato 7 - "Regolamento utilizzo piattaforma Google Workspace for Education per scopi didattico-formativi (eLearning) e per svolgimento di riunioni in modalità telematica".

I docenti prendono visione dell'Informativa sull'Uso di Google Workspace for Education e del relativo Regolamento d'uso, pubblicati sul sito della scuola all'interno dell'area dedicata.

Agli studenti verranno inviate sul registro Argo e/o pubblicate sul sito della scuola formativa all'uso di Google Workspace for Education, il relativo Regolamento d'uso al quale i genitori apporranno la spunta per presa visione e adesione. Viene comunicato l'elenco degli account con password, da cambiare dopo il primo accesso, tramite i docenti coordinatori delle classi.

Nel caso in cui l'Istituto decida di attivare i servizi aggiuntivi della Piattaforma Google Workspace for Education, i genitori dovranno prendere visione dell'informativa relativa al servizio pubblicata su argo questo procedimento consentirà all'Amministratore della piattaforma di attivare per lo studente il servizio. Sarà cura del docente verificare con l'amministratore della piattaforma che sia stata presa visione dell'informativa su argo da parte del genitore. Resta inteso che l'attivazione dell'account studente effettuata il primo anno non necessita di ulteriore autorizzazione negli anni

successivi.

Altre piattaforme didattiche

Nei casi in cui i docenti voglia ricorrere ad altre piattaforme per la didattica senza utilizzare email di conferma come ad esempio Scratch Code.org, sarà compito dei docenti procedere alla profilazione degli studenti con nickname avendo cura di tutelare la riservatezza di eventuali dati sensibili degli alunni (nome, cognome o altri riferimenti).

Per le altre Piattaforme didattiche, tools o siti che richiedono profilazione da parte degli utenti e che devono essere attivate attraverso la conferma via email, si procederà con una comunicazione ai genitori da parte del docente interessato e i genitori degli alunni ne autorizzeranno per presa visione le condizioni di uso. Sarà cura del docente richiedere temporaneamente l'apertura verso l'esterno al gestore della piattaforma in modo da consentirne l'immediata chiusura al termine delle operazioni di registrazione.

Resta inteso che l'attivazione dell'account studente effettuata il primo anno non necessita di ulteriori passaggi negli anni successivi. Al termine del ciclo scolastico gli account vengono chiusi ed archiviati nel sistema dal personale incaricato della gestione.

3.2.5 - Sito web della scuola

Il Dirigente Scolastico e il personale incaricato di gestire le pagine del sito della Scuola hanno la responsabilità di garantire che il contenuto pubblicato sia accurato e appropriato. La scuola offre all'interno del proprio sito una serie di servizi alle famiglie e ai fruitori esterni. I docenti che desiderano pubblicare materiali e/o presentazioni delle attività didattiche svolte con i propri alunni dovranno chiedere l'autorizzazione al Dirigente tramite e-mail. Tutti i servizi offerti tramite il sito web della scuola, nel rispetto delle norme vigenti, non potranno ricondursi ad esempio, anche indirettamente, al trattamento dei dati personali sensibili o dei dati giudiziari.

3.2.6 - Registro elettronico

La scuola si avvale di diversi strumenti informatici a sostegno sia delle funzioni amministrative che di quelle didattiche. Il software Argo a cui possono accedere Dirigente, il DSGA e il personale amministrativo offre supporto alla gestione amministrativa delle utenze, venendo incontro alle nuove esigenze di integrazione dei servizi e dematerializzazione che sono uno degli obiettivi delle pubbliche amministrazioni.

docenti

Il registro elettronico "Didup" di Argo supporta i docenti nella gestione quotidiana delle proprie attività didattiche, rendendo le operazioni di valutazione e di scrutinio più efficienti. L'accesso dei docenti al registro avviene attraverso credenziali di cui il docente è responsabile che gli vengono assegnate dal personale incaricato alla gestione degli accessi. All'interno dell'area Didup è possibile accedere al registro di classe, al registro del docente. La compilazione viene effettuata giornalmente secondo modalità illustrate ai docenti ad inizio anno scolastico attraverso specifici incontri formativi/informativi tenuti dalla funzione Referente e/o dai Responsabili di Argo. Eventuali modifiche alla piattaforma e/o aggiornamenti della stessa vengono prontamente comunicati a tutto il personale docente che viene adeguatamente istruito attraverso specifici incontri. Il registro contiene anche diversi spazi per l'archiviazione della documentazione dei docenti (verifiche effettuate con l'uso delle TIC) secondo le procedure illustrate nel Piano di DDI elaborato dall'Istituto. All'interno della piattaforma Argo è possibile accedere anche all'area dedicata al personale tramite la quale possono essere richiesti permessi brevi e/o assenze.

Genitori

I genitori accedono al registro elettronico attraverso l'applicazione ARGO Famiglia utilizzando credenziali a loro assegnate dal sistema grazie alla quale possono visualizzare il registro di classe, la sezione bacheca visualizzando le comunicazioni che vengono indirizzate alla classe o direttamente al genitore da parte dei docenti della classe e alla sezione dei compiti assegnati. Possono altresì prendere visione delle assenze e giustificare le stesse, possono visualizzare gli avvisi apportando

la spunta di presa visione e approvazione, quando richiesto e possono scaricare le pagelle del/ della proprio/a figlio/a.

Le credenziali di accesso sono personali e i genitori devono garantirne la custodia. Vengono consegnate dalla segreteria alunni ai genitori che prendono visione con spunta dell'informativa sul sito stesso. L'informativa sul trattamento dei dati sarà resa visibile sul sito della scuola nell'area regolamento o sul registro Argo, sul quale i genitori appongono un flag per presa visione e autorizzazione (Allegato 6 ePolicy - Informativa per il trattamento dei dati personali – alunni e loro famiglie).

3.2.7 - Social network

E' fatto esplicitamente divieto ad alunni, docenti, personale ATA e Genitori di pubblicare immagini, video, commenti su qualunque social network se non ad esclusivo scopo didattico previa autorizzazione esplicita da parte dei tutori, in accordo con quanto previsto nel rispetto della privacy e delle regole relative ai Social Network. Si ricorda che la diffusione di foto/filmati senza il consenso e, comunque, all'insaputa delle persone coinvolte può determinare ricadute di carattere anche penale, come ad esempio la diffamazione. Si invitano pertanto tutti gli studenti a non prelevare o diffondere immagini, video o registrazioni – anche solo audio – non autorizzate, ed eliminare da internet eventuali riferimenti offensivi o comunque illeciti (ed inopportuni) nei confronti dell'Istituto e dei suoi docenti e studenti. Allo stesso tempo, si invitano gli allievi e i genitori a fare un uso prudente dei Social Network, in particolare Facebook e Whatsapp, limitandone l'uso alle sole comunicazioni funzionali, evitando ad ogni modo di esprimere giudizi sull'operato degli altri studenti o del personale della scuola, giudizi che una volta pubblicati comportano sempre una assunzione di responsabilità da parte di chi li ha scritti o anche semplicemente diffusi.

La scuola ha un account twitter: ICCasteldaccia palermo e un account instagram: ICCasteldacciapalermo, creato dall'AD di Istituto e gestiti da docenti con il coordinamento di una funzione delegata allo scopo annualmente. I docenti che ne gestiscono i contenuti sono responsabili di quanto pubblicato in accordo con la normativa a tutela della privacy.

La scuola ha un canale youtube: (<https://www.youtube.com/channel/UCJOZK93nJpyVAniywP8oQtA/featured>) per la pubblicazione di materiali video inerenti attività didattiche svolte dai docenti insieme agli studenti in orario curriculare ed extracurriculare. Il canale è gestito dal DSGA che effettua la pubblicazione del materiale che si riferisce alla divulgazione di specifiche iniziative/attività didattiche. Sono da ritenersi autorizzati i video contenenti immagini di minori che in nessun modo devono essere riconoscibili, come da informativa per il trattamento dei dati personali di cui viene presa visione sul sito della scuola/registro Argo e del quale viene fornita autorizzazione in segreteria (Allegato 6 ePolicy - Informativa per il trattamento dei dati personali – alunni e loro famiglie).

I coordinatori delle classi e tutti i docenti che, nel corso di attività didattiche specifiche svolte in orario scolastico ed extrascolastico, pubblicano materiale sui propri canali a scopo didattico-divulgativo avranno cura verificare che l'immagine dello studente minorenne che viene ritratto nella presentazione pubblicata non sia riconoscibile.

Nel caso in cui la classe o il singolo studente partecipi ad attività esterne nelle quali è possibile che vengano pubblicate immagini degli studenti sarà cura dell'Ente che gestisce la manifestazione/evento acquisire la liberatoria all'uso delle immagini.

3.3 - BYOD

La presente ePolicy conterrà indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device"). Risulta infatti fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/le studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

Vengono di seguito definite per le diverse categorie di utenti le modalità di gestione degli strumenti personali in uso in Istituto.

3.3.1- Studenti

Il Regolamento di Istituto vieta l'uso del cellulare personale che deve essere consegnato all'inizio delle lezioni al docente della classe e tenuto sotto custodia in appositi spazi predisposti per tutta la durata delle lezioni. Per specifiche attività è permesso agli studenti l'accesso ad Internet da propri dispositivi (esclusivamente tablet e pc) utilizzando la rete Wi-Fi dell'Istituto esclusivamente utilizzando i voucher comunicati dal docente con scadenza temporale e fornite dalla funzione di riferimento (vedi punto 3.2). Nel caso di specifiche esigenze di studenti che necessitano di un uso continuativo di dispositivi elettronici propri (ad. es. alunni Bes o con specifiche necessità), gli stessi potranno essere profilati sul firewall del sistema su richiesta esplicita dei genitori, per un accesso diretto alla rete. Nel caso in cui gli studenti volessero utilizzare il proprio dispositivo per utilizzare i supporti didattici non cartacei, gli stessi dovranno essere scaricati sul proprio dispositivo e fruiti offline. Gli studenti potranno altresì utilizzare i propri strumenti ricorrendo alla rete personale sempre sotto la sorveglianza del personale docente ed esclusivamente per attività didattiche.3.-

3.3.2 - Docenti

E' consentito l'uso della strumentazione personale dei docenti all'interno delle aule didattiche solo per fini professionali o didattici. I docenti possono accedere alla rete internet con la propria strumentazione attraverso credenziali registrate, comunicate per email dall'amministratore del sistema.

3.3.3 - Personale ATA

Allo scopo di mantenere l'efficienza della linea disponibile non è consentito accesso alla rete didattica con i propri strumenti personali al personale ATA in nessuno dei plessi dell'IC Casteldaccia. Nel caso in cui fosse necessario accedere alla rete per corsi di aggiornamento il DSGA comunicherà gli eventuali voucher necessari allo scopo, mettendo a disposizione gli strumenti della scuola.

Cap 4 - Segnalazione e gestione dei casi

4.1 - Cosa Segnalare

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire). Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Queste, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola.

Nelle procedure sono indicate le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso, nonché le modalità di coinvolgimento del Dirigente Scolastico e del Referente per il contrasto al bullismo e al cyberbullismo. Inoltre, la scuola individua le figure che costituiranno un team preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica. La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

A seguire, le problematiche a cui fanno riferimento le procedure allegate:

Cyberbullismo: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/le studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).

Adescamento online: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

Sexting: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere, per quanto possibile, la rimozione del materiale on-line e il blocco della sua diffusione per mezzo dei dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete.

Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;
- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

Per i casi che non rientrano in queste categorie, ma che costituiscono un'infrazione alle regole dell'Istituto in riferimento all'utilizzo delle TIC e/o della rete scolastica i Referenti e il team di supporto sono a disposizione per fornire indicazioni e/o raccogliere le segnalazioni di docenti, alunni e genitori. La segnalazione può essere effettuata in presenza contattando direttamente a scuola un componente del team di supporto o tramite email all'indirizzo del gruppo di supporto cyberbull@istitutocomprensivocasteldaccia.net. La segnalazione deve contenere una breve sintesi del caso osservato, il riferimento al luogo in cui è avvenuto l'evento e l'indicazione delle persone coinvolte. Sarà compito del team condividere con il DS e il coordinatore della classe quanto contenuto nella segnalazione decidendo come procedere ulteriormente in base alla gravità dell'infrazione.

La scuola gestirà le infrazioni all'e-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni con il coinvolgimento delle parti interessate.

In base alla tipologia e gravità dell' infrazione l'Istituto intende procedere come segue:

TIPOLOGIA DI INFRAZIONE	PROVVEDIMENTI	FIGURE COINVOLTE
	Annotazione sul registro di classe; Incontri con gli alunni coinvolti con assetto di ascolto reciproco e presa di coscienza; Discussione aperta in classe;	
Atteggiamenti intimidatori episodici verso gli altri (condotti in contesti reali e/o attraverso la comunicazione digitale)	Attività ludico-espressive per la presa di coscienza; Informazione e coinvolgimento dei genitori sospensione breve (max 3 giorni) con obbligo di frequenza alle attività didattiche Richiamo e annotazione sul registro;	Dirigente Scolastico, Referente e team per Bullismo e Cyber bullismo, Coordinatore e Docenti della classe, Genitori, Psicopedagoga
Danni alle strutture/attrezzature scolastiche (hardware e software), uso improprio delle tecnologie	Incontri con gli alunni coinvolti con assetto di ascolto reciproco e presa di coscienza; Comunicazione ai genitori per il risarcimento stabilito sospensione breve (max 3 giorni) con obbligo di frequenza alle attività didattiche	Dirigente Scolastico, Referente per le nuove tecnologie, Referente Cyberbullismo e team per Bullismo e Cyberbullismo, Coordinatore di classe, Docenti Genitori, Psicopedagoga

Nel caso in cui si renda opportuno il provvedimento di sospensione, questo deve essere comminato dal Consiglio di Classe in seduta straordinaria (senza componente genitori) con la presenza di un componente del Team per il Bullismo e il Cyberbullismo a supporto di un'ottimale progettazione dell'intervento rieducativo e/o riparativo. Le decisioni intraprese devono essere tempestivamente rese note al genitore attraverso comunicazione ufficiale della Segreteria scolastica.

Il team per il Bullismo e il Cyberbullismo e il Ref. per il Cyberbullismo hanno il compito di raccordarsi con i docenti della classe coinvolta per verificare, succesivamente, l'effettiva efficacia dell'intervento rieducativo.

4.2 - Quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale (ex [art. 357 c.p.](#)) in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Il Codice Penale Italiano, all'[art. 357](#), definisce il pubblico ufficiale come colui che esercita una "pubblica funzione legislativa, giudiziaria o amministrativa". Questa definizione si estende ai docenti nel momento in cui sono impegnati nell'esercizio delle loro funzioni all'interno degli istituti scolastici.

La Corte di Cassazione, con la sentenza [n. 15367/2014](#), ha ribadito la qualifica di pubblico ufficiale per l'insegnante, estendendo tale riconoscimento non solo alla tenuta delle lezioni, ma anche a tutte le attività connesse. Questo include, ad esempio, gli incontri con i genitori degli allievi.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite da un team di docenti composto da:

1. Dirigente
2. Docente referente,
3. L'animatore digitale (secondo il Piano Nazionale per la Scuola Digitale, abbreviato in PNSD, introdotto dalla Legge 107/2015)
4. Referente bullismo (ex. Legge Italiana Contro il Cyberbullismo, l. 71/2017)
5. Altri docenti già impegnati nelle attività di promozione dell'educazione civica.

Le situazioni di pregiudizio presunto o reale possono richiedere il supporto e l'intervento di esperti esterni alla scuola.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due macro - casi:

CASO A (SOSPETTO) - Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente. La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, il Dirigente e i docenti coinvolti procedono alla valutazione del caso (valutare l'invio o meno della relazione agli organi giudiziari preposti) e agiscono tramite percorsi di sensibilizzazione.

CASO B (EVIDENZA) – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente. La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, si procede alla valutazione approfondita e alla verifica di quanto segnalato, avviando (se appurato la rilevanza penale) la procedura giudiziaria con denuncia all'autorità giudiziaria per attivare un procedimento penale.

Qualora si rilevasse un fatto riconducibile alla fattispecie di reato, l'insegnante - nel ruolo di pubblico ufficiale - non deve procedere con indagini di accertamento ma ha sempre l'obbligo di segnalare l'evento all'autorità giudiziaria. (ex. l. 71/2017). Con autorità competente si intendono:

- Procure Ordinarie: nel caso in cui il minore/i sia la vittima/e e il presunto autore del reato sia maggiorenne,
- Procura Minorile: in caso il presunto autore del reato sia minorenni.

Vi è anche l'obbligatorietà della segnalazione delle situazioni di pregiudizio a carico dei minori: L. 216/1991: per le situazioni di grave rischio l'istituzione scolastica è tenuta alla segnalazione delle medesime. Per pregiudizio si intende una condizione di rischio o grave difficoltà che provocano un danno reale o potenziale alla salute, alla sopravvivenza, allo sviluppo o alla dignità del bambino, nell'ambito di una relazione di responsabilità, fiducia o potere.

La segnalazione come da procedura interna è il primo passo per aiutare un minore che vive una situazione di rischio o di grave difficoltà e va intesa come un momento di condivisione e solidarietà nei confronti del minore. La mancata segnalazione costituisce, infatti, omissione di atti d'ufficio (art.328 C.P.).

Può essere utile, valutando accuratamente ciascuna situazione, attivare colloqui individuali con tutti i minori coinvolti, siano essi vittime, testimoni e/o autori. È importante considerare il possibile coinvolgimento dei genitori e di coloro incaricati della tutela dei minori coinvolti. L'intervento va indirizzato valutando l'eventuale impatto educativo e/o il contesto emotivo senza discriminare tra vittime, testimoni e/o autori.

Prevedere possibili incontri di mediazione tra i minori coinvolti vanno ponderati con la consapevolezza del loro stato emotivo, anche e in base agli elementi raccolti in merito del fatto/episodio avvenuto (elementi che si dovrebbero valutare di caso in caso). Importante è prevedere il coinvolgimento dei genitori sia della vittima che del bullo (ove possibile).

Anche i genitori devono e possono segnalare casi di sospetto o evidenza dei fenomeni, segnalarlo al Dirigente, o al docente coordinatore di classe o referente di istituto oppure direttamente al team antibullismo attraverso apposita procedura che definisce l'istituto (mail ad hoc, tramite gli uffici e postazioni specifiche, etc...).

Gli insegnanti e i genitori, come studenti e studentesse, si possono rivolgere alla Helpline del progetto Generazioni Connesse, al numero gratuito 19696, attraverso la chat disponibile sul [sito](#) o tramite chat WhatsApp per ricevere supporto e consulenza. Per tutti i dettagli, il riferimento è agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

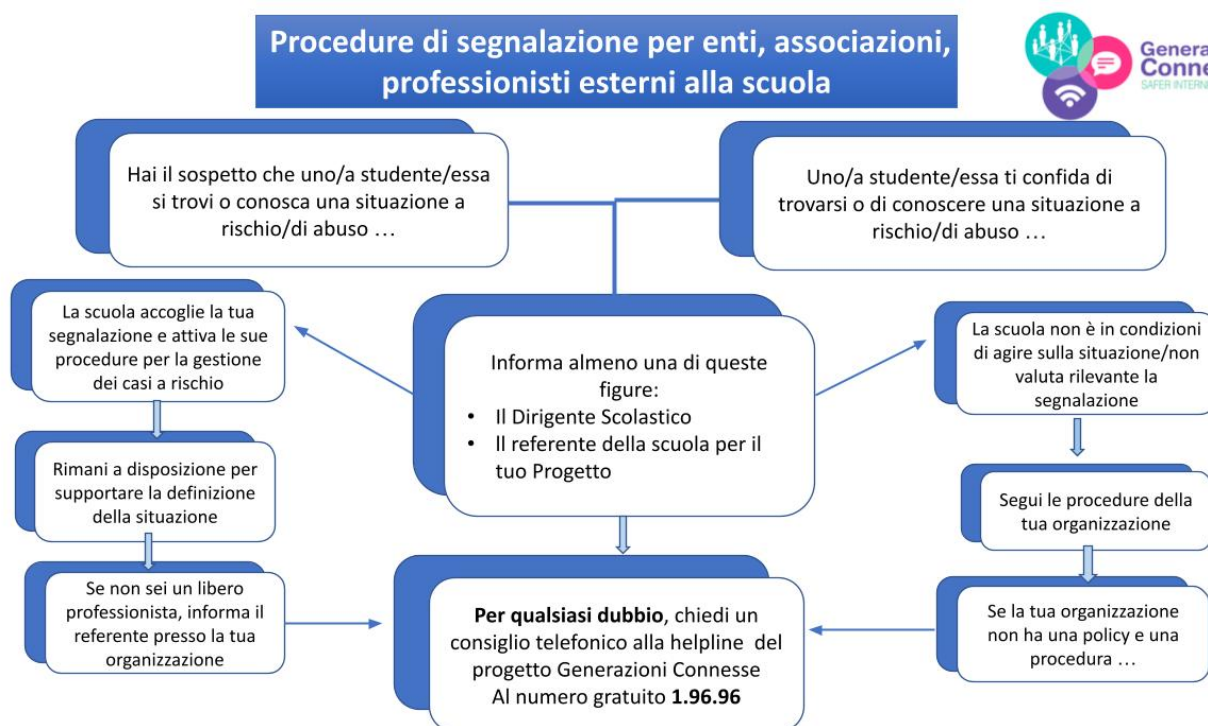
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola; sportello di ascolto con professionisti; docente referente per le segnalazioni.

In particolare, sarebbe utile che la scuola attivi un sistema di segnalazione utile anche al monitoraggio dei fenomeni dal

quale partire per integrare azioni didattiche preventive e giornate di sensibilizzazione, insieme agli Enti/Servizi presenti sul territorio di riferimento. Importante, altresì, immaginare e programmare percorsi di peer education per la prevenzione e il contrasto degli agiti.

Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle [Linee di Orientamento per la prevenzione e il contrasto dei fenomeni di Bullismo e Cyberbullismo del MI \(Ministero dell'Istruzione\)](#) aggiornate al 2021, al Patto educativo di corresponsabilità e annessa appendice relativa agli impegni che le parti in causa dovranno assumere per l'espletamento efficace della DID e, in ultimo, al Piano scolastico per la Didattica Digitale Integrata, allegato al PTOF.

Procedure



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo



Il docente ha evidenza che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Se non è già stato fatto, avvisa il referente per il cyberbullismo (e/o il team antibullismo) che attiva le procedure ("Corso 4" della piattaforma ELISA) e il Dirigente Scolastico.

Ricordare sempre che in base alla legge 71-2017:

A) Se c'è fattispecie di reato va fatta la segnalazione alle forze dell'ordine

B) Se non c'è fattispecie di reato.

Il DS (e/o il team antibullismo):

- informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto) su quanto accade e condivide informazioni e strategie.
- Informa i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy)
- Attiva il consiglio di classe.

Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

NELLE CLASSI

Il team antibullismo collabora coi docenti della classe per realizzare l'intervento nella classe:

a seconda della situazione valutata se

- affrontare direttamente l'accaduto o
- sensibilizzare la classe (vedi Corso 4 Piattaforma Elisa)
- trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.

A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla Polizia Postale:

a) contenuto; b) modalità di diffusione.

Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



Il docente riceve una segnalazione (da un genitore, un altro studente ...) o sospetta che stia accadendo qualcosa a uno/a studente/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

Condividi con il referente o al team antibullismo: si attiva il processo di attenzione e valutazione a cura del referente.

- Insieme si valuta se è il caso
- di avvisare il consiglio di classe;
 - di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.

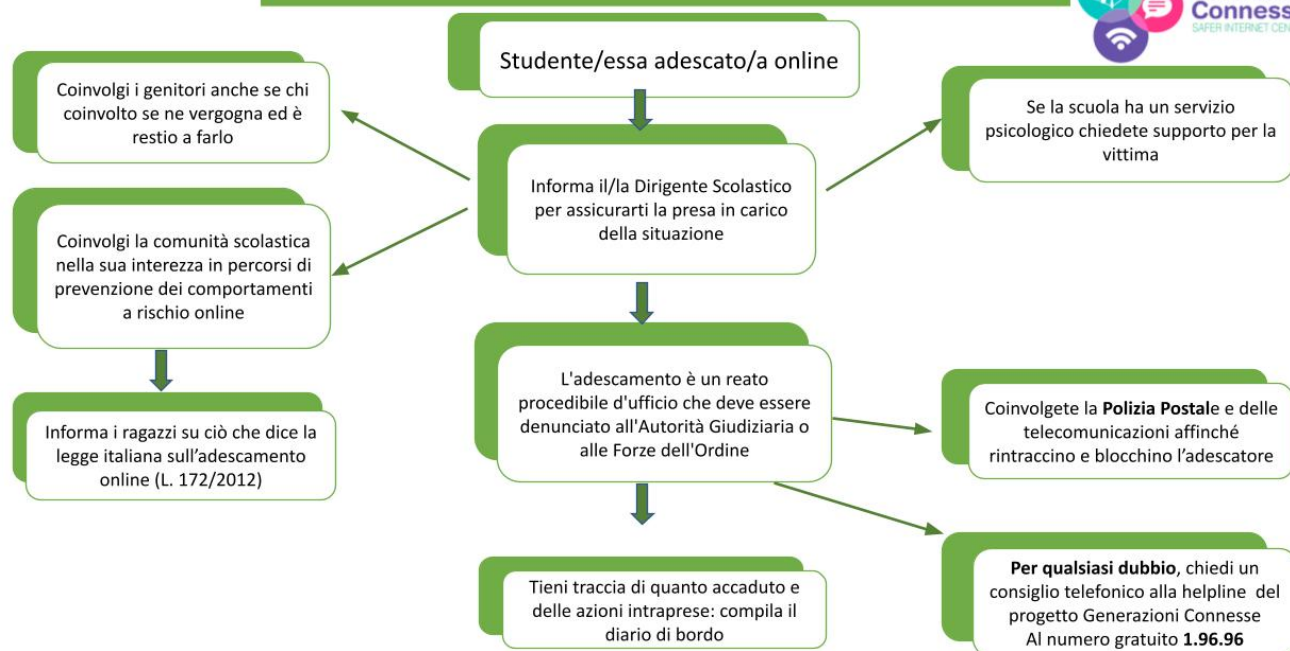
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Scarica le linee di orientamento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo

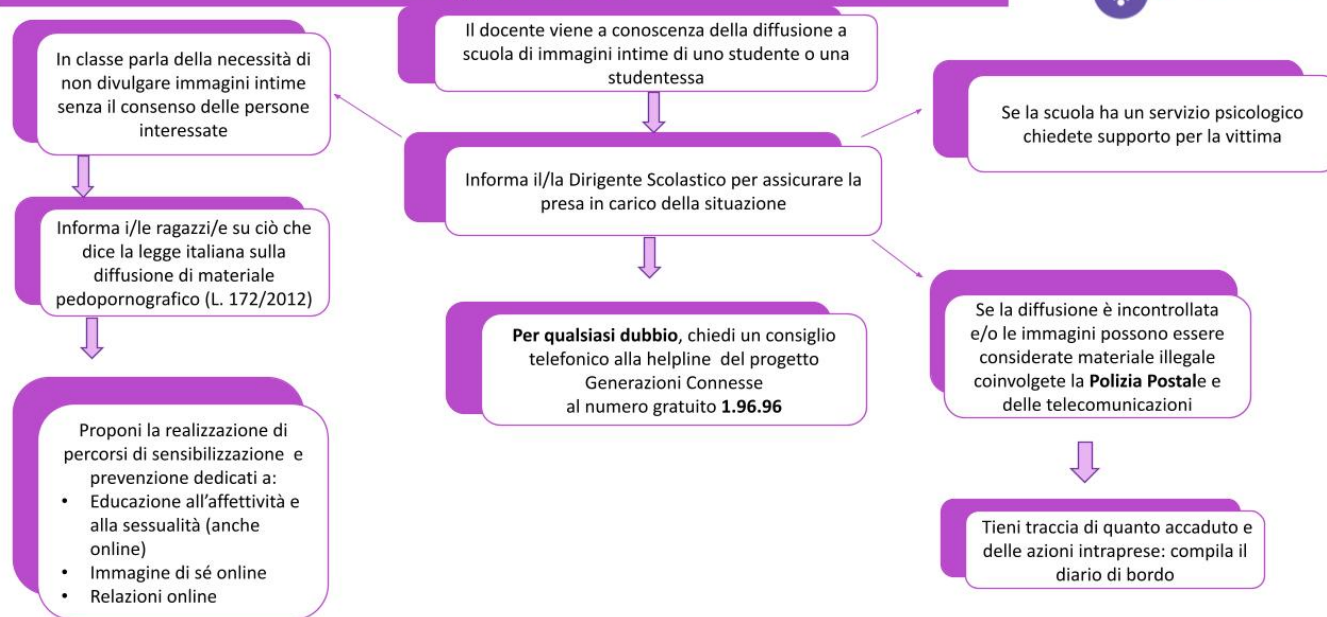
Se emergono evidenze passa allo schema successivo

Ricorda a studenti/esse che possono chiedere in qualsiasi momento una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 o via chat

Procedure interne: cosa fare in caso di Adescamento Online?



Procedure interne: cosa fare in caso di diffusione non consensuale di immagini intime?



I casi segnalati devono essere registrati ricorrendo alla compilazione dell'allegato 8 _ Modulo segnalazione casi di rischio. Sarà compito del Referente e dei componenti del "Team Antibullismo/Cyberbullismo e Team per l'Emergenza" mettere in atto le procedure necessarie dopo avere accolto la segnalazione.

Il Referente e il Team si incontrano periodicamente con cadenza bimestrale, fatta eccezione interventi urgenti. All'inizio dell'anno scolastico, in riferimento alle necessità emerse, il gruppo programma interventi e progetta nel dettaglio quanto previsto nel piano di azione facendosi promotore delle iniziative tra docenti e studenti della scuola.

Il componente del "Tavolo Permanente di Monitoraggio" con i suoi componenti avrà il compito di effettuare un controllo dei dati raccolti (vedi Allegato 9- Diario di Bordo dei casi), promuovendo interventi e favorendo la collaborazione tra le varie parti. Il tavolo si riunisce almeno tre volte durante ciascun anno scolastico (inizio anno scolastico, fase intermedia e fine anno scolastico) secondo un calendario stabilito.

Elenco Allegati E-policy:

- Allegato 1- ePolicy: Informativa e Dichiarazione di presa visione e adesione all'informativa sull'Epolicy dell'IC Casteldaccia e Modulo segnalazione di situazioni a rischio per personale esterno
- Allegato 2 ePolicy: Autorizzazione e istruzioni al trattamento dei dati - assistenti amministrativi ;
- Allegato 3:ePolicy: Autorizzazione e istruzioni al trattamento dei dati – docenti;
- Allegato 4 ePolicy: Autorizzazione e istruzioni al trattamento dei dati collaboratori scolastici;
- Allegato 5 ePolicy: Autorizzazione e istruzioni al trattamento dei dati – AD e team digitale;
- Allegato 6 ePolicy: Informativa per il trattamento dati personali – alunni e loro famiglie
- Allegato 7 ePolicy: Regolamento uso Google Workspace e suoi allegati
- Allegato 8 ePolicy: Modulo per la segnalazione delle situazioni di rischio
- Allegato 9 ePolicy: Diario di Bordo

Allegato 1 ePolicy- Informativa e Dichiarazione di presa visione e adesione all'informativa sull'Epolicy per “Personale esterno” dell'IC Casteldaccia e Modulo segnalazione di situazioni a rischio



Informativa e Dichiarazione di presa visione e adesione all'informativa sull'Epolicy per "Personale esterno" dell'IC Casteldaccia e Modulo segnalazione di situazioni a rischio

MINISTERO DELLA PUBBLICA ISTRUZIONE

Istituto Comprensivo Statale "Casteldaccia"

Istituto ad indirizzo musicale

Via Carlo Cattaneo N.80 - 90014 CASTELDACCIA (PA) C.F.: 90007610828 - Cod. Min.: PAIC84200X

☎ 091-954299 - Fax 091-9100217

Informativa e Dichiarazione di presa visione e adesione all'informativa sull'Epolicy per "Personale esterno" dell'IC Casteldaccia e Modulo segnalazione di situazioni a rischio

Premessa e obiettivi dell'informativa

Il presente documento ha lo scopo di fornire informazioni relative al regolamento in vigore all'interno dell'Istituto a tutela di studenti e studentesse, ai sensi della normativa vigente e delle norme comportamentali previste dall'Epolicy di Istituto.

Il presente documento è destinato a tutti coloro che operano nella scuola individualmente o come facenti parte di organizzazioni esterne che collaborano a titolo gratuito o con contratto per la realizzazione di attività didattiche, di sensibilizzazione /formazione previste dal Consiglio di Classe e/o proposte dal singolo docente nell'ambito delle proprie discipline e concordate preventivamente con il Dirigente Scolastico.

Ambiti di applicazione (inserire il titolo del progetto specifico o delle attività):

Ruoli (inserire i nomi dei docenti di riferimento del progetto specifico o delle attività):

Regolamento / Codice di comportamento

1. E' possibile usare gli strumenti della scuola previa richiesta al docente

di supporto all'attività utilizzando l'account studente; La richiesta verrà formalizzata dalla persona che esercita l'incarico al docente che è incaricato di seguire l'attività (coordinatore della classe, docente referente, tutor). Il docente della scuola riferirà quanto richiesto alla funzione Funzione strumentale nuove tecnologie secondo le modalità in atto presso l'Istituto (Calendar strumenti/aule specifiche almeno una settimana prima l'evento)

2. Qualunque tipo di software necessiti di installazione negli strumenti in dotazione alla scuola deve essere preventivamente concordato con la funzione di riferimento (Funzione strumentale nuove tecnologie);
3. Se si usano App o Tools per la partecipazione degli studenti ed è necessaria l'iscrizione da parte degli stessi inserendo dati anagrafici e/o email è necessario verificare con la funzione di riferimento (Coordinatore di classe e Gestione Workspace for education) se tali app/tool rispettano quanto previsto dalle norme vigenti in fatto di tutela della privacy o concordare con la funzione di riferimento la modalità con cui procedere alla creazione del profilo da parte degli studenti.
4. E' fatto divieto di effettuare foto e/o riprese video/audio degli studenti per attività diverse da quelle didattiche sia all'interno dei locali scolastici, che all'esterno che durante collegamenti online, senza avere avuto esplicita liberatoria da parte dei genitori degli studenti coinvolti.
5. Durante le attività svolte a scuola sia a titolo remunerativo che gratuito ci si impegna a vigilare sul corretto comportamento degli studenti che potranno utilizzare i propri dispositivi solo ed esclusivamente per svolgere le attività proposte e a comunicare tempestivamente al docente di riferimento (tutor, docente) qualunque comportamento considerato a rischio
6. Applicare le procedure previste dal regolamento e dall'e-policy e comunicare eventuali comportamenti scorretti osservati, utilizzando la modulistica allegata
7. E' fatto esplicito divieto di avere contatti con gli studenti per attività didattiche svolte in orario curriculare o extracurriculare da parte di soggetti che abbiano condanne o procedimenti in corso per alcuni reati previsti dal Codice penale:

articoli 600-bis (prostituzione minorile),

600-ter (pornografia minorile),

600-quater (detenzione di materiale pornografico),

600-quinquies (iniziative turistiche volte allo sfruttamento della prostituzione minorile),

609-undecies (adescamento di minorenni),

l'irrogazione di sanzioni interdittive all'esercizio di attività che

comportino contatti diretti e regolari con i minori.

Si allega alla presente Modulo per la segnalazione di situazioni a rischio da consegnare al docente di riferimento dell'attività svolta.

Il Dirigente si riserva di procedere nel seguente modo in base ai diversi casi secondo quanto segue. Provvedimenti nel caso di:

omessa segnalazione: Il Dirigente si riserva di interrompere in qualunque momento l'incarico in essere tra la scuola e chi presta il servizio anche se a titolo gratuito;

comportamenti in violazione del codice di comportamento: Il Dirigente si riserva di interrompere in qualunque momento l'incarico in essere tra la scuola e chi presta il servizio anche se a titolo gratuito; Il Dirigente si riserva di procedere secondo quanto previsto da legge in dipendenza della violazione che è stata rilevata.

Il sottoscritto _____ nato a _____ residente a _____ doc
di riferimento _____

dichiara di avere preso visione dell'informativa relativa all'ePolicy di Istituto e di accettare i contenuti della stessa.

data

Firma

Allegato 2 ePolicy - Autorizzazione-e-istruzioni-al-trattamento-dati-assistenti-amministrativi



Autorizzazione-e-istruzioni-al-trattamento-dati-assistenti-amministrativi

MINISTERO DELLA PUBBLICA ISTRUZIONE

Istituto Comprensivo Statale "Casteldaccia"

Istituto ad indirizzo musicale

Via Carlo Cattaneo N.80 – 90014 CASTELDACCIA (PA) C.F.: 90007610828 – Cod. Min.: PAIC84200X

☎ 091-954299 – Fax 091-9100217

IL DIRIGENTE SCOLASTICO

VISTO il Regolamento UE 2016/679 noto come “General Data Protection Regulation” (GDPR); VISTO il “Codice della Privacy” D.Lgs 196/2003 novellato dal D.Lgs. 101/2018;

VISTO il DM 305/2006;

Visto il Modello Organizzativo per la privacy e la protezione dei dati, adottato dall'Istituto;

PREMESSO CHE

- ai sensi dell'art. 4.7 del GDPR il Titolare del trattamento di dati personali è l'Istituto Scolastico stesso, di cui il dirigente scolastico è legale rappresentante pro tempore;
- in base al principio di responsabilizzazione (accountability) ex art. 5.2 e art. 25 del GDPR il Titolare deve definire le misure tecniche ed organizzative adeguate a ciascuna attività di trattamento dei dati personali ed impartire istruzioni a tutti coloro che sono stati autorizzati al trattamento dei dati personali (artt. 5, 24, 29 e 32);
- sono soggetti autorizzati al trattamento tutti i dipendenti dell'istituzione scolastica che trattano i dati personali;
- il Titolare del trattamento ha individuato un gruppo omogeneo di “autorizzati al trattamento di dati personali” negli assistenti amministrativi ATA e nel DSGA in servizio presso l'istituzione scolastica, per il quale il trattamento dei dati è obbligatorio il necessario per lo svolgimento delle proprie specifiche funzioni;

CONSIDERATO CHE

- l'autorizzazione al trattamento dei dati personali non implica l'attribuzione di funzioni ulteriori rispetto a quelle già assegnate, né compensi economici aggiuntivi, ma consente di trattare i dati di cui si viene a conoscenza nell'esercizio della mansione assegnata;
- la S.V., in servizio presso questo Istituto Scolastico e in riferimento ai compiti svolti e alle mansioni assegnate ha necessità di effettuare attività di trattamento dei dati personali;

AUTORIZZA la S.V.

al trattamento dei dati personali detenuti da questa istituzione scolastica, come individuati nel seguito del presente documento, in riferimento al profilo di appartenenza della S.V.

Costituisce trattamento qualunque operazione, svolta con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati, necessari nel particolare per le seguenti attività:

Area didattica:

- gestione archivi elettronici alunni e genitori;
- gestione archivi cartacei, fascicoli personali alunni;

- consultazione documenti e registri di attestazione dei voti e di documentazione della vita scolastica dello studente, nonché delle relazioni tra scuola e famiglia quali ad esempio richieste, istanze e corrispondenza con le famiglie;
- gestione contributi e/o tasse scolastiche versati da alunni e genitori;
- adempimenti connessi alla corretta gestione del registro infortuni;
- adempimenti connessi ai viaggi di istruzione e alle uscite didattiche.

Area del personale:

- gestione degli archivi elettronici del personale ATA e Docenti;
- gestione degli archivi cartacei del personale ATA e Docenti;
- gestione dei documenti e dei registri relativi alla vita lavorativa dei dipendenti (quali ad esempio assenze, convocazioni;)
- gestione delle comunicazioni, della documentazione sullo stato del personale, degli atti di nomina dei supplenti e dei decreti della dirigente;
- operazioni di consultazione ed estrazione dei dati dai verbali degli organi collegiali.

Area del protocollo e dell'archivio della corrispondenza ordinaria

- attività di protocollazione e smistamento alle aree competenti degli atti in ingresso all'Istituto, siano essi recapitati in forma cartacea che elettronica (PEC, mail, eccetera);
- attività di protocollazione ed invio ai destinatari per competenza degli atti in uscita dall'Istituto, siano essi inviati in forma cartacea che elettronica (PEC, mail, eccetera).

Contabilità e finanza

- gestione degli archivi elettronici della contabilità;
- gestione degli stipendi e dei pagamenti, nonché degli adempimenti di carattere previdenziale;
- gestione della documentazione relativa alle ore di servizio (quali ad esempio registrazione delle ore eccedenti, eccetera);
- tenuta dei documenti e dei registri relativi all'attività lavorativa dei dipendenti (quali ad esempio assenze, convocazioni, eccetera);

- gestione dei rapporti con i fornitori;
- gestione del programma annuale e del fondo di istituto;
- corretta tenuta dei registri contabili previsti dal decreto interministeriale numero 129/2018 e correlata normativa vigente.

Il trattamento dovrà essere limitato alle operazioni necessarie ed indispensabili all'adempimento delle mansioni connesse al profilo della S.V., in osservanza delle norme di legge, dei regolamenti interni, delle circolari, degli ordini di servizio e delle istruzioni impartite dal titolare del trattamento e dei suoi delegati.

La S.V. effettuerà le operazioni sopra descritte nel rigoroso rispetto delle istruzioni operative che seguono.

MISURE OPERATIVE GENERICHE

Nello svolgimento delle sue mansioni, la S.V. dovrà:

- accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni;
- trattare i dati personali in modo lecito e secondo correttezza;
- raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi, ed utilizzarli solo per operazioni di trattamento compatibili con le finalità connesse all'attività svolta;
- verificare che i dati siano esatti e, se necessario, aggiornarli;
- verificare che i dati siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- conservare i dati in forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
- non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale;
- informare prontamente il Titolare o il Responsabile per la Protezione dei Dati dell'Istituto (RPD), di seguito indicato, di ogni circostanza idonea a determinare pericolo di dispersione o utilizzo non autorizzato dei dati stessi;
- non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Titolare e, comunque, senza avere la certezza della loro identità;
- non lasciare a disposizione di estranei documenti o supporti di memorizzazione (cd, dvd, pen drive) che contengono dati personali o sensibili;

- accertarsi della distruzione di documenti inutilizzati contenenti dati personali o sensibili;
- non abbandonare la postazione di lavoro, senza aver provveduto a custodire in luogo sicuro i documenti contenenti dati personali;
- collaborare con il Responsabile per la Protezione dei Dati dell'Istituto (DPO), indicato nel seguito del documento, per aspetti specifici relativi ad ogni nuova attività che comporti il trattamento dei dati personali.

MISURE OPERATIVE SPECIFICHE ALL'UTILIZZO DI TECNOLOGIE INFORMATICHE

- scegliere per i diversi software gestionali (area personale, area didattica, eccetera) una password che sia composta da otto caratteri e non facilmente intuibile, evitando che contenga riferimenti alla propria persona (es. proprio nome o di congiunti, date di nascita, ecc.);
- curare la conservazione della propria password dei software gestionali e non comunicarla per alcun motivo a soggetti terzi;
- cambiare periodicamente (almeno una volta ogni tre mesi) la propria password dei software gestionali;
- adottare le stesse cautele di cui sopra per le password di qualsiasi altra piattaforma software ad uso personale e potenzialmente interessata al trattamento di dati personali (mail, account per piattaforme terze, eccetera);
- effettuare il logoff dai software gestionali e, laddove presenti, da sistemi di autenticazione di rete al termine di ogni sessione di lavoro;
- spegnere correttamente il computer al termine di ogni sessione di lavoro al fine di agevolare, se utilizzati, l'azione di software specifici di congelamento delle configurazioni degli stessi;
- non abbandonare la propria postazione di lavoro per la pausa o altri motivi senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
- nella comunicazione multimediale con alunni e genitori utilizzare esclusivamente le piattaforme informatiche messe a disposizione dall'istituto; è fatto divieto utilizzare social network quali facebook o altri;
- nell'utilizzo della posta elettronica non aprire documenti di cui non sia certa la provenienza e controllare accuratamente l'indirizzo dei destinatari prima di inviare email contenenti in allegato o nel corpo del messaggio dati personali;
- nell'esercizio delle proprie mansioni utilizzare esclusivamente le apparecchiature informatiche fornite dalla scuola, presenti negli uffici di segreteria: ufficio segreteria del personale, ufficio di segreteria didattica, ufficio affari generali, eccetera), in quanto tali attrezzature sono regolarmente sottoposte a rigide misure di sicurezza e in linea con le misure minime di sicurezza ICT emanate dall'AGID.

È esplicitamente vietato:

DIVIETI ESPLICITI

effettuare copie su supporti magnetici o trasmissioni non autorizzate di dati oggetto del trattamento o di atti inerenti le mansioni del proprio profilo professionale;

- diffondere e/o divulgare notizie inerenti le proprie mansioni o quelle di altre unità di personale al di fuori degli uffici amministrativi (atti documentati in originale o in copia fotostatica, password, login, ecc.);
- effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento;
- sottrarre, cancellare, distruggere, senza esplicita autorizzazione, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento;
- diffondere via WEB (o altro strumento) dati personali delle famiglie o di altri interessati a meno di quelli, pertinenti e minimi, inclusi negli atti da pubblicare in albo pretorio o in amministrazione trasparente.

Qualunque violazione delle modalità sopra indicate dà luogo a precise responsabilità, ai sensi delle normative vigenti.

Riferimenti del DPO (Responsabile per la Protezione dei Dati) dell'Istituto NetSense S.r.l., con sede legale in via Novaluce 38, a Tremestieri Etneo (CT)

Partita IVA 04253850871,

email: info@netsenseweb.com PEC: netsense@pec.it,

nella persona dell'Ing. Renato Narcisi (PEC: renato.narcisi@arubapec.it)

Il titolare del trattamento dei dati

L'istituto nella persona di Giovanni Taibi

firma autografa sostituita da indicazione a
a mezzo stampa, ai sensi dell'art.3 D.Lgs. 39/1993

Allegato 3 ePolicy - Autorizzazione e istruzioni al trattamento dei dati personali docenti



MINISTERO DELLA PUBBLICA ISTRUZIONE

Istituto Comprensivo Statale "Casteldaccia"

Istituto ad indirizzo musicale

Via Carlo Cattaneo N.80 – 90014 CASTELDACCIA (PA) C.F.: 90007610828 – Cod. Min.: PAIC84200X

☎ 091-954299 – Fax 091-9100217

Autorizzazione e istruzioni al trattamento dei dati personali docenti

Al personale docente Agli assistenti educativi

Ai docenti incaricati di attività integrative

Ai tirocinanti

Oggetto: Autorizzazione e linee guida per il trattamento e la protezione dei dati personali destinate al personale docente

IL DIRIGENTE SCOLASTICO

VISTO il Regolamento UE 2016/679 noto come "General Data Protection Regulation" (GDPR); VISTO il "Codice della Privacy" D.Lgs 196/2003 novellato dal D.Lgs. 101/2018;

VISTO il DM 305/2006;

Visto il Modello Organizzativo per la privacy e la protezione dei dati, adottato dall'Istituto;

PREMESSO CHE

- ai sensi dell'art. 4.7 del GDPR il Titolare del trattamento di dati personali è l'Istituto Scolastico stesso, di cui il dirigente scolastico è legale rappresentante pro tempore;
- in base al principio di responsabilizzazione (accountability) ex art. 5.2 e art. 25 del GDPR il Titolare deve definire le misure tecniche ed organizzative adeguate a ciascuna attività di trattamento dei dati personali ed impartire istruzioni a tutti coloro che sono stati autorizzati al trattamento dei dati personali (artt. 5, 24, 29 e 32);
- sono soggetti autorizzati al trattamento tutti i dipendenti dell'istituzione scolastica che trattano i dati personali;
- il Titolare del trattamento ha individuato un gruppo omogeneo di "autorizzati al trattamento di dati personali" nel personale docente ed educativo in servizio presso l'istituzione scolastica, per il quale il trattamento dei dati rientra

nelle competenze proprie del profilo professionale contrattualmente determinato ed è quindi obbligatorio il necessario per lo svolgimento delle proprie specifiche funzioni;

CONSIDERATO CHE

- l'autorizzazione al trattamento dei dati personali non implica l'attribuzione di funzioni ulteriori rispetto a quelle già assegnate, né compensi economici aggiuntivi, ma consente di trattare i dati di cui si viene a conoscenza nell'esercizio della mansione assegnata;
- la S.V., in servizio presso questo Istituto Scolastico, in qualità di docente (o, in alternativa, di assistente educativo, docente incaricato di attività integrative o tirocinante) ha necessità di effettuare attività di trattamento dei dati personali;

AUTORIZZA la S.V.

al trattamento dei dati personali detenuti da questa istituzione scolastica, come individuati nel seguito del presente documento, in riferimento al profilo di appartenenza della S.V.

Costituisce trattamento qualunque operazione, svolta con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati, necessari nel particolare per le seguenti attività:

- attività didattica e partecipazione agli organi collegiali;
- valutazione alunni;
- tenuta documenti e registri di attestazione delle valutazioni e di documentazione inerente alla vita scolastica dello studente, nonché delle relazioni tra scuola e famiglia quali ad esempio richieste, istanze e corrispondenza con le famiglie;
- rapporti con famiglie e alunni, anche in loro situazione di disabilità e/o disagio psicosociale;
- ricezione dei certificati medici relativi allo stato di salute degli alunni, documentazione alunni disabili, documentazione clinica per assunzione di farmaci, documentazione clinica relativa a intolleranze, documentazione clinica H, DSA e BES, limitatamente alle operazioni di trattamento strettamente indispensabili;
- raccolta di eventuali contributi e/o tasse scolastiche versate da alunni e genitori;
- adempimenti connessi alle visite guidate e ai viaggi di istruzione;
- adempimenti connessi alla realizzazione di progetti e di attività previste dal PTOF, comprese le eventuali attività di alternanza scuola lavoro e/o di orientamento in ingresso ed in uscita;

- conoscenza di dati relativi a professioni di fede religiosa e agli orientamenti sessuali degli alunni;
- eventuali adempimenti connessi all'attività amministrativa, quali ad esempio la registrazione delle presenze, attestazioni inerenti allo stato del personale, eccetera.

Il trattamento dovrà essere limitato alle operazioni necessarie ed indispensabili all'adempimento delle mansioni connesse al profilo della S.V., in osservanza delle norme di legge, dei regolamenti interni, delle circolari, degli ordini di servizio e delle istruzioni impartite dal titolare del trattamento e dei suoi delegati.

La S.V. effettuerà le operazioni sopra descritte nel rigoroso rispetto delle istruzioni operative che seguono.

MISURE OPERATIVE GENERICHE

Nello svolgimento delle sue mansioni, l'incaricato dovrà:

- accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni ed esclusivamente per scopi determinati, espliciti e legittimi, attraverso operazioni di trattamento compatibili con le finalità connesse all'attività svolta;
- trattare i dati personali secondo le modalità definite dalla normativa in vigore, in modo lecito e secondo correttezza con l'osservanza, in particolare, delle prescrizioni di cui al GDPR, al D.Lgs. 196 come novellato dal D.Lgs 101/2018 e dal D.M. 305/2006;
- verificare che i dati siano esatti e, se necessario, aggiornarli;
- verificare che i dati siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- conservare i dati in forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
- non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale;
- non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Titolare e, comunque, senza avere la certezza della loro identità;
- accertarsi che eventuali comunicazioni, anche verbali o telefoniche, agli interessati avvengano in forma riservata;
- non diffondere e comunicare dati personali trattati, a meno che ciò debba avvenire nello svolgimento dei compiti affidati ed autorizzati dal Titolare del trattamento. Si raccomanda particolare attenzione alla tutela del diritto alla riservatezza degli interessati (persone fisiche a cui afferiscono i dati personali);
- informare prontamente il Titolare o il Responsabile per la Protezione dei Dati dell'Istituto (DPO), di seguito indicato, di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi;

- non lasciare a disposizione di estranei documenti o supporti di memorizzazione (cd, dvd, pen drive) che contengono dati personali o sensibili;
- accertarsi della distruzione di documenti o fogli di stampa inutilizzati contenenti dati personali o sensibili;
- non fare uscire dalla sede scolastica documenti della scuola contenenti dati personali, né eventuali copie o riproduzioni, se non dietro espressa autorizzazione del Titolare del trattamento;
- non abbandonare la postazione di lavoro, senza aver provveduto a custodire in luogo sicuro i documenti contenenti dati personali;
- nel caso di utilizzo di registri cartacei, al termine delle attività didattiche giornaliere custodire il registro di classe nella relativa aula, in un luogo protetto dotato di serratura (armadio o cassetto della cattedra);
- relativamente ai dati particolari forniti dagli alunni e dalle famiglie e nell'espletamento delle attività connesse alla funzione docente, la S.V. effettuerà i trattamenti consentiti indicati nelle schede, allegate al D.M. 305/2006 n. 4 (attività propedeutiche all'inizio dell'anno scolastico), n. 5 (attività educativa, didattica e formativa, di valutazione) e n. 7 (rapporti scuola famiglie, gestione del contenzioso) per le finalità di rilevante interesse pubblico indicate e illimitatamente i tipi di dati alle operazioni che sono precisate sia come particolari forme di trattamento sia come altre tipologie più ricorrenti di trattamento.
- collaborare con il Responsabile per la Protezione dei Dati dell'Istituto (DPO), indicato nel seguito del documento, per aspetti specifici relativi ad ogni nuova attività che comporti il trattamento dei dati personali.

MISURE OPERATIVE SPECIFICHE ALL'UTILIZZO DI TECNOLOGIE INFORMATICHE

- scegliere per il registro informatico una password che sia composta da otto caratteri e non facilmente intuibile, evitando che contenga riferimenti alla propria persona (es. proprio nome o di congiunti, date di nascita, ecc.);
- curare la conservazione della propria password del registro informatico e non comunicarla per alcun motivo a soggetti terzi;
- cambiare periodicamente (almeno una volta ogni tre mesi) la propria password del registro informatico;
- adottare le stesse cautele di cui sopra per le password di qualsiasi altra piattaforma software ad uso personale e potenzialmente interessata al trattamento di dati personali (mail, account per piattaforme elearning, eccetera);
- effettuare il logoff dal Registro Informatico e, laddove presenti, da sistemi di autenticazione di rete al termine di ogni sessione di lavoro;
- spegnere correttamente il computer al termine di ogni sessione di lavoro al fine di agevolare, se utilizzati, l'azione di software specifici di congelamento delle configurazioni degli stessi;

- non abbandonare la propria postazione di lavoro per la pausa o altri motivi senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
- nella comunicazione multimediale con alunni e genitori utilizzare esclusivamente le piattaforme informatiche messe a disposizione dall'Istituto; è fatto divieto utilizzare social network quali Facebook o altri;
- nell'utilizzo della posta elettronica non aprire documenti di cui non sia certa la provenienza e controllare accuratamente l'indirizzo dei destinatari prima di inviare email contenenti in allegato o nel corpo del messaggio dati personali;
- rispettare rigorosamente le misure di sicurezza predisposte dall'istituzione scolastica relativamente all'utilizzo delle tecnologie informatiche di comunicazione telematica;
- nella comunicazione multimediale con alunni e genitori utilizzare esclusivamente le piattaforme informatiche messe a disposizione dall'istituto; è fatto divieto utilizzare social network quali facebook o altri;
- non diffondere via WEB (o altro strumento telematico) dati personali delle famiglie o di altri interessati a meno di quelli, pertinenti e minimi, inclusi negli atti da pubblicare a seguito di autorizzazione del Titolare del trattamento o del soggetto designato quale responsabile della pubblicazione WEB.

Gli obblighi sopra descritti fanno parte integrante della prestazione lavorativa e pertanto sono dovuti in base al vigente CCNL. Nel caso di inadempimento si applicheranno le sanzioni disciplinari previste dal vigente CCNL.

La presente autorizzazione ha efficacia fino alla risoluzione del rapporto di lavoro per qualsiasi causa oppure fino alla modifica o alla revoca da parte del Titolare del trattamento.

Riferimenti del DPO (Responsabile per la Protezione dei Dati) dell'Istituto NetSense S.r.l., con sede legale in via Novaluce 38, a Tremestieri Etneo (CT)

Partita IVA 04253850871,

email: info@netsenseweb.com PEC: netsense@pec.it,

nella persona dell'Ing. Renato Narcisi, PEC: renato.narcisi@arubapec.it

Il titolare del trattamento dei dati L'istituto nella persona di Giovanni Taibi

firma autografa sostituita da indicazione a mezzo stampa, ai sensi dell'art.3 D.Lgs. 39/199

Allegato 4 ePolicy - Autorizzazione e istruzioni al trattamento dei dati collaboratori scolastici



MINISTERO DELLA PUBBLICA ISTRUZIONE

Istituto Comprensivo Statale "Casteldaccia"

Istituto ad indirizzo musicale

Via Carlo Cattaneo N.80 – 90014 CASTELDACCIA (PA) C.F.: 90007610828 – Cod. Min.: PAIC84200X

☎ 091-954299 – Fax 091-9100217

Autorizzazione e istruzioni al trattamento dei dati collaboratori scolastici

Ai collaboratori scolastici

Oggetto: Autorizzazione e linee guida per il trattamento e la protezione dei dati personali destinate ai collaboratori scolastici

IL DIRIGENTE SCOLASTICO

VISTO il Regolamento UE 2016/679 noto come "General Data Protection Regulation" (GDPR);

VISTO

il "Codice della Privacy" D.Lgs 196/2003 novellato dal D.Lgs. 101/2018;

VISTO

il DM 305/2006;

VISTO

il Modello Organizzativo per la privacy e la protezione dei dati, adottato dall'Istituto;

PREMESSO CHE

- ai sensi dell'art. 4.7 del GDPR il Titolare del trattamento di dati personali è l'Istituto Scolastico stesso, di cui il dirigente scolastico è legale rappresentante pro tempore;
- in base al principio di responsabilizzazione (accountability) ex art. 5.2 e art. 25 del GDPR il Titolare deve definire le misure tecniche ed organizzative adeguate a ciascuna attività di trattamento dei dati personali ed impartire istruzioni a tutti coloro che sono stati autorizzati al trattamento dei dati personali (artt. 5, 24, 29 e 32);
- sono soggetti autorizzati al trattamento tutti i dipendenti dell'istituzione scolastica che trattano i dati personali;

- il Titolare del trattamento ha individuato un gruppo omogeneo di “autorizzati al trattamento di dati personali” negli collaboratori scolastici in servizio presso l’istituzione scolastica, per il quale il trattamento dei dati è obbligatorio il necessario per lo svolgimento delle proprie specifiche funzioni;

CONSIDERATO CHE

- l’autorizzazione al trattamento dei dati personali non implica l’attribuzione di funzioni ulteriori rispetto a quelle già assegnate, né compensi economici aggiuntivi, ma consente di trattare i dati di cui si viene a conoscenza nell’esercizio della mansione assegnata;
- la S.V., in servizio presso questo Istituto Scolastico e in riferimento ai compiti svolti e alle mansioni assegnate ha necessità di effettuare autori atti ità di trattamento dei dati personali;

AUTORIZZA la S.V.

al trattamento dei dati personali detenuti da questa istituzione scolastica, come individuati nel seguito del presente documento, in riferimento al profilo di appartenenza della S.V.

Costituisce trattamento qualunque operazione, svolta con o senza l’ausilio di mezzi elettronici o comunque automatizzati, concernente la raccolta, la registrazione, l’organizzazione, la conservazione, l’elaborazione, la modificazione, la selezione, l’estrazione, il raffronto, l’utilizzo, l’interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati, necessari nel particolare per le seguenti attività:

- accesso ad archivi cartacei, fascicoli personali degli alunni, del personale ATA e dei Docenti;
- adempimenti connessi alle uscite anticipate degli alunni;
- rapporti con le famiglie, siano essi in presenza che telefonici.

Il trattamento dovrà essere limitato alle operazioni necessarie ed indispensabili all’adempimento delle mansioni connesse al profilo della S.V., in osservanza delle norme di legge, dei regolamenti interni, delle circolari, degli ordini di servizio e delle istruzioni impartite dal titolare del trattamento e dei suoi delegati.

La S.V. effettuerà le operazioni sopra descritte nel rigoroso rispetto delle istruzioni operative che seguono.

MISURE OPERATIVE

Nello svolgimento delle sue mansioni, l’incaricato dovrà:

- trattare i dati personali in modo lecito e secondo correttezza, per scopi determinati e legittimi;
- verificare che siano esatti e, se necessario, indicare al personale amministrativo di aggiornarli;
- comunicare o eventualmente diffondere o trasferire all’esterno i dati personali esclusivamente ai soggetti autorizzati e riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute;

- non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale.;
- informare prontamente il titolare o il responsabile per la protezione dei dati dell'istituto (DPO), indicato nel seguito del documento, di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi;
- accertarsi dell'identità degli interessati e della loro autorizzazione al trattamento e dell'eventuale autorizzazione scritta a terzi, al momento del ritiro di documentazione in uscita;
- non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del titolare e senza avere la certezza della loro identità;
- relazionarsi e collaborare con gli altri incaricati del trattamento dei dati, attenendosi alle indicazioni fornite e provvedendo, a propria volta, a dare indicazioni esaustive in caso di coinvolgimento di altri incaricati nei trattamenti effettuati;
- rispettare il divieto assoluto di divulgazione in qualunque forma o modalità, analogica o digitale, dei dati trattati nel corso del presente incarico, anche per il tempo successivo alla sua cessazione, senza limiti temporali;
- partecipare agli interventi formativi organizzati dall'istituzione scolastica sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle attività connesse alle sue mansioni;
- collaborare con il Responsabile per la Protezione dei Dati dell'Istituto, indicato nel seguito del documento, per aspetti specifici relativi a nuove attività che comportano trattamento dei dati personali;

Qualunque violazione delle modalità sopra indicate dà luogo a precise responsabilità, ai sensi delle normative vigenti.

Riferimenti del DPO (Responsabile per la Protezione dei Dati) dell'Istituto NetSense S.r.l., con sede legale in via Novaluce 38, a Tremestieri Etneo (CT)

Partita IVA 04253850871,

email: info@netsenseweb.com PEC: netsense@pec.it,

nella persona dell'Ing. Renato Narcisi, PEC: renato.narcisi@arubapec.it

Il titolare del trattamento dei dati L'istituto

nella persona di Giovanni Taibi

firma autografa sostituita da indicazione

a mezzo stampa, ai sensi dell'art.3 D.Lgs. 39/1993

Allegato 5 ePolicy - Autorizzazione e istruzioni al trattamento dei dati personale tecnico e animatore digitale



MINISTERO DELLA PUBBLICA ISTRUZIONE

Istituto Comprensivo Statale "Casteldaccia"

Istituto ad indirizzo musicale

Via Carlo Cattaneo N.80 – 90014 CASTELDACCIA (PA) C.F.: 90007610828 – Cod. Min.: PAIC84200X

☎ 091-954299 – Fax 091-9100217

Autorizzazione e istruzioni al trattamento dei dati personale tecnico e animatore digitale

All'animatore digitale / personale tecnico

Oggetto: Autorizzazione e linee guida per il trattamento e la protezione dei dati personali destinate al personale tecnico e/o all'animatore digitale

IL DIRIGENTE SCOLASTICO

VISTO

il Regolamento UE 2016/679 noto come "General Data Protection Regulation" (GDPR); VISTO il "Codice della Privacy" D.Lgs 196/2003 novellato dal D.Lgs. 101/2018;

VISTO

il DM 305/2006;

VISTO

il Modello Organizzativo per la privacy e la protezione dei dati, adottato dall'Istituto;

PREMESSO CHE

- ai sensi dell'art. 4.7 del GDPR il Titolare del trattamento di dati personali è l'Istituto Scolastico stesso, di cui il dirigente scolastico è legale rappresentante pro tempore;
- in base al principio di responsabilizzazione (accountability) ex art. 5.2 e art. 25 del GDPR il Titolare deve definire le misure tecniche ed organizzative adeguate a ciascuna attività di trattamento dei dati personali ed impartire istruzioni a tutti coloro che sono stati autorizzati al trattamento dei dati personali (artt. 5, 24, 29 e 32);
- sono soggetti autorizzati al trattamento tutti i dipendenti dell'istituzione scolastica che trattano i dati personali;

CONSIDERATO CHE

- l'autorizzazione al trattamento dei dati personali non implica l'attribuzione di funzioni ulteriori rispetto a quelle già assegnate, né compensi economici aggiuntivi, ma consente di trattare i dati di cui si viene a conoscenza nell'esercizio della mansione assegnata;
- la S.V., in servizio presso questo Istituto Scolastico e in riferimento ai compiti svolti e alle mansioni assegnate ha necessità di effettuare attività di trattamento dei dati personali;

AUTORIZZA la S.V.

al trattamento dei dati personali detenuti da questa istituzione scolastica, come individuati nel seguito del presente documento, in riferimento al profilo di appartenenza della S.V.

Costituisce trattamento qualunque operazione, svolta con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati, necessari nel particolare per le seguenti attività:

- supporto tecnico ai sistemi informatici di segreteria;
- supporto tecnico ai sistemi informatici d'aula;
- supporto tecnico ai sistemi informatici di laboratorio;
- supporto tecnico ai sistemi informatici a supporto delle attività DAD e DDI;
- supporto tecnico alla rete dati di istituto.

Il trattamento dovrà essere limitato alle operazioni necessarie ed indispensabili all'adempimento delle mansioni connesse al profilo della S.V., in osservanza delle norme di legge, dei regolamenti interni, delle circolari, degli ordini di servizio e delle istruzioni impartite dal titolare del trattamento e dei suoi delegati.

La S.V. effettuerà le operazioni sopra descritte nel rigoroso rispetto delle istruzioni operative che seguono.

MISURE OPERATIVE GENERICHE

Nello svolgimento delle sue mansioni, l'incaricato dovrà:

- accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni;
- trattare i dati personali in modo lecito e secondo correttezza;
- raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi, ed utilizzarli solo per operazioni di trattamento compatibili con le finalità connesse all'attività svolta;
- verificare che i dati siano esatti e, se necessario, aggiornarli;
- verificare che i dati siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- conservare i dati in forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
- non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale;
- informare prontamente il Titolare o il Responsabile per la Protezione dei Dati dell'Istituto (RPD), di seguito indicato, di ogni circostanza idonea a determinare pericolo di dispersione o utilizzo non autorizzato dei dati stessi;
- non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Titolare e, comunque, senza avere la certezza della loro identità;
- non lasciare a disposizione di estranei documenti o supporti di memorizzazione (cd, dvd, pen drive) che contengano dati personali o sensibili;
- accertarsi della distruzione di documenti inutilizzati contenenti dati personali o sensibili;
- non abbandonare la postazione di lavoro, senza aver provveduto a custodire in luogo sicuro i documenti contenenti dati personali;
- nel caso di utilizzo di registri cartacei, al termine delle attività didattiche giornaliere custodire il registro di classe nella relativa aula, in un luogo protetto dotato di serratura (armadio o cassetto della cattedra);
- collaborare con il Responsabile per la Protezione dei Dati dell'Istituto (DPO), indicato nel seguito, per aspetti specifici relativi ad ogni nuova attività che comporti il trattamento dei dati personali.

Misure operative specifiche all'utilizzo di tecnologie informatiche

- nel caso fosse necessario travasare il contenuto delle memorie di massa dei PC in manutenzione, non utilizzare supporti che non siano di proprietà dell'Istituto. Gli stessi supporti dovranno essere custoditi con cura prima del travaso inverso. Una volta verificato il corretto ripristino del funzionamento del PC/sistema in manutenzione, deve essere prontamente effettuata la formattazione del supporto di travaso;
- curare la conservazione della password di amministrazione di PC, Notebook, NAS e non comunicarla per alcun motivo a soggetti terzi;
- curare la conservazione della password di congelamento dei PC (ove tale software è utilizzato) al fine di ridurre la possibilità di immagazzinamento di dati personali negli stessi;
- accertarsi di congelare nuovamente (ove tale software sia utilizzato) la configurazione del pc dopo ogni attività di manutenzione;
- nell'utilizzo della posta elettronica non aprire documenti di cui non sia certa la provenienza e controllare accuratamente l'indirizzo dei destinatari prima di inviare email contenenti in allegato o nel corpo del messaggio dati personali;
- adottare le stesse cautele di cui sopra per le password di qualsiasi altra piattaforma software ad uso personale e potenzialmente interessata al Trattamento di Dati Personali (mail, account per piattaforme terze, eccetera);
- effettuare il logout da qualsiasi software che preveda la fase di login e, laddove presenti, da sistemi di autenticazione di rete al termine di ogni sessione di lavoro;
- spegnere correttamente il computer al termine di ogni sessione di lavoro al fine di agevolare, se utilizzati, l'azione di software specifici di congelamento delle configurazioni degli stessi;
- non abbandonare la propria postazione di lavoro per la pausa o altri motivi senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
- nell'esercizio delle proprie mansioni mantenere scrupolosamente le misure minime di sicurezza ICT adottate dall'Istituto sulla base delle richieste effettuate dall'AGID;

Qualunque violazione delle modalità sopra indicate dà luogo a precise responsabilità, ai sensi delle normative vigenti.

Riferimenti del DPO (Responsabile per la Protezione dei Dati) dell'Istituto NetSense S.r.l., con sede legale in via Novaluce 38, a Tremestieri Etneo (CT)

Partita IVA 04253850871,

email: info@netsenseweb.com PEC: netsense@pec.it,

nella persona dell'Ing. Renato Narcisi, PEC: renato.narcisi@arubapec.it

Il titolare del trattamento dei dati L'istituto
nella persona di Giovanni Taibi

firma autografa sostituita da indicazione

a mezzo stampa, ai sensi dell'art.3 D.Lgs. 39/1993

Allegato 6 ePolicy - Informativa per il trattamento dei dati personali – alunni e loro famiglie



MINISTERO DELLA PUBBLICA ISTRUZIONE

Istituto Comprensivo Statale “Casteldaccia”

Istituto ad indirizzo musicale

Via Carlo Cattaneo N.80 – 90014 CASTELDACCIA (PA) C.F.: 90007610828 – Cod. Min.: PAIC84200X

☎ 091-954299 – Fax 091-9100217

Informativa per il trattamento dei dati personali – alunni e loro famiglie

ex artt. 13 e 14 Regolamento UE 2016/679 ("GDPR")

Gentile Signore/a,

con la presente desideriamo informarla che il Regolamento Europeo 2016/679 (GDPR), nel seguito indicato sinteticamente come Regolamento), ed il Decreto Legislativo n. 196/2003 modificato dal D.Lgs. 101/2018 (nel seguito indicato sinteticamente come Codice), impongono che ogni trattamento dei dati personali dei componenti della sua famiglia sia effettuato osservando severe regole organizzative e tecniche.

Con il termine trattamento dei dati si intende “qualsiasi operazione [...] come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione”.

Di seguito le forniamo maggiori dettagli relativi ai trattamenti dei suoi dati che l'Istituto effettuerà, sottolineando sin da ora che essi saranno improntati ai principi di liceità, correttezza e trasparenza ed effettuati attraverso l'adozione di misure tecniche ed organizzative opportunamente identificate al fine di garantire ai suoi dati riservatezza, correttezza ed integrità e a lei il pieno esercizio dei suoi diritti.

Dati del Titolare e del Responsabile per la Protezione dei Dati (DPO)

Il titolare del trattamento, nel seguito indicato sinteticamente come Titolare, è:

l'Istituto / La Scuola {Denominazione},

con sede legale in {Via}, a {Citta}, provincia di {Provincia},

telefono {Telefono}, codice fiscale {Partita_iva}, codice meccanografico {Meccanografico},

email {Peo}, PEC {Pec},

rappresentato dal Dirigente Scolastico {Dirigente}.

Il Responsabile per la Protezione dei Dati, nel seguito indicato sinteticamente come DPO, è:

NetSense S.r.l. nella persona dell'ing. Renato Narcisi,

con sede legale in via Novaluce 38, a Tremestieri Etneo (CT),

Partita IVA 04253850871,

email aziendale: info@netsenseweb.com, PEC aziendale: netsense@pec.it

INDICE DEL DOCUMENTO:

- 1 Finalità e base giuridica dei trattamenti
- 2 Elenco dei trattamenti effettuati dal Titolare
 - 2.1 Iscrizioni - Fase di acquisizione e gestione delle domande online e cartacee
 - 2.2 Iscrizioni - Fase di acquisizione documentazione aggiuntiva prima dell'avvio del primo anno
 - 2.3 Gestione amministrativa dello studente
 - 2.4 Gestione amministrativa specifica per studenti con disabilità
 - 2.5 Fruizione del servizio di pagamento PagoPA
 - 2.6 Gestione didattica dello studente
 - 2.7 Utilizzo di piattaforme digitali per la didattica
 - 2.8 Trattamenti effettuati da operatori per conto di titolari esterni (soggetti pubblici)
 - 2.9 Gestione foto, immagini e video
 - 2.10 Attività di orientamento, formazione e inserimento professionale
 - 2.11 Viaggi di istruzione, progetti Erasmus ed altri viaggi
 - 2.12 INVALSI - rilevazione del livello di apprendimento
 - 2.13 INVALSI - analisi di contesto
 - 2.14 Utilizzo della rete dati ed Internet (firewall e autenticazione di rete)
 - 2.15 Gestione di eventuali impianti di videosorveglianza
- 3 Provenienza dei dati, soggetti titolati per conto del titolare, modalità e tempi dei trattamenti
- 4 Comunicazione e diffusione dei dati: categorie di destinatari e modalità
- 5 Trasferimento dati verso un paese terzo e/o un'organizzazione internazionale
- 6 Natura del conferimento e conseguenze del rifiuto di rispondere

7 Diritti dell'interessato e modalità di esercizio

8 Riferimenti normativi

Finalità e base giuridica dei trattamenti

Il Titolare, in funzione delle attività che è chiamato a svolgere, effettua molteplici trattamenti di un'ampia categoria di dati personali, compresi quelli appartenenti a categorie particolari (di seguito definiti per brevità "dati particolari"): dati sulla salute, dati giudiziari, dati che rivelano l'origine razziale o etnica, le convinzioni religiose e la vita e l'orientamento sessuale.

Finalità dei trattamenti: tutti i trattamenti dei dati sono effettuati dal Titolare per l'esecuzione di un compito di interesse pubblico o comunque connesso all'esercizio di pubblici poteri. In particolare, i trattamenti di categorie particolari di dati personali sono effettuati solo ove necessario per motivi di interesse pubblico rilevante e, comunque, ove siano previsti da disposizioni di legge (o di regolamento, in tutti quei casi previsti dalla legge) che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Base giuridica dei trattamenti: la base giuridica per ogni trattamento è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento. Pertanto il suo consenso esplicito non è richiesto; valgono, ovviamente, i suoi diritti elencati nella apposita sezione del presente documento.

Elenco dei trattamenti effettuati dal Titolare

L'elenco seguente riporta i trattamenti dei dati personali e particolari effettuati dal Titolare.

Iscrizioni - Fase di acquisizione e gestione delle domande online e cartacee

Durante la fase di iscrizione, tipicamente condotta all'inizio di ogni anno solare, si effettua un trattamento fine alla raccolta delle domande di iscrizione presentate online o in modalità cartacea e alla gestione delle iscrizioni per l'accoglimento della domanda. I dati trattati sono i seguenti:

DATI COMUNI: Dati anagrafici e relativi alla composizione familiare; Dati inerenti situazioni giudiziarie civili, amministrative, tributarie.

Iscrizioni - Fase di acquisizione documentazione aggiuntiva prima dell'avvio del primo anno

La fase di iscrizione si perfeziona solitamente qualche settimana prima dell'inizio di ogni anno scolastico. Durante questa fase si effettua un trattamento fine alla raccolta della documentazione necessaria per il completamento dell'iscrizione e per la successiva gestione dei servizi rivolti all'alunno. I dati trattati sono quelli indicati nel paragrafo precedente, ai quali si potranno aggiungere le seguenti

CATEGORIE PARTICOLARI DI DATI PERSONALI: Dati sulla salute, dati che rivelano l'origine razziale o etnica, le convinzioni religiose e la vita e l'orientamento sessuale.

DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI: Condizione di indagato/imputato o altre situazioni giudiziarie; Sottoposizione a misure detentive carcerarie.

Gestione amministrativa dello studente

La gestione amministrativa dell'alunno in seno all'ordinamento dell'Istituto comporta, nel tempo, molteplici trattamenti fini all'aggiornamento continuo delle informazioni già raccolte nella fase di iscrizione (ad esempio, l'aggiornamento della situazione anagrafica delle famiglie, della sua composizione, delle situazioni giudiziarie che la coinvolgono, dello stato di salute di alcuni dei suoi membri, eccetera).

È necessario porre alla sua attenzione il fatto che l'istituto alimenta e aggiorna continuamente l'Anagrafe Nazionale degli

Studenti, ospitata dalla piattaforma SIDI e gestita in titolarità dal Ministero dell'Istruzione.

I dati trattati durante la gestione amministrativa dello studente negli anni sono i seguenti:

DATI COMUNI: Dati anagrafici; Dati inerenti situazioni giudiziarie civili, amministrative, tributarie.

CATEGORIE PARTICOLARI DI DATI PERSONALI: Dati sulla salute, dati che rivelano l'origine razziale o etnica, le convinzioni religiose e la vita e l'orientamento sessuale.

DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI: Condizione di indagato/imputato o altre situazioni giudiziarie (condanne penali e reati o connesse misure di sicurezza); Sottoposizione a misure detentive carcerarie.

In seno alle attività di gestione amministrativa dello studente, i dati personali e particolari della sua famiglia potranno essere comunicati a soggetti pubblici (quali, ad esempio, ASL, Comune, Provincia, Ufficio scolastico regionale, Ambiti Territoriali, organi di polizia giudiziaria, organi di polizia tributaria, guardia di finanza, magistratura, ministeri) e a membri di organi collegiali per svolgere attività istituzionali previste dalle vigenti disposizioni in materia sanitaria, previdenziale, tributaria, giudiziaria e di istruzione (RifLeg. 5). In questi casi tali soggetti agiranno in base al loro ruolo di autonomi titolari.

I dati personali dei componenti della sua famiglia potranno essere, inoltre, comunicati a soggetti privati che, nel loro ruolo di autonomi titolari, forniscono servizi all'istituzione scolastica quali, ad esempio, imprese di assicurazione (in relazione a polizze in materia infortunistica) e agenzie di viaggio.

Gestione amministrativa specifica per studenti con disabilità

Gli studenti con disabilità necessitano di procedure amministrative atte a garantire tutte le tutele necessarie al soggetto interessato. Tali procedure coinvolgono una serie di trattamenti dei dati fini all'assegnazione degli insegnanti di sostegno, al mantenimento del fascicolo disabile cartaceo, alla creazione e al mantenimento della "partizione alunni disabili" della Anagrafe Nazionale degli Studenti (secondo quanto disposto dal Decreto MIUR 162 del 28 Luglio 2016 e successive circolari al riguardo). A tal riguardo, si informa gli interessati che su istanza dei genitori presentata al fine di ottenere l'assegnazione dell'insegnante di sostegno, i dati di salute di alunni affetti da gravi patologie o disabilità sono trasmessi per mail in forma cifrata agli uffici competenti e per via telematica ad una partizione specifica della banca dati denominata "Anagrafe Nazionale degli Studenti". Da questa partizione accederà, in sola lettura e in forma anonima, il personale autorizzato dagli Enti preposti all'erogazione del servizio.

I dati trattati sono i seguenti:

DATI COMUNI: Piano Educativo Individuale.

CATEGORIE PARTICOLARI DI DATI PERSONALI: rispetto a quelli elencati al punto precedente vi è la conoscenza dei dati di salute relativi a disabilità, anche in riferimento alla legge 104/92.

Fruizione del servizio di pagamento PagoPA

In ottemperanza a quanto previsto dalla vigente normativa, dal 01 marzo 2021 l'uso di PagoPA diventa obbligatorio per i pagamenti verso la Pubblica Amministrazione, per ogni tipologia di incasso.

Al fine di agevolare l'utenza, l'Istituto utilizza sistemi gestionali che consentono i pagamenti dei contributi scolastici (tasse scolastiche, viaggi d'istruzione, ecc.), attraverso bollettini di pagamento associati agli studenti. Tali sistemi possono essere integrati nei gestionali già utilizzati dall'Istituto (ad esempio: Argo, Axios, Spaggiari, Nuvola, ecc.) o, in alternativa, possono essere forniti dal Ministero dell'Istruzione (è questo il caso del servizio "Pago In rete").

Solo nel caso di "Pago in rete" fornito dal Ministero, il quale agisce quale titolare del trattamento autonomo per tutti i trattamenti effettuati in seno alla piattaforma informatica, nasce la necessità di associare direttamente nel portale ministeriale il codice fiscale di uno dei genitori o di un tutore a quello dell'alunno/a pagatore e, dunque, consentire i

pagamenti richiesti. Una ulteriore opzione del sistema ministeriale potrà consentire al rappresentante di classe, al solo fine di fornirle supporto nella gestione del servizio, di effettuare e verificare per suo conto i pagamenti degli avvisi telematici intestati all'alunno/a. Quest'ultima opzione sarà attivabile a sua esplicita richiesta.

Gestione didattica dello studente

La gestione del percorso formativo e didattico dell'alunno/a in seno alle attività indicate dall'istituto nel PTOF comporta il trattamento dei dati di valutazione degli studenti. I dati relativi al progresso formativo degli alunni sono memorizzati nel registro elettronico, gestito da un Responsabile del Trattamento (RdT) nelle modalità descritte nel seguito del documento. Una parte di tali dati sarà anche visibile alle famiglie, in relazione ai diversi livelli di visibilità (riservata / per classe / bacheca scolastica).

I dati relativi agli esiti scolastici degli alunni saranno pubblicati mediante affissione all'albo della scuola, nei limiti delle vigenti disposizioni in materia.

Riteniamo utile informarla che durante particolari attività didattiche potranno essere realizzati video o immagini che riprendono gli alunni, al solo scopo di documentare le attività didattiche. Tale trattamento avviene nelle modalità descritte nel seguito del documento, al paragrafo "Gestione foto, immagini e video".

DATI COMUNI: Dati anagrafici; Dati audio/foto/video; Dati di valutazione e scoring (*).

CATEGORIE PARTICOLARI DI DATI PERSONALI: Dati sulla salute, dati che rivelano l'origine razziale o etnica, le convinzioni religiose e la vita e l'orientamento sessuale.

Utilizzo di piattaforme digitali per la didattica

Ai sensi della normativa vigente l'istituto intende adottare strumenti informatici adatti a fruire di servizi di scambio di materiali didattici, videoconferenza ed interazione in tempo reale attraverso condivisione di audio e video in modalità peer-to-peer quale supporto digitale alle attività didattiche. Ciò al duplice fine di avviare innovative metodologie didattiche innovative da affiancare a quelle consuete, e di garantire livelli di istruzione adeguati anche in situazioni di didattica domiciliare o ospedaliera.

Le modalità di trattamento includono:

- la condivisione da parte del docente per via telematica, agli alunni del gruppo classe, di materiale didattico (file, documentazioni, ecc.) e delle registrazioni audio/video delle lezioni;
- l'acquisizione per via telematica, da parte del docente, degli elaborati degli alunni;
- la videoconferenza online attraverso piattaforme che permettono, tra l'altro, agli studenti l'isolamento del proprio audio e/o video alla bisogna o in base alle loro specifiche necessità.

Sono escluse sessioni in videoconferenza in modalità privata, a meno di casi di lezioni già originariamente previste in forma individuale (ad esempio, lezioni di musica, lezioni previste dai Piani Educativi Individualizzati o lezioni per Alunni con DSA e con bisogni educativi speciali non certificati);

Le uniche comunicazioni dei dati anagrafici identificativi degli alunni e dei loro dati di contatto (email o "id" di programmi di messaggistica) saranno effettuate all'interno del gruppo classe al quale partecipano esclusivamente gli alunni (e le famiglie) della stessa.

Gli interessati sono pregati di dare lettura alle condizioni d'uso delle piattaforme utilizzate, con ogni conseguenza in termini di consapevolezza del trattamento.

Trattamenti effettuati da operatori per conto di titolari esterni (soggetti pubblici)

Non è escluso che soggetti pubblici (quali, ad esempio, ASL, Comune, Provincia, Ufficio scolastico regionale, Ambiti Territoriali, organi di polizia giudiziaria, organi di polizia tributaria, guardia di finanza, magistratura, ministeri), nell'esecuzione del loro compito di interesse pubblico o comunque connesso all'esercizio di pubblici poteri, richiedano l'accesso di loro addetti al trattamento o di loro responsabili del trattamento nei locali della scuola. È il caso, ad esempio, degli operatori socio sanitari (OSS) o dei tirocinanti.

In questi casi i soggetti di cui sopra operano quali titolari del trattamento autonomi.

L'istituto si impegna, ove ritenesse necessario, a fornire alle famiglie ulteriori informazioni riguardo le attività che saranno effettuate. Nel caso necessitasse di ulteriori dettagli, l'interessato dovrà considerare di rivolgersi direttamente al titolare di riferimento.

Gestione foto, immagini e video

Durante particolari attività (progetti / gite / recite / saggi) potranno essere realizzati video o immagini che riprendono gli alunni, allo scopo di documentarne i momenti didattici più significativi. In nessun caso tali immagini, qualora i ragazzi fossero riconoscibili, saranno oggetto di diffusione, né telematica né con qualsiasi altro mezzo. Immagini e Video potranno, invece, essere consegnati esclusivamente ai genitori/tutori direttamente interessati alle attività didattiche. Alla realizzazione di video o immagini nelle modalità sopra indicate lei potrà esercitare il diritto di opposizione citato nel seguito del documento, utilizzando l'apposito modulo pubblicato nell'area privacy dell'Istituto.

I risultati delle attività di cui sopra potranno essere disseminati attraverso la pubblicazione sul sito WEB dell'istituto o su altri canali telematici. In tutti questi casi, gli alunni saranno ripresi di spalle o in esposizioni che non consentiranno la loro identificazione, neanche con tecniche informatiche di riconoscimento facciale. A tale scopo, saranno utilizzate anche tecniche di pixelizzazione o sfocatura delle immagini.

Infine, durante particolari eventi organizzati dall'Istituto potranno essere realizzati video o immagini che riprendono gli alunni da parte di soggetti terzi quali TV / testate giornalistiche / fotografi, che agiranno quali titolari autonomi del trattamento, fornendole proprie informative ed eventuali liberatorie.

Attività di orientamento, formazione e inserimento professionale

Su istanza degli interessati (presentata al fine di agevolare l'orientamento, la formazione e l'inserimento professionale anche all'estero dell'alunno) il Titolare comunicherà o diffonderà, anche a soggetti privati e per via telematica, dati relativi agli esiti formativi, intermedi e finali, degli studenti, nonché il loro nome, cognome, data di nascita ed indirizzo mail o altro recapito indicato dall'interessato nell'istanza di richiesta.

I soggetti destinatari agiranno in quanto autonomi titolari.

Viaggi di istruzione, progetti Erasmus ed altri viaggi

Su istanza degli interessati (presentata al fine di far partecipare l'alunno a viaggi di istruzione, a progetti ERASMUS o ad altre uscite didattiche e la cui organizzazione rende necessaria la conoscenza di alcune informazioni inerenti l'interessato) alcuni dati personali e particolari degli alunni saranno comunicati alle agenzie di viaggio e all'eventuale organizzazione ospitante, sia essa un istituto scolastico, accademico o altro soggetto giuridico; tali soggetti agiranno in qualità di Titolari autonomi del trattamento dei dati personali. Più specificamente i dati oggetto di tali specifici trattamenti sono: nome, cognome, data di nascita, codice fiscale, dati sulla salute (nel caso della presenza di situazioni di disabilità o che necessitano di assistenza particolare) e dati sulle preferenze religiose (direttamente, nel caso di visite in luoghi di culto, o indirettamente, nel caso di indicazione di esigenze alimentari).

Durante questi eventi i dati saranno trattati anche dalle unità di personale interno all'istituto incaricate di gestire il viaggio; tali unità di personale sono regolarmente istruite come "addetti al trattamento", secondo quanto previsto dal Regolamento.

In riferimento alle immagini e video prodotti in seno al viaggio o al progetto, valgono le indicazioni già sopra specificate, e cioè che non saranno diffuse foto o immagini che ritraggono gli alunni in maniera da renderli riconoscibili. Gli addetti al trattamento potranno ritrarre gli alunni, in linea con le indicazioni e le linee guida del “Garante per la Protezione dei Dati Personali” (cioè in atteggiamento positivo e con un chiaro riferimento alle attività progettuali e didattiche) al solo scopo di consegnare ai genitori alcune foto e video ricordo che saranno immediatamente eliminati dai sistemi informatici del Titolare.

INVALSI - rilevazione del livello di apprendimento

L'ente Invalsi effettua annualmente attività di rilevazione del livello di apprendimento degli alunni, sia nelle scuole statali che in quelle paritarie. Per tali trattamenti tale ente agisce quale titolare autonomo e fornisce agli interessati una propria informativa relativa al trattamento dei dati personali.

Le prove sono somministrate dagli insegnanti di classe o da altro docente appositamente incaricato in modalità cartacea o in modalità elettronica (computer based). In ciascuno dei due casi le informazioni sono raccolte in forma pseudonimizzata. Durante la somministrazione delle prove sono applicate le doverose misure di sicurezza, sia organizzative che tecniche.

L'istituto si impegna a pubblicare prontamente l'informativa Invalsi nell'area “Privacy” del proprio sito WEB e a fornire alle famiglie informazioni dettagliate riguardo le attività che saranno effettuate. Nel caso necessitasse di ulteriori dettagli, l'interessato dovrà considerare di rivolgersi direttamente al titolare di riferimento.

INVALSI - analisi di contesto

L'ente Invalsi effettua annualmente attività di rilevazione della situazione di contesto socio-economico nel quale l'Istituto opera. Per tali trattamenti tale ente agisce quale titolare autonomo e fornisce agli interessati una propria informativa relativa al trattamento dei dati personali.

I questionari, la cui compilazione è facoltativa, sono somministrati dagli insegnanti di classe o da altro personale appositamente incaricato, in modalità cartacea e pseudonimizzata. I questionari sono prontamente trascritti da personale amministrativo autorizzato in piattaforme informatiche INVALSI e successivamente distrutti.

L'istituto si impegna a pubblicare prontamente l'informativa Invalsi nell'area “Privacy” del proprio sito WEB e a fornire alle famiglie informazioni dettagliate riguardo le attività che saranno effettuate. Nel caso necessitasse di ulteriori dettagli, l'interessato dovrà considerare di rivolgersi direttamente al titolare di riferimento.

Utilizzo della rete dati ed Internet (firewall e autenticazione di rete)

Durante le attività didattiche si fa uso di risorse presenti in Internet e della piattaforma DAD istituzionale scelta dall'istituto (si faccia riferimento al paragrafo dedicato alle attività DAD / DDI / FAD per maggiori dettagli).

Si ritiene utile e doveroso informarla che agli alunni non sarà richiesta o permessa l'attivazione di qualsivoglia account che non sia esclusivamente quello relativo alla piattaforma istituzionale e che l'utilizzo della rete dati avviene in totale sicurezza, grazie al mantenimento degli standard previsti da AGID “Misure minime di sicurezza ICT per le PA” e all'utilizzo di opportuni firewall che impediscono l'uso della rete agli alunni se non sotto la supervisione del personale docente.

I dati trattati durante tali attività sono quelli derivanti da tracciamenti (log) delle attività di navigazione e a disposizione esclusivamente delle autorità giudiziarie nel caso di loro esplicita richiesta.

Gestione di eventuali impianti di videosorveglianza

L'Istituto potrà attivare, presso i propri plessi, degli impianti di videosorveglianza realizzati e gestiti al solo fine di garantire la sicurezza del patrimonio scolastico. Tali impianti, dotati di telecamere di ripresa video (la cui dislocazione e raggio di azione è disponibile in planimetria su richiesta), permette la visione delle immagini in tempo reale (“live”) e la registrazione delle immagini.

Ogni impianto di videosorveglianza, eventualmente realizzato, è in funzione esclusivamente negli orari di chiusura dell'Istituto, a meno delle telecamere esterne le quali, riprendendo aree perimetrali dell'edificio, potrebbero essere attivate anche in orari pomeridiani.

La visualizzazione delle immagini riprese attraverso l'impianto di videosorveglianza avviene solo ad opera del titolare o di persone da questi appositamente incaricate per iscritto. I dati sono conservati per la durata massima di 24 ore, fatta eccezione per i giorni festivi e le chiusure aziendali in genere, con successiva cancellazione automatica.

I dati di natura personale forniti potranno essere comunicati a destinatari, nominati ex art. 28 del Reg. UE 2016/679, che tratteranno i dati in qualità di responsabili e/o in qualità di persone fisiche che agiscono sotto l'autorità del Titolare e del Responsabile, al fine di ottemperare ai contratti o finalità connesse. Più specificamente, i dati potranno essere comunicati a soggetti esterni incaricati alla gestione/ manutenzione/ amministrazione dell'impianto di videosorveglianza e a pubblici ufficiali e/o autorità giudiziarie, in caso di loro esplicita richiesta.

Provenienza dei dati, soggetti titolati per conto del titolare, modalità e tempi dei trattamenti

A) Provenienza dei dati

I dati personali dell'alunno e dei familiari sono acquisiti direttamente dall'alunno stesso, dai genitori o dalla scuola di provenienza nel caso dei trasferimenti. In casi sporadici alcuni dati possono essere acquisiti da soggetti pubblici con i quali l'Istituto collabora secondo quanto disposto da specifiche norme di legge o di regolamento.

B) Soggetti titolati al trattamento per conto del Titolare

I trattamenti dei dati per conto del Titolare sono effettuati dal personale della scuola nella loro qualità di addetti autorizzati al trattamento (docenti, collaboratori scolastici, assistenti amministrativi e tecnici e il direttore amministrativo). Ogni addetto al trattamento è debitamente istruito.

È anche previsto che i trattamenti dei dati per conto del Titolare possano essere effettuati da soggetti esterni contrattualizzati dall'Istituto per l'esecuzione di particolari compiti. In questi casi i soggetti esterni sono espressamente nominati quale "responsabili del trattamento" e limiteranno il trattamento dei dati alle sole finalità indicate negli accordi contrattuali; è prevista la riconsegna di tutti i dati da parte di ogni responsabile del trattamento all'Istituto all'esaurimento delle finalità contrattuali, fatte salve specifiche disposizioni di legge.

C) Modalità di trattamento: strumenti per la conservazione, la compilazione e l'aggiornamento

I trattamenti sono effettuati sia con strumenti cartacei che elettronici, nel rispetto delle misure di sicurezza indicate dal Regolamento Europeo 2016/679 e da specifiche norme di legge o di regolamento, con particolare riferimento alle norme del Codice delle Amministrazioni Digitali e alle regole tecniche emanate dall'AGID.

I sistemi elettronici di proprietà del Titolare o dei propri responsabili del trattamento (software gestionali, registro elettronico, servizi amministrativi digitali) con i quali i dati vengono trattati dai soggetti autorizzati, sono in linea anche con gli adempimenti in merito alle misure minime di sicurezza ICT dettate dall'AGID, nell'ottica della massima tutela della riservatezza e dell'integrità dei dati non solo nella fase di conservazione ma anche durante tutte le altre fasi di trattamento.

I dati saranno conservati secondo le indicazioni di legge e nei tempi e nei modi indicati dalle Linee Guida per le Istituzioni scolastiche e dai Piani di conservazione e scarto degli archivi scolastici definiti dalla Direzione Generale degli Archivi presso il Ministero dei Beni Culturali, non esclusivamente presso l'Istituzione scolastica ma anche presso il Ministero dell'Istruzione e le sue articolazioni periferiche, presso altre Amministrazioni dello Stato, presso Regioni ed enti locali, presso Enti con cui la scuola coopera in attività e progetti nei casi previsti da disposizioni di legge o di regolamento. I soggetti sopra menzionati agiranno di volta in volta come titolari autonomi o come contitolari.

D) Tempi di conservazione

Il Titolare tratterà i dati personali per il tempo necessario per adempiere alle finalità di cui sopra e comunque per non oltre 10 anni dalla cessazione del rapporto per le finalità di servizio. I tempi di conservazione sia cartacei che telematici sono stabiliti dalla normativa di riferimento per le Istituzioni scolastiche in materia di Archivistica (RifLeg. 3 e RifLeg. 4).

Comunicazione e diffusione dei dati: categorie di destinatari e modalità

Tutte le comunicazioni o le diffusioni dei dati personali e particolari della sua famiglia a soggetti diversi da quelli che li trattano per conto del Titolare (addetti sotto la sua autorità o sotto l'autorità dei suoi responsabili del trattamento) saranno effettuate esclusivamente se ammesse da una norma di legge o, nei casi previsti dalla legge, di regolamento.

Una attenzione maggiore da parte dell'Istituto sarà posta nei confronti di comunicazioni o di diffusioni dei dati particolari della sua famiglia; per questi ultimi, infatti, esistono particolari specifiche previste dalla normativa relativamente alla tipologia di dati che possono essere trattati, alle operazioni eseguibili e al motivo di interesse pubblico rilevante, nonché alle misure appropriate e alle specifiche per tutelare i diritti fondamentali dell'interessato (RifLeg. 5).

Le comunicazioni potranno avvenire attraverso invio cartaceo o trasmissione elettronica; in quest'ultimo caso saranno esclusivamente utilizzati mezzi e piattaforme informatiche che tutelano la riservatezza e l'integrità dei dati.

Tutte le comunicazioni previste per i diversi trattamenti sono indicate, trattamento per trattamento, nei paragrafi precedenti.

Trasferimento dati verso un paese terzo e/o un'organizzazione internazionale

I dati personali sono normalmente conservati su server ubicati all'interno dell'Unione Europea da parte dei fornitori dei servizi.

Resta in ogni caso inteso che il Titolare, ove si rendesse necessario, avrà facoltà di attivare servizi che comportino la presenza di server anche extra-UE (ad esempio, nel caso di utilizzo delle piattaforme Google Suite for Education, Office 365, Amazon Chime). In tal caso, il Titolare assicura sin d'ora che il trasferimento dei dati extra-UE avverrà in conformità alle disposizioni di legge applicabili e, più specificamente, attraverso l'applicazione di "clausole contrattuali tipo".

Per sua maggiore informazione e tutela il Titolare sottolinea che, in linea col parere della Corte di Giustizia europea, la pubblicazione in piattaforme di comunicazione WEB non rientra nei casi di "flussi transfrontalieri dei dati".

Natura del conferimento e conseguenze del rifiuto di rispondere

Il conferimento dei dati per i trattamenti descritti nel presente documento è obbligatorio per l'esecuzione dei compiti del Titolare. Restano validi, ovviamente, i suoi diritti elencati nella apposita sezione del presente documento.

Diritti dell'interessato e modalità di esercizio

Nella Sua qualità di interessato ha i diritti di cui all'art. 15 del Regolamento e precisamente i diritti di:

1. ottenere la conferma dell'esistenza o meno di dati personali che La riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile;
2. ottenere l'indicazione:
 - a) dell'origine dei dati personali;
 - b) delle finalità e modalità del trattamento;
 - c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
 - d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art. 3, comma 1,

GDPR;

e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati;

3. ottenere:

a) l'aggiornamento, la rettifica ovvero, quando vi ha interesse, l'integrazione dei dati;

b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli obblighi in capo al Titolare;

c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;

4. opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che La riguardano, ancorché pertinenti allo scopo della raccolta, con le conseguenze descritte nella sezione 6 del presente documento.

Per far valere i suoi diritti potrà rivolgersi senza particolari formalità sia al Titolare del trattamento sia al Responsabile per la Protezione dei dati, ai riferimenti indicati alla sezione.

Ha altresì il diritto di reclamo all'Autorità Garante.

Riferimenti normativi

RifLeg. 1: Regolamento UE 2016/679 "Regolamento Generale sulla Protezione dei Dati"

RifLeg. 2: D.Lgs. 101/2018 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

RifLeg. 3: DPR 445/2000 "Disposizioni legislative in materia di documentazione amministrativa".

RifLeg. 4: Decreto Legislativo 22 gennaio 2004 n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137".

RifLeg. 5: D.M. 305/2006, "Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione, in attuazione degli articoli 20 e 21 del decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali».

Il titolare del trattamento dei dati

L'istituto nella persona di {Dirigente}

firma autografa sostituita da indicazione a mezzo stampa,

ai sensi dell'art.3 D.Lgs. 39/1993

Per comodità l'apposizione del flag per presa visione e adesione sul Registro elettronico Argo sostituisce la compilazione del seguente modulo da parte dei genitori dell'alunno

Alla cortese att.ne del Titolare del trattamento

Presa visione dell'informativa per il trattamento dei dati personali

La/Il sottoscritta/o _____, nata/o a _____ il _____

e la/Il sottoscritta/o _____, nata/o a _____ il _____

genitori/tutori dell'alunna/o _____

o, in alternativa (alunno maggiorenne), la/il sottoscritta/o

frequentante la classe _____ sez. _____ dell'Istituto, (di seguito denominati per semplicità "interessato"),

DICHIARA / DICHIARANO

a) di avere acquisito in data odierna l'informativa "alunni e famiglie" fornita dal titolare ai sensi degli artt. 13 e 14 del Regolamento 2016/679 e reperibile nella sezione dedicata alla Privacy e Protezione dei dati personali del sito WEB dell'Istituto, al link:

<https://netcrm.netsenseweb.com/scuola/privacy/netsense/PAIC84200X>.

b) Di impegnarsi, qualora fosse destinatario di elaborati contenenti foto e video dei ragazzi ripresi durante attività didattiche di particolare rilievo (progetti / recite / gite / saggi / ecc), ad utilizzarli esclusivamente per fini personali e in ambito familiare o amicale, astenendosi dal diffonderli attraverso canali sociali (facebook / ecc.), web o qualsiasi altro mezzo di comunicazione senza il consenso delle persone riprese. Tali elaborati non saranno oggetto di diffusione da parte dell'Istituto. Resta fermo il diritto di opposizione dell'interessato a tale trattamento, da esercitare utilizzando l'apposito modulo messo a

disposizione nell'area privacy e protezione dei dati del sito WEB dell'istituto.

Solo nel caso di utilizzo del sistema "Pago in rete"

codice fiscale da associare a quello dell'alunno _____

☐ Si richiede di associare all'alunno/a il profilo del rappresentante di classe, al fine di permettere a quest'ultimo di effettuare per conto del/i dichiarante/i i pagamenti degli avvisi telematici. (barrare nel caso di richiesta)

Data _____ Firma gen.1/maggiorenne _____ Firma gen.2 _____

Il/la sottoscritt____, data l'impossibilità di ottenere la firma congiunta di entrambi i genitori, consapevole delle conseguenze amministrative e penali per chi rilasci dichiarazioni non corrispondenti a verità ai sensi del DPR 445/2000, dichiara di aver effettuato la scelta in osservanza delle disposizioni sulla responsabilità genitoriale di cui agli artt. 316, 337 ter e 337 quater del codice civile.

Data _____ Firma del genitore _____

Allegato 7 e-Policy - Regolamento utilizzo piattaforma Google Workspace for education

per scopi didattico-formativi (eLearning) e per svolgimento di riunioni in modalità telematica



MINISTERO DELLA PUBBLICA ISTRUZIONE

Istituto Comprensivo Statale "Casteldaccia"

Istituto ad indirizzo musicale

Via Carlo Cattaneo N.80 - 90014 CASTELDACCIA (PA) C.F.: 90007610828 - Cod. Min.: PAIC84200X

☎ 091-954299 - Fax 091-9100217

REGOLAMENTO UTILIZZO PIATTAFORMA GOOGLE WORKSPACE FOR EDUCATION PER SCOPI DIDATTICO-FORMATIVI (E-LEARNING) E PER SVOLGIMENTO DI RIUNIONI IN MODALITÀ TELEMATICA

INDICE

[Art. 1 - Descrizione del servizio](#)

[Art. 2 - Definizioni](#)

[Art. 3 - Natura e finalità del servizio](#)

[Art. 4 - Amministratore della piattaforma](#)

[Art. 5 - Soggetti che possono accedere al servizio in qualità di utenti](#)

[Art. 6 - Condizioni e norme generali di utilizzo](#)

[Art. 7 - Norme finali](#)

[Art. 8 - Entrata in vigore](#)

[Art. 9 - Allegati](#)

Art. 1 - Descrizione del servizio

1. L'Istituto mette a disposizione ai propri docenti, studenti e al personale ATA autorizzato, la piattaforma "Google Workspace for Education" che sarà attivata come supporto digitale alla didattica (di seguito denominato eLearning) e come strumento per la conduzione delle attività che la normativa vigente permette di svolgere in modalità agile (da remoto), incluso il lavoro agile e alle riunioni telematiche. Più specificamente, è prevista la possibilità di condurre in modalità telematica le riunioni degli organismi in cui è coinvolta l'istituzione scolastica a tutti i livelli:

- Programmazione educativa
- Dipartimenti disciplinari
- Commissioni
- Assemblee di sezione/classe con i genitori Incontri scuola-famiglia
- Colloqui individuali con i genitori
- Formazione
- Gruppo di progetto
- Gruppo di lavoro operativo per l'inclusione (GLO) Riunioni di Staff della dirigenza
- Ogni altra riunione che può essere svolta on line, non avente carattere deliberativo, salvo sopravvenute cause di

forza maggiore notificate da parte del DS con apposito decreto. Per questi casi è possibile convocare gli OO.CC. in modalità online o mista e seguire quanto contenuto nel presente regolamento integrandolo come previsto da Allegato 4 (Regolamento Riunioni a distanza OO.CC).

2. Il presente regolamento disciplina le condizioni di amministrazione e di utilizzo della piattaforma con le applicazioni ad essa connesse e definisce le modalità di accesso per la fruizione del servizio.
3. Il regolamento si applica a tutti gli utenti titolari di un account.
4. Il servizio è fornito gratuitamente ed è fruibile fino al termine del percorso di studio degli studenti o al termine dell'attività lavorativa presso l'istituto dei dipendenti.
5. La Piattaforma sarà impostata e gestita dall'Amministratore designato, al quale sarà assegnato un account con privilegi superiori al fine di poter gestire gli aspetti tecnici dei singoli servizi.

Art. 2 - Definizioni

Nel presente regolamento i termini qui sotto elencati hanno il seguente significato:

1. Istituto: "Istituto Comprensivo Casteldaccia".
2. Piattaforma: l'insieme dei software che compongono la suite Google Workspace for education.
3. Amministratore di Piattaforma: il responsabile incaricato dal Dirigente Scolastico per l'amministrazione del servizio.
4. Servizio: servizio "Google Workspace for Education", messo a disposizione dalla scuola.
5. Fornitore: Google Inc. con sede in 1600 Amphitheatre Parkway, Mountain View, CA 94043.
6. Dominio scolastico: l'insieme dei servizi offerti dalla piattaforma entro il nome istitutocomprensivocasteldaccia.net.
7. Account: insieme di funzionalità, applicativi, strumenti e contenuti attribuiti ad un nome utente con le credenziali di accesso.
8. Utente: colui che utilizza un account del servizio.
9. Riunioni in modalità telematica: incontri virtuali sulla piattaforma, in cui tutti le/i partecipanti intervengono da luoghi diversi attraverso gli strumenti messi a disposizione dalla piattaforma stessa (a titolo esemplificativo e non esaustivo: Google Meet / Google Drive / Classroom).

Art. 3 - Natura e finalità del servizio

Il servizio consiste nell'accesso agli applicativi di "Google Workspace for Education" del fornitore. In particolare ogni utente

avrà a disposizione un account personale, oltre alla possibilità di utilizzare tutti i servizi aggiuntivi di (Google Drive, Google Documenti, Google Moduli, Google Classroom, Google Suites, ecc.) senza la necessità di procedere ad alcuna installazione per la loro funzionalità sui PC, in quanto applicazioni Web Based.

Il servizio è inteso come supporto eLearning e come strumento per la condizione delle attività che la normativa vigente permette di svolgere in modalità agile (da remoto), incluso il lavoro agile e gli incontri online degli OO.CC.

Pertanto gli account creati devono essere usati esclusivamente per tali fini.

Art. 4 - Amministratore della piattaforma

L'amministratore della piattaforma sarà designato con apposito atto, secondo il modello allegato al presente regolamento. All'amministratore saranno anche fornite delle istruzioni di base, redatte seguendo i principi dettati dal Regolamento Europeo sulla protezione dei dati (GDPR).

All'amministratore sarà fornito l'account amministratoregsuiteicc@istitutocomprensivocasteldaccia.net, il quale costituirà il punto di contatto per la risoluzione delle diverse problematiche tecniche.

Art. 5 - Soggetti che possono accedere al servizio in qualità di utenti

Le credenziali per l'accesso (account utente) saranno fornite dall'Amministratore a studenti, docenti e al personale ATA autorizzato a tempo determinato e indeterminato al momento dell'assunzione fino al termine dell'attività lavorativa presso l'Istituto.

Ai docenti sarà anche associata una casella email senza limiti di comunicazione verso l'esterno del dominio scolastico.

Agli studenti sarà associata una casella email limitata alle comunicazioni entro il dominio scolastico ad eccezione del portale Argo e della mail istituzionale della scuola; in altre parole, dalle caselle studente non si potranno ricevere (o inviare) email dall'esterno (o all'esterno) dei domini informatici scolastici.

Altre categorie di utenti possono richiedere la creazione di un account, sempre in relazione alle necessità didattiche o di servizio; in questo caso l'accoglimento della domanda è a insindacabile giudizio del Dirigente Scolastico.

Art. 6 - Condizioni e norme generali di utilizzo

Per tutti gli utenti l'attivazione del servizio è subordinata all'accettazione esplicita del presente Regolamento e delle seguenti condizioni generali di utilizzo, valide per tutti i profili utenti e per qualsiasi tipo di utilizzo della piattaforma, sia di tipo didattico (eLearning) sia per la conduzione di attività legate al lavoro agile o alle riunioni telematiche.:

14. L'utente può accedere direttamente al suo account istituzionale collegandosi a google.it, inserendo il suo account, la password fornita inizialmente dall'Amministratore che sarà necessario modificare al primo accesso.
15. Gli account fanno parte del dominio di cui l'Istituto è proprietario indicato nel paragrafo "definizioni".
16. Nel caso di smarrimento della password, l'utente potrà rivolgersi direttamente all'Amministratore della piattaforma scolastica.
17. Ogni account è associato ad una persona fisica ed perciò strettamente personale. Le credenziali di accesso non possono, per nessun motivo, essere comunicate ad altre persone, né cedute a terzi in quanto come dettato dall'art. 24 del CAD (Codice dell'Amministrazione Digitale) sono equiparate all'uso della firma elettronica debole.

18. L'Utente accetta pertanto di essere riconosciuto quale autore dei messaggi inviati dal suo account e di essere il ricevente dei messaggi spediti al suo account.
19. L'utente si impegna a collegarsi ricorrendo agli strumenti per le videochiamate online (Google meet) da qualsiasi luogo che assicuri il rispetto delle prescrizioni di cui al presente regolamento, in luogo non pubblico, né aperto al pubblico e comunque in assenza di terzi.
20. L'utente s'impegna ad utilizzare l'account esclusivamente per le finalità indicate al precedente Art. 3.
21. L'utente s'impegna a non utilizzare il servizio per effettuare azioni e/o comunicazioni che arrechino danni alla rete o a terzi utenti o che violino le leggi ed i regolamenti d'Istituto vigenti.
22. L'utente s'impegna a rispettare le regole che disciplinano il comportamento nel rapportarsi con altri utenti e a non ledere i diritti e la dignità delle persone.
23. L'utente s'impegna a non trasmettere o condividere informazioni che possano presentare forme o contenuti di carattere pornografico, osceno, blasfemo, diffamatorio o contrario all'ordine pubblico o alle leggi vigenti in materia civile, penale ed amministrativa.
24. È vietato immettere in rete materiale che violi diritti d'autore, o altri diritti di proprietà intellettuale o industriale o che costituisca concorrenza sleale.
25. L'utente s'impegna a non procedere all'invio massivo di mail non richieste (spam).
26. L'utente s'impegna a non fare pubblicità, a non trasmettere o rendere disponibile attraverso il proprio account qualsiasi tipo di software, prodotto o servizio che violi il presente regolamento o la legge vigente.
27. L'utente è responsabile delle azioni compiute tramite il suo account e pertanto esonera l'Istituto da ogni pretesa o azione che dovesse essere rivolta all'Istituto medesimo da qualunque soggetto, in conseguenza di un uso improprio.

Alle presenti condizioni e norme generali di utilizzo si aggiungono quelle specifiche per i diversi ruoli dell'utenza (studente, docente) e per le diverse funzionalità di utilizzo della piattaforma (didattica, lavoro agile, riunioni telematiche). Tali norme specifiche sono indicate nelle corrispondenti disposizioni al soggetto interessato, allegate al presente documento.

Art. 7 - Norme finali

In caso di violazione delle norme stabilite nel presente regolamento e nei suoi allegati, l'Istituto nella persona del Dirigente Scolastico potrà sospendere l'account dell'utente o revocarlo definitivamente senza alcun preavviso e senza alcun addebito a suo carico e fatta salva ogni altra azione di rivalsa nei confronti dei responsabili di dette violazioni.

L'Istituto si riserva la facoltà di segnalare alle autorità competenti - per gli opportuni accertamenti ed i provvedimenti del caso - le eventuali violazioni alle condizioni di utilizzo indicate nel presente Regolamento, oltre che alle leggi ed ai regolamenti vigenti.

L'account viene temporaneamente sospeso a seguito di violazioni del presente regolamento per le opportune verifiche.

L'account viene revocato:

- a seguito di reiterate violazioni del presente regolamento
- dopo 90 giorni dal termine del percorso di studi presso l'Istituto per gli studenti
- dopo 90 giorni dal termine del rapporto lavorativo per i docenti assunti a tempo indeterminato e determinato (con termine incarico: giugno)
- nel caso di supplenze brevi, l'account sarà invece sospeso dopo 30 giorni dal termine del contratto; trascorsi ulteriori 30 giorni, l'account sarà revocato.

La revoca dell'account da parte dell'amministratore comporta la perdita irreversibile dei dati ad esso collegati (file su Google Drive, messaggi di posta elettronica etc.). Pertanto, gli utenti dovranno provvedere autonomamente a effettuare il download o il trasferimento di tutti i materiali e dei file di interesse collegati al proprio account prima della revoca.

L'Istituto s'impegna a tutelare i dati forniti dall'utente in applicazione del D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" e del D.Lgs. n. 101/2018 e successive modifiche e integrazioni, ai soli fini della creazione e mantenimento dell'account.

Il servizio è erogato dal fornitore che applica la propria politica alla gestione della privacy; l'utente può conoscere in dettaglio tale politica visitando il sito web del fornitore a questo link: <https://policies.google.com/privacy>.

Art. 8 - Entrata in vigore

Il presente Regolamento entra in vigore dalla data di pubblicazione sul sito della relativa delibera di approvazione del Consiglio d'Istituto della scuola.

Art. 9 - Allegati

Fanno parte integrante del presente regolamento:

1. Allegato 1: nomina amministratore della piattaforma e istruzioni di amministrazione
2. Allegato 2: disposizioni operative per le famiglie - eLearning
3. Allegato 3: disposizioni operative per i docenti - eLearning e riunioni telematiche
4. Allegato 4: Regolamento riunioni online OO.CC

Allegato 1 - Regolamento per Google Workspace- Nomina e istruzioni piattaforma (allegato dell'Allegato7- Epolicy)



MINISTERO DELLA PUBBLICA ISTRUZIONE

Istituto Comprensivo Statale "Casteldaccia"

Istituto ad indirizzo musicale

Via Carlo Cattaneo N.80 – 90014 CASTELDACCIA (PA) C.F.: 90007610828 – Cod. Min.: PAIC84200X

☎ 091-954299 – Fax 091-9100217

Spett.le

Prof.ssa Lorena Ragusa

C.F. RGSLRN76P62G273Q

NOMINA ED ISTRUZIONI AMMINISTRATORE PIATTAFORMA

E DESIGNAZIONE AI SENSI DELL'ART. 2 QUATERDECIS CODICE PRIVACY

"Attribuzione di funzioni e compiti a soggetti designati"

IL DIRIGENTE SCOLASTICO

- in qualità di Titolare del trattamento dei dati personali dell'Istituzione scolastica (di seguito denominato Istituto);
- visto quanto disposto dal Regolamento Generale per la Protezione dei Dati (GDPR) in merito alle misure di sicurezza minime che ogni Titolare dei dati deve garantire;
- visto quanto previsto dall'art. 2-quaterdecis del Codice Privacy (D.Lgs. 196/2003 novellato dal D.Lgs. 101/2018);
- visto quanto disposto dal provvedimento Garante del 25/06/2009 in merito all'utilizzo di figure specializzate per la gestione e l'amministrazione delle infrastrutture informatiche;
- preso atto della necessità di gestire la piattaforma software online scelta dall'istituto per la conduzione di attività a distanza, di seguito denominata "Piattaforma";
- verificato che l'ambito operativo della Piattaforma non è incluso nelle sfere di competenza dell'Amministratore di Sistema e dell'Amministratore di rete dell'Istituto;
- visto il modello organizzativo privacy dell'istituto, in cui è citata l'opportunità di nominare ed incaricare le figure sopracitate in seno all'organizzazione dell'istituto;

- tenuto conto delle competenze possedute dalla S.V., dopo averne anche verificato l'idoneità rispetto alle caratteristiche di esperienza, capacità e affidabilità richieste dalle vigenti disposizioni per adempiere agli obblighi in materia di sicurezza del trattamento informatico specifico della Piattaforma;

NOMINA

la S.V. quale Amministratore della Piattaforma, anche ai sensi dell'art. 2-quaterdecis del Codice Privacy.

La S.V. accetta tale nomina, al fine di potere erogare legittimamente i servizi offerti, e si impegna ad osservare e rispettare, col presente atto, tutte le norme che regolano la materia del trattamento dei dati personali e le istruzioni di trattamento impartite di seguito.

ART. 1 - MISURE TECNICHE GENERALI

In qualità di Amministratore della Piattaforma la S.V. ha la responsabilità di applicare tutte le misure tecniche necessarie alla:

- impostazione dei differenti permessi di utilizzo delle varie APP della suite, con particolare riferimento a quelle che permettono la fuoriuscita dal dominio scolastico (queste ultime vietate per gli studenti a meno di una esplicita autorizzazione da parte degli utenti interessati);
- impostazione dei criteri di sicurezza da assegnare ai dispositivi tablet android e/o chromebook da affidare in comodato d'uso;
- creazione, modifica o cancellazione delle unità organizzative / gruppi di utenza;
- creazione, attivazione, disattivazione, modifica o cancellazione degli account utente;
- suddivisione degli utenti nei vari gruppi / unità organizzative, anche in relazione alle misure di sicurezza impostate;
- attivazione delle procedure di recupero password per gli utenti che ne facessero esplicita richiesta (con l'obbligo, in questi casi, di rendere necessario, per l'utente, il cambio della password al primo utilizzo);
- risoluzione di problematiche tecniche bloccanti;
- azzeramento dei dati a fine anno scolastico.

Sono escluse le attività di mero supporto tecnico agli utenti.

ART. 2 - MISURE TECNICHE SPECIFICHE E OBBLIGATORIE

Si sottolinea alla S.V. alcune impostazioni da implementare obbligatoriamente, in ossequio ai principi di minimizzazione del trattamento dei dati personali e di utilizzo dei soli dati pertinenti e non eccedenti:

- Richiedere solo nome e cognome dell'utente, unici dati essenziali all'attivazione dell'account.

- Disattivare l'autenticazione a due fattori con SMS: questa richiederebbe di memorizzare il numero di telefono dell'utente, azione esplicitamente vietata.
- Controllare le impostazioni e attivare solo le app essenziali (Gmail, Meet, Drive e Calendario).
- Disattivare i servizi Google aggiuntivi non autorizzati dal Dirigente Scolastico.
- Disattivare il Google Marketplace, ad eccezione dei componenti aggiuntivi autorizzati dal Dirigente Scolastico.
- Disattivare per scelta predefinita l'accesso ad app di terze parti ed utilizzare esclusivamente le disposizioni elencate nel seguito per attivare esclusivamente quelle necessarie alle specifiche attività.

POLITICA DI SICUREZZA APP TERZE PARTI

Le fonti in ordine di processo:

a) <https://support.google.com/a/answer/7281227>

b) <https://support.google.com/a/answer/13288950?hl=it#zippy=%2Cche-cosa-sono-i-servizi-google-soggetti-a-restrizioni-e-non-soggetti-a-restrizioni>

In sintesi:

A) PRIMO PASSO: verificare di aver impostato in console le impostazioni di accesso in base all'età, indicando che nelle Unità Organizzativa degli Studenti ci sono dei minorenni:

Vi si accede dalla console di amministratore, Voce: Account->Impostazioni account-> ..selezionare le UO (Unità Organizzative) con studenti -> Etichetta Età

Selezionare "Alcuni o tutti gli utenti di questo gruppo o di questa unità organizzativa sono minori di 18 anni"

B) SECONDO PASSO: assegnare il permesso per APP che richiedono in "Accedi con google" esclusivamente il nome e la email dell'utente
Obiettivo: Fare in modo che gli utenti identificati come minori di 18 anni possano usare "Accedi con Google" per quelle app che richiedono esclusivamente le informazioni di base (nome, email ed eventuale immagine del profilo).

Metodo: selezionare nell'impostazione "App di terze parti non configurate per gli utenti identificati come minori di 18 anni" la seguente opzione: "Consenti agli utenti di accedere alle app di terze parti che richiedono solo le informazioni di base necessarie per Accedi con Google"

C) TERZO PASSO: proteggere per default i dati interni alla workspace di istituto

Impostare tutti i servizi Google nella modalità "Con restrizioni" (in modo tale che questi servizi consentano l'accesso ai dati alle sole APP contrassegnate come Attendibili, negando invece alle altre).

D) QUARTO PASSO: Classificare le APP terze parti da attivare, privilegiando l'impostazione "con restrizioni"

Nella scheda "Controllo accesso app" è possibile accedere alle richieste di accesso alle app terze parti.

Queste richieste di accesso possono essere classificate dall'amministratore come:

- Con restrizioni (da ritenere l'opzione predefinita, da preferire): gli utenti possono accedere con Google a questa app, la quale può richiedere l'accesso solo ai dati di Google non soggetti a restrizioni. Quindi nel caso dell'istituto, grazie all'impostazione di cui alla lettera C), praticamente ai soli dati a basso rischio.

- Attendibile (da usare solo se necessario e se si conosce la politica di rispetto dei dati da parte del fornitore della app): gli utenti possono accedere con Google a questa app di terze parti, la quale può richiedere l'accesso ai dati di Google, sia ai servizi Google non soggetti a restrizioni che (attenzione) a quelli soggetti a restrizioni.

- Bloccato: gli utenti non possono accedere con Google all'app di terze parti, la quale non può richiedere l'accesso ai dati di Google.

ART. 3 - OBBLIGHI DELL'AMMINISTRATORE DELLA PIATTAFORMA

Al designato è vietato comunicare eventuali dati personali di cui venisse a conoscenza durante l'espletamento delle funzioni di amministratore della piattaforma, se non esplicitamente autorizzato dal Titolare del Trattamento.

E' sempre vietata la diffusione dei dati personali.

Il designato inoltre:

- ha il dovere di custodire le credenziali di accesso di amministrazione alla piattaforma a lei/lui assegnate, le quali sono da considerarsi personali. In qualsiasi momento potrà modificare le proprie credenziali in modo tale da mantenere alto il livello di sicurezza dell'accesso;

- ha il potere e il dovere di compiere tutto quanto si renderà necessario ai fini del rispetto e della corretta applicazione delle misure di sicurezza nella custodia e nel trattamento dei dati personali;
- si impegna ad informare prontamente il Titolare del Trattamento di tutte le questioni rilevanti ai fini di legge ed in termini di sicurezza;
- si impegna a non utilizzare i dati trattati e le informazioni acquisite per finalità che non siano strettamente inerenti alla presente designazione e autorizzazione;
- si impegna ad attenersi, in ogni caso, a tutte le istruzioni che saranno impartite dal Titolare del Trattamento.

L'attività sarà retribuita con n. 20 ore a euro 19,25 al lordo delle ritenute previste.

La presente nomina produce effetti tra le parti per la durata del rapporto in essere tra l'Istituto e la S.V. o fino a revoca dell'incarico.

Riferimenti del Responsabile per la Protezione dei Dati (DPO) dell'Istituto

NetSense S.r.l., Partita IVA 04253850871,

email aziendale: info@netsenseweb.com, PEC aziendale: netsense@pec.it

nella persona di: Ing. Renato Narcisi, PEC personale: renato.narcisi@arubapec.it

Per accettazione Per l'Istituto

L'Amministratore della Piattaforma IL DIRIGENTE SCOLASTICO

Allegato 2 - Regolamento Google Workspace- Disposizioni operative e informativa famiglie (allegato dell'Allegato 7 - Epolicy)



MINISTERO DELLA PUBBLICA ISTRUZIONE

Istituto Comprensivo Statale "Casteldaccia"

Istituto ad indirizzo musicale

Via Carlo Cattaneo N.80 - 90014 CASTELDACCIA (PA) C.F.: 90007610828 - Cod. Min.: PAIC84200X

☎ 091-954299 - Fax 091-9100217

DISPOSIZIONI OPERATIVE E INFORMATIVA DATI PERSONALI GOOGLE WORKSPACE FOR EDUCATION FAMIGLIE E

STUDENTI PER L'UTILIZZO DEI TOOL DI DIDATTICA DIGITALE (e-LEARNING)

Ai sensi della normativa vigente l'istituto intende adottare strumenti informatici adatti a fruire di servizi di scambio di materiali didattici, videoconferenza ed interazione in tempo reale attraverso condivisione di audio e video in modalità peer-to-peer quale supporto digitale alle attività didattiche e alle riunioni telematiche del personale.

In particolare, l'istituto ha scelto quale piattaforma istituzionale la "Google Workspace for Education" (di seguito denominata "piattaforma"), sottoscrivendo regolare contratto e nomina del fornitore a Responsabile del Trattamento ai sensi dell'art. 28 del GDPR.

Il Dirigente scolastico, in riferimento all'utilizzo di tale piattaforma per scopi di eLearning rivolta agli studenti,

EMANA LE SEGUENTI DISPOSIZIONI OPERATIVE

valide per le famiglie e gli studenti che ne utilizzano i servizi eLearning.

ART. 1 - NORME GENERALI DI UTILIZZO

Le norme generali di utilizzo sono elencate nel corrispondente articolo del regolamento per l'utilizzo della Google Workspace, al quale il presente documento è allegato.

ART. 2 - NORME E DISPOSIZIONI SPECIFICHE PER LE ATTIVITA' DI E-LEARNING

- A meno di comprovate necessità, i genitori NON dovranno partecipare alle attività che coinvolgono lo studente.
- NON effettuare fotografie o registrazioni durante le video lezioni.
- NON condividere i parametri di accesso alle video lezioni o ad altri strumenti di condivisione dei materiali didattici con soggetti non autorizzati.
- NON utilizzare la piattaforma in modo da danneggiare, molestare o insultare altre persone.
- NON creare e non trasmettere immagini, dati o materiali offensivi, osceni o indecenti.
- NON creare e non trasmettere materiale offensivo per altre persone o enti.
- NON creare e non trasmettere materiale commerciale o pubblicitario se non espressamente richiesto.
- NON interferire, danneggiare o distruggere il lavoro dei propri docenti o dei propri compagni.
- NON curiosare nei file e non violare la riservatezza degli altri compagni.
- Gli elaborati prodotti devono essere consegnati esclusivamente nelle modalità indicate dal docente, NON condividendoli mai con soggetti terzi.

L'utilizzo del materiale audiovisivo è riservato esclusivamente agli alunni della classe ed è perciò consentito soltanto un uso privato da parte degli stessi allievi per fini didattici. Il materiale didattico è protetto dalle vigenti normativa in materia di

tutela del diritto d'autore (Legge n. 633/1941 e ss. mm. e ii.) nonché dalla normativa in tema di tutela dei dati personali (D.lgs. n. 196/2003 e ss.mm. e ii. e Regolamento UE n. 679/2016 - GDPR), pertanto ne è assolutamente vietata la divulgazione a terzi in qualsiasi forma, ivi compresa la sua riproduzione, pubblicazione e/o condivisione su social media (come ad esempio Facebook), piattaforme web (come ad esempio YouTube) applicazioni di messaggistica (come ad es. Whatsapp). Ogni utilizzo indebito e/o violazione sarà perseguita a termini di legge.

Si ribadisce alle famiglie, inoltre, la necessità di supervisionare l'uso degli ausili informatici eventualmente forniti agli studenti. L'Istituto non è responsabile del loro utilizzo al di fuori del dominio informatico della scuola.

ART. 3 - INFORMATIVA TRATTAMENTO DATI PERSONALI

(ex art. 13 Regolamento UE 2016/679 "GDPR")

Ai sensi della normativa vigente l'istituto intende adottare strumenti informatici adatti a fruire di servizi di scambio di materiali didattici, videoconferenza ed interazione in tempo reale attraverso condivisione di audio e video in modalità peer-to-peer quale supporto digitale alle attività didattiche e alle riunioni telematiche del personale.

In particolare, l'istituto ha scelto quale piattaforma istituzionale la "Google Workspace for Education" (di seguito denominata "piattaforma"), sottoscrivendo regolare contratto e nomina del fornitore a Responsabile del Trattamento ai sensi dell'art. 28 del GDPR.

La piattaforma scelta, in linea con quanto previsto dalle indicazioni e dalle norme in vigore, consente:

- l'autenticazione degli utenti e la gestione di accesso selettivo ai dati per categoria di utente;
- l'utilizzo di processi automatici e robusti di assegnazione agli utenti di credenziali;
- l'utilizzo di canali di trasmissione sicuri tenendo conto dello stato dell'arte;
- la possibilità di escludere la geo-localizzazione (impostazione scelta dall'amministratore della piattaforma) e il social-login;
- l'esclusiva erogazione di servizi dedicati alla didattica;
- il confinamento di ogni tool dello studente (mail, forum, ecc.) entro il dominio informatico della scuola.

In maniera del tutto analoga a quanto avviene in seno alla didattica in presenza, le attività condotte con tale piattaforma comportano il trattamento di alcuni dati personali degli studenti.

Tipo di dati e loro provenienza

Nome, Cognome, data di nascita, risultati di test telematici, indirizzo IP del dispositivo che si collega, elaborati telematici.

I dati personali sono acquisiti direttamente dall'anagrafica gestita dall'istituto grazie al software utilizzato in segreteria.

Finalità e base giuridica

Tutti i trattamenti dei dati sono effettuati dal Titolare per l'esecuzione di un compito di interesse pubblico o comunque connesso all'esercizio di pubblici poteri.

La base giuridica per ogni trattamento è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento. Pertanto il suo consenso esplicito non è richiesto; valgono, ovviamente, i suoi diritti elencati nella apposita sezione del presente documento.

Soggetti titolati al trattamento per conto del Titolare

I trattamenti dei dati per conto del Titolare sono effettuati dai docenti nella loro qualità di addetti autorizzati al trattamento e dall'amministratore della piattaforma. Ogni addetto al trattamento è debitamente istruito.

È anche previsto che i trattamenti dei dati per conto del Titolare possano essere effettuati da soggetti esterni contrattualizzati dall'Istituto per l'esecuzione di particolari compiti. In questi casi i soggetti esterni sono espressamente nominati quale "responsabili del trattamento" e limiteranno il trattamento dei dati alle sole finalità indicate negli accordi contrattuali; è prevista la riconsegna di tutti i dati da parte di ogni responsabile del trattamento all'Istituto all'esaurimento delle finalità contrattuali, fatte salve specifiche disposizioni di legge.

Modalità di trattamento

I trattamenti sono effettuati con strumenti elettronici, nel rispetto delle misure di sicurezza indicate dal Regolamento Europeo 2016/679 e da specifiche norme di legge o di regolamento, con particolare riferimento alle norme del Codice delle Amministrazioni Digitali e alle regole tecniche emanate dall'AGID.

I sistemi elettronici di proprietà del Titolare o dei propri responsabili del trattamento sono in linea anche con gli adempimenti in merito alle misure minime di sicurezza ICT dettate dall'AGID, nell'ottica della massima tutela della riservatezza e dell'integrità dei dati non solo nella fase di conservazione ma anche durante tutte le altre fasi di trattamento.

Maggiori informazioni circa il funzionamento delle Google Apps for Education sono fornite dal Centro didattico di Google Workspace raggiungibile all'indirizzo <https://support.google.com/a/users/?hl=it#topic=9917952>

Per ulteriori informazioni la pagina della guida di Google è disponibile all'indirizzo <https://support.google.com>.

E' possibile consultare l'informativa sulla privacy di Google Workspace for Education agli indirizzi:

https://gsuite.google.com/terms/education_privacy.html

<https://www.google.com/intl/it/policies/privacy/>

Infine all'indirizzo https://gsuite.google.com/terms/user_features.html è disponibile il riepilogo dei servizi di Google Workspace.

Tempi di conservazione

Il Titolare tratterà i dati personali per tutto il corso di permanenza dello studente nel ciclo scolastico di riferimento.

Comunicazione e diffusione dei dati

I dati non saranno comunicati o diffusi a terzi, a meno dei soggetti sopra descritti quali "Responsabili del trattamento".

Trasferimento dati verso un paese terzo e/o un'organizzazione internazionale

I servizi comportano la presenza di server anche extra-UE. Il Titolare assicura sin d'ora che il trasferimento dei dati extra-UE avverrà in conformità all'accordo transfrontaliero siglato tra UE e gli USA.

Natura del conferimento e conseguenze del rifiuto di rispondere

Il conferimento dei dati per i trattamenti descritti nel presente documento è obbligatorio per l'esecuzione dei compiti del

Titolare. Restano validi, ovviamente, i suoi diritti elencati nella apposita sezione del presente documento.

Diritti dell'interessato e modalità di esercizio

Nella Sua qualità di interessato ha i diritti di cui all'art. 15 del Regolamento e precisamente i diritti di:

1. ottenere la conferma dell'esistenza o meno di dati personali che La riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile;
2. ottenere l'indicazione:
 - a) dell'origine dei dati personali;
 - b) delle finalità e modalità del trattamento;
 - c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
 - d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art. 3, comma 1, GDPR;
 - e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati;
3. ottenere:
 - a) l'aggiornamento, la rettifica ovvero, quando vi ha interesse, l'integrazione dei dati;
 - b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli obblighi in capo al Titolare;
 - c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;
4. opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che La riguardano, ancorché pertinenti allo scopo della raccolta, con le conseguenze descritte nella sezione 6 del presente documento.

Per far valere i suoi diritti potrà rivolgersi senza particolari formalità sia al Titolare del trattamento sia al Responsabile per la Protezione dei dati, ai riferimenti indicati alla sezione.

Ha altresì il diritto di reclamo all'Autorità Garante.

Allegato 3 - Regolamento Google Workspaces- Disposizioni operative e informativa docenti e ATA (allegato dell'Allegato7 - Epolicy)



MINISTERO DELLA PUBBLICA ISTRUZIONE

Istituto Comprensivo Statale "Casteldaccia"

Istituto ad indirizzo musicale

Via Carlo Cattaneo N.80 – 90014 CASTELDACCIA (PA) C.F.: 90007610828 – Cod. Min.: PAIC84200X

☎ 091-954299 – Fax 091-9100217

DISPOSIZIONI OPERATIVE E INFORMATIVA DATI PERSONALI GOOGLE WORKSPACE FOR EDUCATION DOCENTI E PERSONALE ATA (ADDETTI AL TRATTAMENTO) PER :

A) UTILIZZO DI TOOL DI DIDATTICA DIGITALE (E-LEARNING)

B) RIUNIONI TELEMATICHE

PREMESSE

Ai sensi della normativa vigente l'istituto intende adottare strumenti informatici adatti a fruire di servizi di scambio di materiali didattici, videoconferenza ed interazione in tempo reale attraverso condivisione di audio e video in modalità peer-to-peer quale supporto digitale alle attività didattiche e alle riunioni telematiche del personale.

In particolare, l'istituto ha scelto quale piattaforma istituzionale la "Google Workspace for Education" (di seguito denominata "piattaforma"), sottoscrivendo regolare contratto e nomina del fornitore a Responsabile del Trattamento ai sensi dell'art. 28 del GDPR.

Ogni docente dell'istituto, in quanto "persona autorizzata al trattamento", ha il dovere primario di rispettare la riservatezza di tutti i soggetti coinvolti e la loro sfera privata. Ha, altresì, il dovere di utilizzare e condividere solo informazioni esclusivamente inerenti l'attività didattica e le attività legate alle riunioni telematiche.

Il Dirigente scolastico, in riferimento all'utilizzo di tale piattaforma per scopi di eLearning rivolta agli studenti,

EMANA

le seguenti disposizioni operative, valide per i docenti e le unità di personale ATA autorizzato che utilizzano la piattaforma per erogare agli studenti i servizi eLearning e/o che siano coinvolti nelle riunioni telematiche.

ART. 1 - NORME GENERALI DI UTILIZZO

Le norme generali di utilizzo sono elencate nel corrispondente articolo del regolamento per l'utilizzo della Google Workspace, al quale il presente documento è allegato.

ART. 2 - NORME E DISPOSIZIONI SPECIFICHE PER LE ATTIVITA' DI E-LEARNING

Nell'utilizzo della piattaforma si prescrive di:

- Adottare una password robusta a protezione del proprio account, accertandosi di non cederla mai ad altri.
- Evitare la registrazione delle video lezioni effettuate con ausili informatici di videoconferenza. Ciò al fine di ridurre i rischi legati ad una possibile diffusione incontrollata o ad un uso improprio di tali registrazioni.

- Durante le sessioni di videoconferenza, è necessario regolamentare l'uso delle webcam, sia quelle degli studenti che quelle dei docenti e degli ATA, e fare in modo che lo stesso avvenga nel rispetto della vita privata di ciascuno.

NOTA SUI RISCHI LEGATI ALLA DIFFUSIONE DELLE REGISTRAZIONI: per quanto sia fatto espresso divieto agli studenti di effettuare registrazioni o fotografie durante le video lezioni, non ci sono garanzie che ciò non possa accadere e che le registrazioni effettuate possano essere successivamente diffuse o utilizzate impropriamente.

- Evitate di instaurare videochat con un solo studente, a meno dei casi già previsti nella didattica in presenza (ad esempio: lezioni di musica, lezioni con studenti disabili, ecc.)
- Utilizzare esclusivamente la/le piattaforme scelte dall'istituto quali piattaforma/e istituzionale.
- Adottare tutte le misure di cautela per evitare la diffusione di elaborati, lezioni o altro materiale all'esterno del gruppo classe di riferimento.
- È espressamente vietato l'utilizzo di social network che non offrono ausili dedicati esclusivamente all'education.
- Il mezzo di comunicazione telematica istituzionale con gli studenti è esclusivamente la suite Google Workspace for education.
- Il mezzo di comunicazione telematica istituzionale con le famiglie è esclusivamente il registro elettronico. Nell'utilizzo di quest'ultimo quale mezzo di comunicazione scuola-famiglia, bisogna porre estrema attenzione al livello di condivisione di una comunicazione, distinguendo tra:

a) condivisione di notizie a livello globale (tutti i genitori dell'istituto; es. circolari, ecc),

b) condivisione di notizie a livello di classe (tutti i genitori di una singola classe),

c) condivisione di notizie a livello privato (solo i genitori di un/una studente/ssa).

- In caso di forza maggiore, se si fosse costretti ad utilizzare temporaneamente un programma di messaggistica da cellulare, si ricorda con la presente di evitare i gruppi e che la maggior parte delle APP di messaggistica prevedono la conoscenza del proprio numero di telefono da parte gli interlocutori.

ART. 3 - MODALITA' E DISPOSIZIONI SPECIFICHE PER LE RIUNIONI TELEMATICHE

Con delibera del Collegio docenti del 9/05/2024 è stato proposto e deliberato quanto segue:

- L'opportunità di riunirsi o meno in modalità telematica è prerogativa dirigenziale sulla base di valutazioni di ordine organizzativo e di indicazioni pervenute con congruo anticipo riferite a necessità didattiche.
- Per le riunioni telematiche, la convocazione sarà comunicata tramite circolare sul sito ovvero inviata via posta elettronica almeno 5 giorni prima della riunione stessa.
- Per la validità della riunione telematica si attuano le seguenti modalità:

- a) Convocazione/autoconvocazione/impegno di servizio
 - b) Uso di strumenti telematici adeguati: computer, videocamera, casse, auricolari, ecc.
 - c) Verbalizzazione e verifica delle presenze
 - d) Trattazione degli argomenti all'eventuale ordine del giorno
 - e) Presa visione dell'informativa privacy
 - f) Sottoscrizione dell'impegno relativo al lavoro a distanza.
- Durante la riunione, la videocamera deve essere attiva per permettere l'identificazione di ciascun partecipante. La mancata identificazione di un partecipante comporterà per lo stesso l'obbligo di motivare e giustificare l'assenza secondo le norme previste.
 - La verbalizzazione delle riunioni in modalità telematica avviene redigendo apposito verbale in cui si attesta la data e ora, estremi della convocazione, presenti ed assenti, gli argomenti trattati, gli interventi, l'orario di chiusura della riunione, la firma del/della verbalizzante.

Programmazioni educative

- a). Le programmazioni educative sono previste in via ordinaria nel piano annuale delle attività
- b). Le ore vengono firmate sul registro cartaceo e il verbale viene caricato sul registro elettronico.

Dipartimenti disciplinari e Commissioni

- a) La convocazione per i lavori da svolgere nelle riunioni di dipartimenti disciplinari e commissioni sarà comunicata almeno 5 giorni prima tramite circolare, o in caso di lavori urgenti, sarà comunicata dal Dirigente Scolastico a tutti i componenti tramite circolare sul registro elettronico o posta elettronica. L'invio delle comunicazioni vale come avvenuta notifica.
- b) Le assenze saranno attestate nel verbale.
- c) Le riunioni saranno verbalizzate dal/dalla referente del dipartimento disciplinare e/o della commissione e i verbali resi disponibili ai componenti tramite registro elettronico.

Assemblee di sezione/classe con i genitori - Incontri scuola-famiglia - Colloqui individuali

- a) Le assemblee di sezione/classe con i genitori e gli incontri scuola-famiglia si svolgeranno previa convocazione a mezzo circolare inviata dal Dirigente Scolastico pubblicata sul registro elettronico almeno 5 giorni prima della data di svolgimento.
- b) Sarà generato un link a cui insegnanti e genitori accedono. Tutti i genitori saranno muniti di credenziali di accesso del/la proprio/a figlio/a create dal Team digitale di istituto; ognuno dovrà impegnarsi a custodirle nel rispetto della privacy.
- c) Per le assemblee di sezione/classe, gli/le insegnanti producono verbale di riunione in cui si riporta la data, l'ora della riunione, gli estremi della convocazione, gli argomenti trattati e la data di termine della riunione.
- d) Riguardo i colloqui individuali, i genitori previo appuntamento preso con i/le docenti di sezione/classe si incontreranno accedendo al link suddetto che sarà comunicato per tempo dai/dalle insegnanti anticipatamente.

Formazione

a) La convocazione per svolgere attività di formazione in modalità telematica deve avvenire tramite circolare del Dirigente Scolastico pubblicata sul registro elettronico o inviata per posta elettronica, almeno 5 giorni prima, e deve contenere giorno e ora di inizio e di fine incontro formativo e il link di accesso alla piattaforma.

b) Le presenze saranno attestate tramite link predisposto in piattaforma.

c) La prenotazione per gli interventi avverrà tramite la funzione "Alza mano".

Gruppo di lavoro operativo per l'inclusione (GLO)

a) La convocazione per svolgere attività di GLO in modalità telematica deve avvenire tramite circolare comunicata da parte delle/dei referenti/insegnanti di sostegno a genitori e terapeuti, almeno 5 giorni prima della riunione.

Riunioni di Staff della dirigenza

a) La convocazione per i lavori da svolgere sarà comunicata almeno 5 giorni prima, o in caso di lavori urgenti, sarà comunicata dalla Dirigente Scolastica a tutti i componenti tramite circolare sul registro elettronico o posta elettronica.

b) L'invio delle comunicazioni vale come avvenuta notifica.

ART. 4 - INFORMATIVA TRATTAMENTO DATI PERSONALI

(ex art. 13 Regolamento UE 2016/679 "GDPR")

Ai sensi della normativa vigente l'istituto intende adottare strumenti informatici adatti a fruire di servizi di scambio di materiali didattici, videoconferenza ed interazione in tempo reale attraverso condivisione di audio e video in modalità peer-to-peer quale supporto digitale alle attività didattiche e alle riunioni telematiche del personale.

In particolare, l'istituto ha scelto quale piattaforma istituzionale la "Google Workspace for Education" (di seguito denominata "piattaforma"), sottoscrivendo regolare contratto e nomina del fornitore a Responsabile del Trattamento ai sensi dell'art. 28 del GDPR.

La piattaforma scelta, in linea con quanto previsto dalle indicazioni e dalle norme in vigore, consente:

- l'autenticazione degli utenti e la gestione di accesso selettivo ai dati per categoria di utente;
- l'utilizzo di processi automatici e robusti di assegnazione agli utenti di credenziali;
- l'utilizzo di canali di trasmissione sicuri tenendo conto dello stato dell'arte;
- la possibilità di escludere la geo-localizzazione (impostazione scelta dall'amministratore della piattaforma) e il social-login;
- l'esclusiva erogazione di servizi dedicati alla didattica;
- il confinamento di ogni tool dello studente (mail, forum, ecc.) entro il dominio informatico della scuola.

In maniera del tutto analoga a quanto avviene in seno alla didattica in presenza, le attività condotte con tale piattaforma comportano il trattamento di alcuni dei suoi dati personali.

Tipo di dati e loro provenienza

Nome, Cognome, data di nascita, contenuti didattici e indirizzo IP del dispositivo che si collega, elaborati telematici.

I dati personali sono acquisiti direttamente dall'anagrafica gestita dall'istituto grazie al software utilizzato in segreteria.

Finalità e base giuridica

Tutti i trattamenti dei dati sono effettuati dal Titolare per l'esecuzione di un compito di interesse pubblico o comunque connesso all'esercizio di pubblici poteri.

La base giuridica per ogni trattamento è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento. Pertanto il suo consenso esplicito non è richiesto; valgono, ovviamente, i suoi diritti elencati nella apposita sezione del presente documento.

Soggetti titolati al trattamento per conto del Titolare

I trattamenti dei dati per conto del Titolare sono effettuati dai docenti e dal personale ATA nella loro qualità di addetti autorizzati al trattamento e dall'amministratore della piattaforma. Ogni addetto al trattamento è debitamente istruito.

È anche previsto che i trattamenti dei dati per conto del Titolare possano essere effettuati da soggetti esterni contrattualizzati dall'Istituto per l'esecuzione di particolari compiti. In questi casi i soggetti esterni sono espressamente nominati quale "responsabili del trattamento" e limiteranno il trattamento dei dati alle sole finalità indicate negli accordi contrattuali; è prevista la riconsegna di tutti i dati da parte di ogni responsabile del trattamento all'Istituto all'esaurimento delle finalità contrattuali, fatte salve specifiche disposizioni di legge.

Modalità di trattamento

I trattamenti sono effettuati con strumenti elettronici, nel rispetto delle misure di sicurezza indicate dal Regolamento Europeo 2016/679 e da specifiche norme di legge o di regolamento, con particolare riferimento alle norme del Codice delle Amministrazioni Digitali e alle regole tecniche emanate dall'AGID.

I sistemi elettronici di proprietà del Titolare o dei propri responsabili del trattamento sono in linea anche con gli adempimenti in merito alle misure minime di sicurezza ICT dettate dall'AGID, nell'ottica della massima tutela della riservatezza e dell'integrità dei dati non solo nella fase di conservazione ma anche durante tutte le altre fasi di trattamento.

Maggiori informazioni circa il funzionamento delle Google Apps for Education sono fornite dal Centro didattico di Google Workspace raggiungibile all'indirizzo <https://support.google.com/a/users/?hl=it#topic=9917952>

Per ulteriori informazioni la pagina della guida di Google è disponibile all'indirizzo <https://support.google.com>

E' possibile consultare l'informativa sulla privacy di Google Workspace for Education agli indirizzi:

https://gsuite.google.com/terms/education_privacy.html

<https://www.google.com/intl/it/policies/privacy/>

Infine all'indirizzo https://gsuite.google.com/terms/user_features.html è disponibile il riepilogo dei servizi di Google Workspace.

Tempi di conservazione

Il Titolare tratterà i dati personali per tutta la durata del rapporto contrattuale con l'interessato.

Comunicazione e diffusione dei dati

I dati non saranno comunicati o diffusi a terzi, a meno dei soggetti sopra descritti quali “Responsabili del trattamento”.

Trasferimento dati verso un paese terzo e/o un’organizzazione internazionale

I servizi comportano la presenza di server anche extra-UE. Il Titolare assicura sin d’ora che il trasferimento dei dati extra-UE avverrà in conformità all’accordo transfrontaliero siglato tra UE e gli USA.

Natura del conferimento e conseguenze del rifiuto di rispondere

Il conferimento dei dati per i trattamenti descritti nel presente documento è obbligatorio per l'esecuzione dei compiti del Titolare. Restano validi, ovviamente, i suoi diritti elencati nella apposita sezione del presente documento.

Allegato 4: Regolamento google workspace for education - Regolamento riunioni online OO.CC. (allegato dell'Allegato 7 E-policy)



REGOLAMENTO RIUNIONI ONLINE OO.CC.

Art. 1 - Ambito di applicazione

Il presente Regolamento disciplina lo svolgimento, in modalità telematica, delle riunioni degli OO. CC. dell'Istituto Comprensivo Casteldaccia nonché delle riunioni di staff, del Comitato per la valutazione dei docenti, del Consiglio di Istituto e Giunta esecutiva così come previsto e disciplinato dal T.U. delle disposizioni legislative vigenti in materia di istruzione (D.lgs. 297/1994 e s.m.i.).

Art. 2 - Strumenti utilizzabili per lo svolgimento delle riunioni collegiali in modalità telematica.

Le riunioni in modalità telematica si terranno tramite l'applicazione MEET della piattaforma Google Workspace, conforme al GDPR e con accesso riservato ai soli utenti accreditati, che permette servizi di videoconferenza e condivisione di documenti, nel rispetto della normativa vigente in materia di trattamento dei dati personali e di privacy (Regolamento UE 679/2016). Le riunioni potranno svolgersi in modalità telematica ogni volta che se ne ravvisi la necessità.

Art. 3 - Definizione

Ai fini del presente regolamento, per “riunioni in modalità telematica”, nonché per “sedute telematiche”, si intendono le riunioni degli organi collegiali di cui all'art.1 per le quali è prevista la possibilità che tutti i componenti dell'organo partecipino a distanza, esprimendo la propria opinione e/o il proprio voto mediante l'uso di apposite funzioni presenti nell'applicazione MEET della piattaforma telematica Google Workspace.

Art. 4 - Requisiti tecnici minimi

1. La partecipazione a distanza alle riunioni dei suddetti OO. CC. presuppone la disponibilità di strumenti telematici idonei a consentire la comunicazione in tempo reale a due vie e, quindi, il collegamento simultaneo fra tutti i partecipanti.

2. Le strumentazioni e gli accorgimenti adottati devono comunque assicurare la massima riservatezza possibile delle comunicazioni e consentire a tutti i partecipanti alla riunione la possibilità di:

- a. visione degli atti della riunione;
- b. intervento nella discussione;
- c. scambio di documenti;
- d. votazione;
- e. approvazione del verbale.

3. Sono considerate tecnologie idonee: teleconferenza, videoconferenza, posta elettronica, chat, modulo di Google (o altro simile).

Art. 5 - Materie/argomenti oggetto di deliberazione in modalità telematica

L'adunanza telematica sarà utilizzata dagli OO. CC. per deliberare sulle materie di propria competenza per le quali è impossibilitata di fatto la partecipazione collegiale in presenza. Nell'ipotesi di votazioni a scrutinio segreto viene assicurata la riservatezza del voto con idonei strumenti informatici.

Art. 6 - Convocazione

1. Gli organi collegiali, in caso di impedimento per causa di forza maggiore, possono essere convocati con modalità online, da remoto, e svolti nello stesso modo con utilizzo di strumenti individuali adatti allo scopo, utilizzando piattaforme che garantiscano la privacy.

2. La convocazione delle adunanze degli OO. CC. in modalità telematica deve essere inviata, a cura del Presidente o del Dirigente Scolastico, a tutti i componenti dell'organo almeno 5 giorni prima della data fissata per l'adunanza, tramite Registro Elettronico Argo e/o posta elettronica all'indirizzo mail istituzionale di ogni docente/componente o tramite altra apposita funzione prontamente comunicata. L'invio delle suddette comunicazioni vale come avvenuta notifica.

3. La convocazione contiene l'indicazione del giorno, dell'ora, degli argomenti all'ordine del giorno e dello strumento telematico utilizzato nella modalità a distanza: videoconferenza, posta elettronica certificata, posta elettronica di cui il componente dell'organo garantisca di fare uso esclusivo e protetto, modulo di Google (o altro simile) di cui il componente organo garantisca di fare uso esclusivo e protetto.

Art. 7 - Svolgimento delle sedute

1. La rilevazione della presenza avverrà attraverso il report di partecipazione fornito dall'applicazione Meet della piattaforma Google Workspace, in grado di registrare, in automatico, la data e l'ora.

2. Per la validità dell'adunanza telematica restano fermi i requisiti di validità richiesti per l'adunanza ordinaria:

- a. regolare convocazione di tutti gli aventi diritto;
- b. verifica del quorum costitutivo (la metà più uno degli aventi diritto) tramite l'applicazione Meet
- c. verifica del quorum deliberativo (la metà più uno dei voti validamente espressi) attraverso la seguente modalità: videoregistrazione dell'esito della votazione espressa tramite chat (se tutti in modalità on line), in caso di riunioni eseguite in modalità mista verranno contati i voti espressi via chat e sommati a quelli dei presenti in aula.

La sussistenza di quanto indicato alle lettere a), b) e c) è verificata e garantita da chi presiede l'organo collegiale e dal segretario che ne fa menzione nel verbale di seduta.

1. Preliminarmente alla trattazione dei punti all'Ordine del giorno, compete al Dirigente/coordinatore, con l'ausilio del Segretario verbalizzante, verificare la sussistenza del numero legale dei partecipanti. In caso di Collegio Docenti saranno individuati dal Dirigente un docente facente funzione di moderatore della chat per la richiesta di interventi e un docente che si occuperà di seguire il processo di votazione. Qualora nell'ora prevista per l'inizio delle riunioni o durante lo svolgimento delle stesse vi siano dei problemi tecnici che rendano impossibile il collegamento, si darà ugualmente corso all'assemblea, se il numero legale è garantito, considerando assente giustificato il componente dell'Organo che sia impossibilitato a collegarsi in videoconferenza. Se il numero legale non è garantito, la seduta dovrà essere interrotta e/o rinviata ad altro giorno.

Art. 8 - Verbale di seduta

La verbalizzazione delle sedute degli OO. CC. avviene redigendo apposito verbale nel quale devono essere riportati:

1. l'indicazione del giorno e dell'ora di apertura e chiusura della seduta;
2. la griglia con i nominativi dei componenti che attesta le presenze/assenze/assenze giustificate;
3. l'esplicita dichiarazione di chi presiede l'organo sulla valida costituzione dell'organo;
4. la chiara indicazione degli argomenti posti all'ordine del giorno;
5. i fatti avvenuti in sintesi durante la seduta e le dichiarazioni rese dai partecipanti alla seduta, anche a distanza;
6. il contenuto letterale della deliberazione formatasi su ciascun argomento all'ordine del giorno;
7. le modalità di votazione e la volontà collegiale emersa dagli esiti della votazione stessa.

La redazione materiale del verbale avviene posteriormente alla seduta e la sua approvazione è rimandata alla seduta successiva.

Art. 9 - Registrazione della video seduta del Collegio Docenti o del Consiglio d'Istituto

L'uso della videoregistrazione della seduta del Collegio Docenti e del Consiglio d'Istituto è consentito solo se finalizzato alla redazione del verbale e non anche all'uso personale. In tal caso, e previa proposta da parte del Presidente, deve essere comunque autorizzato dallo stesso organo collegiale con apposita mozione ad hoc che sarà sottoposta a votazione prima di ogni seduta.

Art. 10 - Consiglio di Istituto.

1. Il Consiglio di Istituto può essere consultato in modalità telematica, anche mista, attraverso l'uso della piattaforma di comunicazione dell'istituto. Il voto elettronico è previsto esclusivamente per l'assunzione di delibere chiaramente formulate e relative ad aspetti tecnico-esecutivi, al termine di un percorso istruttorio noto. L'avviso relativo alla consultazione, corredato dalla necessaria documentazione relativa alle delibere, deve pervenire con anticipo di almeno 5 giorni.
2. Tutti i membri del Consiglio sono tenuti a esprimere il proprio voto, favorevole o contrario, o a palesare la propria astensione. Il risultato della votazione sarà considerato valido soltanto se espresso dalla metà più uno dei componenti del Consiglio.
3. L'assunzione della delibera telematica viene ratificata da apposito verbale ed inserita nel Registro dei verbali del Consiglio.
4. Analogamente, qualora non si raggiunga il quorum della metà più uno dei votanti rispetto agli aventi diritto, il Consiglio sarà convocato in seduta straordinaria.
5. Per consentire le sedute telematiche, i genitori componenti del Consiglio useranno l'account istituzionale dei propri figli.

6. Relativamente alle delibere si procederà alle votazioni durante la seduta online tramite chat e/o moduli all'uopo predisposti.

Art. 11 - Collegio dei Docenti.

A) Il Collegio dei Docenti può essere consultato in modalità telematica, attraverso l'uso della piattaforma di comunicazione dell'istituto.

1. Il voto elettronico è previsto esclusivamente per l'assunzione di delibere chiaramente formulate e relative ad aspetti tecnico-esecutivi, al termine di un percorso istruttorio noto.

2. Tutti i membri del Collegio sono tenuti a esprimere solo il proprio voto contrario o a palesare la propria astensione, adducendo opportuna motivazione.

3. L'assunzione della delibera telematica viene ratificata da apposito verbale, da prodursi allo scadere del tempo previsto per lo scrutinio e inserirsi nel Registro dei verbali del Collegio dei docenti.

4. Qualora un decimo dei componenti richieda di procedere a una consultazione in presenza, il Dirigente Scolastico convoca in seduta straordinaria il Collegio dei Docenti per consentirne lo svolgimento.

5. Analogamente, qualora non si raggiunga il quorum della metà più uno dei votanti rispetto agli aventi diritto, il Collegio sarà convocato in seduta straordinaria.

6. Può essere convocato un Collegio docenti online sia ordinario (cioè previsto nel piano annuale delle attività), sia straordinario per urgenti e gravi motivi adottando le seguenti procedure:

a. Il collegamento in remoto non può avvenire dal luogo pubblico (es. piazze, stazioni, locali pubblici in genere) e l'intervenuto dovrà essere l'unico presente alla call dalla propria postazione.

b. I partecipanti sono tenuti al segreto d'ufficio per quanto previsto dalla normativa vigente e dal rispetto delle norme in materia di privacy ex Regolamento Europeo 2016/679 ed a tal fine: dovranno usare cuffie e non audio in open.

c. I partecipanti hanno l'obbligo di utilizzare la massima riservatezza e discrezione su dati personali oggetto di discussione e delle informazioni di cui dovessero comunque venire a conoscenza.

Per tale motivo:

d. i partecipanti sono tenuti a non diffondere o effettuare alcuna comunicazione a terzi riguardo ai dati personali o alle informazioni di cui verranno a conoscenza. Il vincolo di riservatezza continuerà ad avere valore anche dopo la cessazione dell'appartenenza agli Organi Collegiali e comunque finché le informazioni riservate non diventino di pubblico dominio.

7. La prenotazione degli interventi avverrà usando la chat della videoconferenza e/o per alzata di mano. Dopo l'introduzione in videoconferenza del Dirigente, ad ogni punto sarà chiesto, a chi abbia intenzione di intervenire, di prenotarsi nella chat e sarà data la parola in base alle prenotazioni. Gli eventuali interventi devono avere una durata massima di cinque minuti.

8. Qualora durante una votazione si manifestino dei problemi di connessione, e non sia possibile ripristinare il collegamento in tempi brevi, il Dirigente ripete la votazione dopo aver ricalcolato il quorum di validità della seduta e della conseguente votazione, tenuto conto che i componenti collegati in videoconferenza sono considerati assenti giustificati. In tal caso restano valide le deliberazioni adottate fino al momento della sospensione della seduta.

B) Svolgimento del collegio dei docenti in modalità asincrona

9. Il Collegio dei Docenti può essere consultato in modalità asincrona nel caso ci sia la necessità di acquisire delibere urgenti (bandi ed avvisi in scadenza).

10. Il voto in modalità asincrona è previsto esclusivamente per l'assunzione di delibere chiaramente formulate e relative ad aspetti tecnico-esecutivi al termine di un percorso istruttorio noto ovvero quando l'argomento oggetto di delibera sia stato già in precedenza affrontato.

11. L'avviso della consultazione, corredato dalla necessaria documentazione relativa alle delibere da assumere, deve pervenire il giorno precedente all'avvio delle votazioni e contenere l'indicazione della durata prevista della consultazione, di norma non inferiore alle 24 ore, e l'esplicita indicazione dell'orario di chiusura.

12. Le votazioni si effettuano compilando il form e trasmettendo lo stesso nei tempi indicati.

13. Tutti i membri del Collegio sono tenuti ad esprimere il proprio voto, favorevole o contrario, o a manifestare la propria astensione. In caso di voto contrario il docente dovrà esprimere le proprie motivazioni compilando il form predisposto. I risultati saranno consultabili previo accesso alla piattaforma.

Art.12 - Consiglio di Intersezione, di Interclasse e di Classe, Dipartimenti

Gli OO. CC. di cui sopra possano essere convocati online sia in via ordinaria (cioè previsto nel piano annuale delle attività), sia straordinaria per urgenti e gravi motivi adottando le seguenti procedure:

a) la convocazione in modalità online, deve essere inviata, a cura del Dirigente scolastico, a tutti i componenti dell'organo, almeno 5 giorni prima della data fissata per l'adunanza, tramite registro elettronico e/o posta elettronica all'indirizzo mail istituzionale di ogni docente e genitore rappresentante. L'invio delle suddette comunicazioni vale come avvenuta notifica.

Il presente Regolamento entra in vigore dal momento della sua approvazione.

Allegato 8- ePolicy Modulo per la segnalazione delle situazioni di rischio



Descrizione
dell'episodio o del
problema

	Vittima/e:	Autore/autrice e sostenitori:
	1.....	1.....
Soggetti coinvolti	Classe:	Classe:
	2.....	2.....
	classe.....	Classe:
Chi ha riferito dell'episodio?	- La vittima - Un compagno della vittima, nome: - Genitore, nome: - Insegnante, nome: - Altri, specificare:	
Atteggiamento del gruppo	Da quanti compagni/persona è sostenuto chi ha compiuto l'azione? Quanti compagni supportano la vittima o potrebbero farlo?	

Gli insegnanti sono
interventuti in
qualche modo ?

La famiglia o altri adulti hanno cercato di
intervenire ?

Chi è stato informato della situazione?

- ☐ coordinatore di classe
data: ☐ la famiglia del bullo/i
☐ consiglio di classe data: data:
☐ dirigente ☐ le forze dell'ordine
scolastico data: data:
☐ la famiglia della vittima/e ☐ altro, specificare:
data:

MODULO PER IL FOLLOW-UP DEI CASI

AZIONI INTRAPRESE

Aggiornamento 1
Aggiornamento 2
Aggiornamento 3
Aggiornamento 4
Aggiornamento 5

La situazione è

☐ migliorata ☐ invariata ☐ peggiorata Come:
☐ migliorata ☐ invariata ☐ peggiorata Come:
☐ migliorata ☐ invariata ☐ peggiorata Come:
☐ migliorata ☐ invariata ☐ peggiorata Come:
☐ migliorata ☐ invariata ☐ peggiorata Come:

Documento di e-policy - I.C. CASTELDACCIA

Data di protocollo: 06/10/2021 - 14:58



Allegato 9 ePolicy - Diario di Bordo dei casi



Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi							
Scuola _____				Anno Scolastico _____			
N°	Data	ora	Episodio (riassunto)	Azioni intraprese		Insegnante con cui l'alunno/a si è confidato	Firma
				Cosa?	Da chi?		