ALLEGATO B AL REGOLAMENTO DI ISTITUTO

Documento di ePolicy

PAIC84200X

I.C. CASTELDACCIA

VIA CARLO CATTANEO N. 80 - 90014 - CASTELDACCIA - PALERMO (PA)

Giovanni Taibi

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse. Internet rappresenta oggi un'enorme opportunità per fare ricerca, comunicare, documentare il proprio lavoro, pubblicare elaborati, condividere risorse ed esperienze. L'IC Casteldaccia si è posto l'obiettivo di potenziare l'uso delle tecnologie informatiche nella didattica e nell'organizzazione generale della scuola per svolgere esperienze formative e condurre in modo più efficiente le funzioni amministrative.

Le "competenze digitali" sono, infatti, fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

Gli strumenti informatici però, 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 E-Policy 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:

- 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.

Argomenti del Documento

Perché è importante dotarsi di una E-policy?

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.

1.2 - Ruoli e responsabilità

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

RUOLO	RESPONSABILITÀ'
Il Dirigente Scolastico	Responsabilità di una adeguata informazione del personale sui ruoli da svolgere per la sicurezza online e per la formazione di altri colleghi; Titolarità sul del trattamento dei dati (PPO); Garantire che la scuola utilizzi un Internet Service filtrato approvato, conforme ai requisiti di legge vigenti Essere a conoscenza delle procedure da seguire in caso di infrazione della e–Safety Policy; Ruolo di primo piano nello stabilire e rivedere la e- Safety Policy; Ricevere relazioni di monitoraggio periodiche della sicurezza online da parte del responsabile; Garantire che vi sia un sistema in grado di monitorare il personale di supporto che svolge le procedure di sicurezza online interne
I responsabili della sicurezza online (DSGA)	Responsabilità per i problemi di sicurezza online; Promuovere la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica; Garantire che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente per la

	sicurezza online; Garantire che sia tenuto un registro di incidenti di sicurezza online; Facilitare la formazione e la consulenza per tutto il personale; Coordinare con le autorità locali e le agenzie competenti; Controllare la condivisione di dati personali; Controllare l'accesso a materiali illegali / inadeguati; Controllare probabili azioni di cyberbullismo
Funzione strumentale	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 e ne garantisce l'abilitazione; Comunicare al DS e al DSGA l'elenco dei docenti abilitati all'uso delle aule informatiche; Comunicare ai docenti e agli studenti le procedure per il corretto utilizzo degli strumenti;
DPO DPO (Data Protection Officer)	Coadiuva il Responsabile della Gestione del Firewall nella gestione del Firewall della scuola per la parte di rete didattica; Redigere un report annuale che includa le azioni svolte nell'ambito del proprio incarico. Informare e fornire consulenza al titolare del trattamento; Sorvegliare l'osservanza del regolamento e di altre disposizioni dell'Unione o degli Stati membri, relative alla protezione dei dati;

	Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne l'attuazione; Cooperare con l'autorità di controllo; Fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento.
Referente Privacy	supporta il DS e la segreteria nel diffondere e mettere in atto quanto previsto dalla normativa sulla privacy
L'Animatore Digitale ed il Team Digitale	Promuovere azioni di sensibilizzazione/formazione per un uso consapevole delle nuove tecnologie e della rete; Promuovere l'uso delle nuove tecnologie nella didattica; Verifica attraverso survey periodici le necessità formative dei docenti; Coordinare la partecipazione ad eventi inerenti lo sviluppo delle competenze digitali degli utenti della scuola;
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
I docenti	Inserire tematiche legate alla sicurezza online in tutti gli aspetti del programma di studi e di altre attività scolastiche secondo le indicazioni contenute nel curricolo digitale di Istituto; Supervisionare e guidare gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono la tecnologia online; Mettere in atto i passaggi riportati nella procedura per il trattamento di casi sospetti/evidenti legati al cyberbullismo Mettere in atto norme, procedure e regolamenti per il corretto uso delle tecnologie al servizio della didattica Comprendere e contribuire a promuovere politiche di sicurezza ; Essere consapevoli dei problemi di sicurezza online connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili;

	Monitorare l'uso di dispositivi tecnologici in dotazione alle proprie aule e attuare politiche e le procedure scolastiche per quanto riguarda questi dispositivi; Garantire che le comunicazioni digitali con gli studenti dovrebbero essere a livello professionale e solo attraverso i sistemi scolastici, non attraverso meccanismi personali, per esempio mail, telefoni cellulari, ecc.
Referenti Bullismo e Cyberbullismo	Mettere in atto i passaggi riportati nella procedura per il trattamento di casi evidenti/sospetti legati al Cyberbullismo interagendo con i diversi attori a seguito di opportune valutazioni
Team Cyber bullismo e Team per L'emergenza Bullismo	Supervisionare l'acquisizione e l'archiviazione delle autorizzazioni a garanzia che i dati pubblicati sul sito siano tutelati secondo le norme vigenti; Coadiuvare i referenti nel mettere in atto i passaggi riportati nella procedura per il trattamento di casi evidenti/sospetti legati al Cyberbullismo;
Commissione Regolamento di Istituto	Aggiornare e pubblicare Regolamento e la e-Safety Policy sul sito della scuola Diffondere la Safety ePolicy e i Regolamento di Istituto attraverso documenti informativi
OPT (Operatore Psicopedagogico Territoriale	Fornisce supporto alle attività del Team e del DS Gestisce lo sportello di ascolto per genitori e studenti
Il personale scolastico (personale ATA o personale di supporto alla scuola)	Comprendere e contribuire a promuovere politiche di sicurezza ; Essere consapevoli dei problemi di sicurezza online connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili; Usare comportamenti sicuri, responsabili e professionali nell'uso della tecnologia; Segnalare alterazioni negli strumenti assegnati alle aule e attuare politiche e le procedure scolastiche per quanto riguarda questi dispositivi; Segnalare qualsiasi abuso sospetto o problema ai responsabili della sicurezza online
Gli alunni	Comprendere e contribuire a promuovere politiche di sicurezza ; Essere consapevoli dei problemi di sicurezza online connessi con l'uso di telefoni cellulari, fotocamere e

	dispositivi portatili; Usare comportamenti sicuri, responsabili e professionali nell'uso della tecnologia; Segnalare alterazioni negli strumenti assegnati alle aule e attuare politiche e le procedure scolastiche per quanto riguarda questi dispositivi; Segnalare qualsiasi abuso sospetto o problema ai responsabili della sicurezza online
I genitori	Conoscere e capire la politica della scuola sull'uso di immagini e il cyberbullismo; Capire l'importanza di adottare buone pratiche di sicurezza online quando si usano le tecnologie digitali fuori dalla scuola; Assumersi la responsabilità di conoscere i benefici e i rischi di utilizzo di Internet e di altre tecnologie in modo sicuro, sia a scuola che a casa. Sostenere la scuola nel promuovere la sicurezza online e approvare l'accordo di E Safety Policy con la scuola contenuto all'interno del patto di corresponsabilità, facendosi parte attiva dell'attuazione dei contenuti dello stesso; Leggere, comprendere e controfirmare il suddetto accordo; Accedere al sito Web della scuola e al registro ARGO della scuola in conformità con quanto stabilito dalla stessa

I nomi e cognomi delle figure di riferimento per l'attuazione del presente documento sono aggiornati con cadenza annuale in accordo alla normativa scolastica e sono consultabili all'interno del sito della scuola nella sezione denominata "La scuola" https://www.iccasteldaccia.edu.it/docenti-referenti/ .

1.3 - Un’informativa per i soggetti esterni che erogano attività educative nell’ Istituto

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 presavisione e adesione).

1.4 - Condivisione e comunicazione dell’e-Policy all’intera comunità scolastica

Il documento di e-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.
L’e-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola https://www.iccasteldaccia.edu.it/e-safety-policy-distituto/ ;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all’inizio dell’anno scolastico;
- sul Registro elettronico area “Bacheca”;
- Una versione semplificata è resa fruibile in diversi punti dell’Istituto in prossimità delle aule

specifiche (laboratori) e delle aule didattiche;

- Nel corso di incontri specifici indirizzati a docenti/Personale scolastico/genitori/studenti/sse;
- Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

1.5 - Gestione delle infrazioni alla ePolicy

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.
Al fine di garantire la gestione il più possibile corretta, l'Istituto attua le seguenti strategie:
Il Dirigente Scolastico si riserva, sentiti i responsabili, di limitare l'accesso e l'uso della rete interna (intranet) ed esterna (internet) secondo i normali canali di protezione presenti nei sistemi operativi e attraverso il Firewall scolastico. Si adopera per evitare comportamenti che non rientrano nelle norme che il Collegio dei Docenti delinea in proposito, come:

- scaricare file video-musicali protetti da copyright utilizzando strumenti e reti scolastiche;
- visitare siti non necessari ad una normale attività didattica;
- alterare i parametri di protezione dei computer in uso;
- utilizzare la rete per interessi privati e personali che esulano dalla didattica;
- non rispettare le leggi sui diritti d'autore;
- navigare sui siti non accettati dalla protezione interna della scuola.

Disposizioni, comportamenti, procedure:

- il sistema informatico è periodicamente controllato dai responsabili (DSGA e Funzione strumentale per le nuove tecnologie)
- la scuola può controllare periodicamente i file utilizzati, i file temporanei e i siti visitati da ogni macchina;
- è vietato installare e scaricare da internet software non autorizzati;
- al termine di ogni collegamento la connessione deve essere chiusa;
- verifiche antivirus sono condotte periodicamente sui computer e sulle unità di memorizzazione di rete
- l'utilizzo di dispositivi di memoria esterna (chiavi USB, Hard disk) personali deve essere autorizzato dal docente e solo previa scansione antivirus per evitare qualsiasi tipo di infezione alla rete di Istituto
- la scuola si riserva di limitare il numero di siti visitabili e le operazioni di download attraverso il Firewall
- il materiale didattico dei docenti può essere messo in rete, anche su siti personali collegati all'Istituto, sempre nell'ambito del presente regolamento e nel rispetto delle leggi.

La scuola prenderà tutte le precauzioni necessarie per garantire la sicurezza on-line. Tuttavia, a causa della scala internazionale collegata ai contenuti internet, la disponibilità di tecnologie mobili e velocità di cambiamento, non è possibile garantire che il materiale non idoneo apparirà mai su un computer della scuola o dispositivo mobile. Né la scuola,

né l'autorità locale può assumersi la responsabilità per il materiale accessibile o le conseguenze di accesso a internet.
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 (coordinatore di classe, DS, responsabile cyberbullismo/team cyberbullismo, DS, genitori).
In base alla tipologia e gravità dell' infrazione l'Istituto intende procedere come segue

TIPOLOGIA DI INFRAZIONE	PROVVEDIMENTI	FIGURE COINVOLTE
Atteggiamenti intimidatori verso gli altri (reali e virtuali)	Richiamo annotazione sul registro di classe; Incontri con gli alunni coinvolti; Discussione condivisa in classe; Informare coinvolgere genitori Responsabilizzare gli alunni coinvolti; Rinegoziare le regole condivise; Richiamo e annotazione sul registro; Incontri con gli alunni coinvolti; Convocazione dei genitori e riparazione del danno;	Dirigente Scolastico Referente Docenti Genitori Psicopedagogist
Danni alle strutture/attrezzature scolastiche	Richiamo e annotazione sul registro; Condurre gli alunni alla riflessione sull'accaduto In caso di danni a persone o cose, comunicazione ai genitori per il risarcimento stabilito	Dirigente Scolastico Referente Docenti Genitori Psicopedagogist

Gli interventi di tipo educativo che l'IC Casteldaccia potrà mettere in atto vedranno il coinvolgimento delle seguenti figure: Team Per il Cyberbullismo , Docenti, Genitori, Alunni Psicopedagogisti. Di seguito riportiamo esempi di tali interventi:

1. Incontri con gli alunni coinvolti,
2. contrasto all'isolamento della vittima,
3. percorsi educativi di recupero,
4. interventi e discussioni in classe
5. informazione e coinvolgimento dei genitori
6. promozione del miglioramento delle relazioni tra coetanei e del clima scolastico
7. responsabilizzazione degli alunni coinvolti
8. richiamo alle regole di comportamento del singolo/della classe
9. sportello d'ascolto

10. eventuale trasferimento in altra classe.

Al personale e agli alunni saranno date informazioni sulle infrazioni in uso e le eventuali sanzioni. Le suddette sanzioni possono includere uno o più punti tra quelli riportati di seguito e verranno assegnate in base alla tipologia e alla gravità dell'infrazione dal Consiglio di Classe, dal Dirigente e dal team a supporto dei referenti per Bullismo e Cyberbullismo:

1. informare il docente della classe, il docente responsabile della sicurezza in rete (Referente Cyberbullismo/Team cyberbullismo), il Dirigente Scolastico;
2. informare i genitori o i tutor;
3. il ritiro del cellulare fino a fine giornata;
4. la comunicazione alle autorità component (servizi sociali, forze dell'ordine);
5. informare le figure responsabili della sicurezza online (Responsabile rete didattica e referente Workspace) e il Referente per il Cyberbullismo/team cyberbullismo, riguardo infrazioni relative all'uso della piattaforma scolastica (ad es. incontri online su meet, email…)
6. Denunce di bullismo on-line saranno trattate in conformità con la legge attuale;
7. Reclami relativi alla protezione dei bambini saranno trattati in conformità alle procedure di protezione dell'infanzia.
8. partecipazione ad esperienze didattiche finalizzate
9. produzione di elaborati in relazione al problema specifico
10. richiamo scritto sul registro di classe.
11. sospensione temporanea dalle attività didattiche
12. Risarcimento economico dei danni materiali eventualmente arrecati in favore della comunità scolastica;

1.6 - Integrazione dell'e-Policy con Regolamenti esistenti

Il Regolamento dell' IC Casteldaccia viene aggiornato con specifici riferimenti all'e-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto. Il documento di e-policy, aggiornato annualmente, è parte integrante del Regolamento di Istituto di cui costituisce un allegato.

1.7- Monitoraggio dell'implementazione della e-Policy e suo aggiornamento

L'e-policy viene aggiornata periodicamente 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 Gruppo di Supporto al progetto che si fanno carico di raccogliere le necessità da parte dei diversi utenti. Le modifiche vengono discusse con tutti i membri del personale docente riuniti in Collegio ed approvate.

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

Il nostro piano d'azioni

Piano d'azione

Gli interventi di comunicazione/condivisione nel corso dell'a.s. 2020-21 sono stati piuttosto limitati a causa delle modifiche imposte alle attività dall'emergenza Covid. Tuttavia l'IC Casteldaccia, che dal 2018 ha predisposto il documento di e-policy, ha svolto regolare divulgazione dei contenuti del documento attraverso i canali che sono stati attivati:

- il sito web della scuola all'interno dell'area dedicata al regolamento
- il sito gestito dall'Animatore digitale e il suo Team "Didattica innovativa". All'interno di questo sito esiste uno spazio specifico per gli aspetti legati alla sicurezza in rete e l'uso delle tecnologie.
- Circolari per docenti, studenti, genitori
- Attraverso la comunicazione effettuata dai docenti nelle diverse classi in riferimento all'attuazione del Regolamento di Istituto e delle norme comportamentali specifiche da tenere per l'uso delle nuove tecnologie (doc. e-policy)
- Realizzazione di almeno un incontro con personale specializzato per comunicare i contenuti dell'e-policy
- Realizzazione di almeno un incontro per la divulgazione dell'e-policy effettuato nel corso dell'anno a studenti/docenti/genitori
- Periodicamente (fine anno e inizio anno scolastico, salvo ulteriori necessità specifiche) i docenti che si occupano della revisione del documento raccolgono i suggerimenti da parte di docenti, studenti e genitori e apportano le modifiche al documento che vengono valutate necessarie condividendo le decisioni prese con il DS e il DSGA. Tali modifiche vengono successivamente condivise con il Collegio dei Docenti e con il Consiglio di Istituto.

Azioni da svolgere nei prossimi 3 anni:

- Organizzare almeno un incontro volto a presentare il progetto e consultare i docenti dell'Istituto per la stesura aggiornamento dell'e-Policy;
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse e degli strumenti disponibili in piattaforma per l'approfondimento di specifiche tematiche relative alla sicurezza rivolto agli studenti/genitori;
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse e degli strumenti disponibili in piattaforma per l'approfondimento di specifiche tematiche relative alla sicurezza rivolto ai docenti;

Capitolo 2 - Formazione e curricolo

2.1- Curricolo sulle competenze digitali per gli studenti

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 curricolo digitale che è stato redatto e approvato dal Collegio dei docenti nel corso dell’as. 2020-21 e che viene riportato in allegato (https://www.iccasteldaccia.edu.it/wp-content/uploads/2020/11/Curricolo-digitale-IC-Casteldaccia.pdf). Alcuni aspetti formativi sono inoltre inerenti il curriculo 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 (vedi sito web dell’IC Casteldaccia)

2.2 - Formazione dei docenti sull’utilizzo e l’integrazione delle TIC (Tecnologie dell’Informazione e della Comunicazione) nella didattica

È fondamentale che i docenti tutti siano formati ed aggiornati sull’uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo. Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti. A tale scopo l’IC Casteldaccia promuove attraverso i canali attivi (sito web, circolari, comunicazioni interne) tutte le iniziative formative disponibili sul territorio provinciale (Ambito 21), Regionale, Nazionale e internazionale (progetti Erasmus+). Periodicamente l’AD effettua un monitoraggio in modo da aggiornare l’analisi dei bisogni formativi da cui partire per predisporre in accordo con le figure di riferimento e il DS eventuali attività formative che rientrano all’interno delle mansioni dell’AD e del suo Team.

L’IC Casteldaccia è sede certificata da Certipass per la realizzazione di corsi di formazione specifici con rilascio di certificazione Eipass. L’IC Casteldaccia promuove l’aggiornamento continuo delle competenze digitali dei docenti attraverso la promozione di percorsi specifici per la didattica con le TIC (Certificazione Teacher, LIM, Tablet) per le

quali l'AD in qualità di Formatore certificato Eipass fornisce supporto su richiesta.

L'IC Casteldaccia da anni propone interventi finalizzati allo sviluppo delle competenze digitali di studenti e genitori portando avanti iniziative promosse dal MIUR ricorrendo a finanziamenti della Comunità Europea (FONDI FSE PON, PNSD). Tali interventi vengono di volta in volta programmati dal DS, dall'AD e dal TEAM digitale, dalle funzioni a supporto del DS (Gruppo NIV), tenendo conto di un'analisi dei bisogni che viene elaborata ad inizio anno scolastico da parte dell'AD di Istituto sentite le parti coinvolte.

2.3 - Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avviene tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (Animatore Digitale, Referente Bullismo e Cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

2.4. - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'e-Policy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" (vedi Allegato G del Regolamento di Istituto) e attraverso una sezione dedicata sul sito WEB dell'IC Casteldaccia nell'area gestita direttamente dall'AD denominata "Tecnologie digitali" alla sezione "sicurezza". In quest'area in particolare è possibile trovare i link agli eventi promossi da Generazioni connesse per genitori e docenti e i documenti all'approfondimento di problemi connessi alla sicurezza on line (https://sites.google.com/istitutocomprensivocasteldaccia.net/didattica-innovativa/home-pag).

Il nostro piano d'azioni

Piano di azioni

AZIONI sviluppate nell'anno scolastico in corso

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare e promuovere per il corpo docente incontri formativi e informativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi e informativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Promuovere ed organizzare incontri con esperti per i docenti sulle competenze digitali.
- Promuovere ed organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi)

- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi ed informativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi ed informativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT della e nella scuola

3.1 - Protezione dei dati personali

“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.

La protezione dei dati personali è un diritto fondamentale dell’individuo ai sensi della Carta dei diritti fondamentali dell’Unione europea (art. 8), tutelato dal 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).

Anche le scuole, quindi, hanno oggi l’obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato in vigore il 19 settembre dello stesso anno.

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 definitivi, 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;

Personale esterno

Per quanto attiene il personale esterno occorre fare riferimento a quanto già espresso nel

paragrafo 1.3 in materia di tutela della privacy dei minori rispettando quanto riportato nell'informativa. 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.

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).

3.2 - 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.

3.2.1 Accesso ad internet: filtri, antivirus e sulla navigazione

L'Istituto dispone di 2 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.
Il plesso della primaria è anch'esso dotato di linea internet il cui accesso è gestito da firewall.

Rete segreteria

L'accesso alla rete della segreteria è consentito esclusivamente dalle postazioni fisse 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. Tutti i pc della segreteria sono collegati al server della segreteria del quale il DSGA effettua periodicamente il backup dei dati.

Rete didattica

Plesso scuola primaria: 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 è possibile previo inserimento di una password di accesso alla rete scolastica. Tale password è comunicata ai docenti che avranno cura di custodirla garantendone la segretezza.

Sede centrale scuola secondaria (via C. Cattaneo):

La rete didattica della scuola secondaria è accessibile solo agli utenti identificati da user e password e protetta da Firewall. I docenti profilati sono responsabili delle proprie credenziali di accesso. 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. 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. Ogni docente assegna un voucher allo studente all'atto dell'attività. 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- 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 sono dotati di pw e us con funzioni di amministratore che vengono comunicate, ad uso esclusivo dei docenti , su richiesta degli stessi alla funzione strumentale. Grazie a tale account sarà possibile scaricare gli applicativi indispensabili per la didattica. Tale operazione deve comunque essere concordata con la funzione di riferimento. 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.

Accesso studenti

L'accesso da parte degli studenti agli strumenti della scuola è consentito esclusivamente con l'account denominato "studente" che impedisce di apportare alla macchina qualunque modifica alla configurazione.

Sui dispositivi delle aule informatiche l'archiviazione dei dati è eseguita sul server delle aule. Ogni utente segue la procedura di archiviazione prevista per l'uso della strumentazione. Sia per le postazioni delle aule che per le postazioni mobili non è previsto alcun servizio di backup dei file, 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.

3.3 - 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.

3.3.1 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.

Per quanto attiene 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 dll'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, tools o siti che richiedono profilazione da parte degli utenti

Ai docenti e agli studenti è consentito anche l'uso di altre piattaforme didattiche, tools o siti per la realizzazione di attività specifiche della propria disciplina purché la profilazione degli studenti avvenga attraverso la creazione di classi nelle quali gli studenti vengono profilati con un nickname dal docente. Nel caso in cui l'accesso a piattaforme esterne fosse regolato da sistemi di autenticazione che richiedono l'uso di registrazione tramite email tale passaggio sarà effettuato dal genitore con il proprio account previa presa visione dell'informativa specifica della piattaforma.

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.

3.3.2 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.

3.3.3 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. 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. 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. L'Istituto ha attualmente in uso Google Workspace for education avendo registrato un proprio dominio (istitutocomprensivocasteldaccia.net). All'interno di quest'area vengono create classi virtuali (google classroom) e gli studenti e i docenti possono comunicare in modo sicuro e protetto. All'interno di drive sono state create repository per lo scambio di materiali e documenti da parte dei docenti.
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 regolamentoo sul registro Argo, sul quale i genitori appongono un flag per presa visione e autorizzazione (Allegato 6).

3.3.4 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 cura il proprio giornalino scolastico attraverso la pagina web promossa da Repubblica@scuola (https://scuola.repubblica.it/sicilia-palermo-icistitutocomprensivocasteldaccia/) il cui accesso agli studenti per la pubblicazione di articoli, foto e disegni o la partecipazione ad eventi è protetto da us e pw gestiti dai docenti caporedattori del progetto. Ogni studente all'atto di partecipazione consegna una liberatoria con la firma dei genitori/tutori emessa dal gruppo Gedi. Tale documento viene conservato agli atti per la durata della partecipazione al progetto dal docente (caporedattore) che ne cura l'inserimento nel portale. Le liberatorie verranno archiviate in un'apposita cartella depositata negli uffici della segreteria alunni. I docenti e di genitori sono altresì ritenuti responsabili dei materiali pubblicati da parte degli studenti. Annualmente il DS incarica un docente quale referente del progetto Repubblica@scuola.
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).
I coordinatori delle classi e tutti i docenti che, nel corso di attività didattiche specifiche svolte in orario scolastico ed extrascolastico, pubblichino 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.**

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle 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.
La presente e-Policy contiene 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 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.

3.4.1 - Studenti

Il Regolamento di Istituto vieta l'uso del cellulare ad eccezione di specifiche attività didattiche svolte sotto la supervisione del docente che ne autorizza l'uso in byod. In questi casi agli studenti è consentito l'accesso ad Internet da propri dispositivi 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).

Gli studenti potranno altresì utilizzare i propri strumenti ricorrendo alla rete personale sempre sotto la sorveglianza del personale docente ed esclusivamente per attività didattiche.

3.4.2 - 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.

3.4.3 - 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.

Il nostro piano d'azioni

AZIONE da svolgere nel corso dell'a.s. in corso:

Tutti i docenti delle classi organizzano annualmente nell'ambito delle proprie attività curriculari un'attività volta a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity) in accordo con quanto previsto dal curricolo di ed. civica e dal curricolo digitale di Istituto. I prodotti realizzati come risultato dell'attività saranno condivisi nella sezione dedicata all'educazione civica della scuola e nella sezione dedicata a Generazioni Connesse.

- AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).

Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere/integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.

Capitolo 4 - Rischi on line: conoscere, prevenire e rilevare

4.1 - Sensibilizzazione e Prevenzione

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 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 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.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

La legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", nell'art. 1, comma 2, definisce il cyberbullismo:

"Qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo".

La stessa legge e le relative Linee di orientamento per la prevenzione e il contrasto del cyberbullismo indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo.

Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;

- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente** per le iniziative di prevenzione e contrasto che:
  - Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo, anche in accordo con il Referente alla Legalità dell'Istituto. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
  - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

4.3 - Hate speech: che cos'è e come prevenirlo

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

A tale scopo l'IC Casteldaccia:

- si impegna a promuovere la partecipazione ad iniziative specifiche proposte dal MIUR e da Associazioni/Enti specifici (Generazioni- connesse, TelefonoAzzurro, #iosonoqui…) che si occupano del contrasto dell'Hate-speeching.
- I docenti delle classi svolgeranno nell'ambito delle iniziative previste dal curricolo di ed. civica e curriculo digitale a svolgere un'attività specifica finalizzata a promuovere la riflessione su questa tematica.

4.4 - Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

A tale scopo l'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale (es. esperimenti sociali, settimane di monitoraggio uso rete, etc) attivati attraverso i canali istituzionali presenti sul territorio locale e nazionale.

4.5 – Sexting

Il “sexting” è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti mediali sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

4.6 - Adescamento online

Il grooming (dall’inglese “groom” - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di teen dating (siti di incontri per adolescenti). Un’eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

In Italia l’adescamento si configura come reato dal 2012 (art. 609-undecies – l’adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell’adescamento.

A tale scopo l’IC Casteldaccia si impegna a promuovere iniziative finalizzate a comunicare i rischi specifici di grooming attraverso la realizzazione di almeno un incontro aperto ai docenti, ai genitori e al personale ATA, su tale tematica con personale specifico (allo scopo ad esempio di far conoscere statistiche e testimonianze del fenomeno a livello territoriale, nazionale ed internazionale)

4.7 – Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, concrete o simulate o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

La legge n. 269 del 3 agosto 1998 “Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù”, introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella legge n. 38 del 6 febbraio 2006 “Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet”, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest’ultima, introduce, tra le altre cose, il reato di “pornografia minorile virtuale” (artt. 600 ter e 600 quater c.p.) che si verifica quando il

materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 - Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione "Segnala contenuti illegali" (Hotline).

Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico).

Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.

- - Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale (realizzazione di attività specifiche da svolgere in classe con gli studenti nell'ambito delle attività progettate dal consiglio di classe).

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).

- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

  Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

-

-

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

Per i casi che non rientrano in queste categorie resta inteso che i Referenti e il team di supporto sono a disposizione per raccogliere le segnalazioni di docenti, alunni e genitori.

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. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).

Nelle procedure:

- sono indicate le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso.
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

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. Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

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/lle 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 la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via 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 a 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.

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale 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**.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due 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.
- **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.

  Per tutti i dettagli fate riferimento 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 gestito dal Referente e dal gruppo di supporto;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti (OPT di Istituto);
- docente referente e gruppo di supporto per le segnalazioni.
- Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

5.3. - Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi ad altre figure, enti, istituzioni e servizi presenti sul territorio qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.
Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse “Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all’utilizzo delle tecnologie digitali da parte dei più giovani” (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell’offrire una guida competente ed un supporto in tale percorso. A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all’utilizzo di Internet può presentare:

- Comitato Regionale Unicef: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell’infanzia.
- Co.Re.Com. (Comitato Regionale per le Comunicazioni): svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- Ufficio Scolastico Regionale: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all’uso di Internet.
- Polizia Postale e delle Comunicazioni: accoglie tutte le segnalazioni relative a comportamenti a rischio nell’utilizzo della Rete e che includono gli estremi del reato.
- Aziende Sanitarie Locali: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- Garante Regionale per l’Infanzia e l’Adolescenza e Difensore Civico: segnalano all’Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono

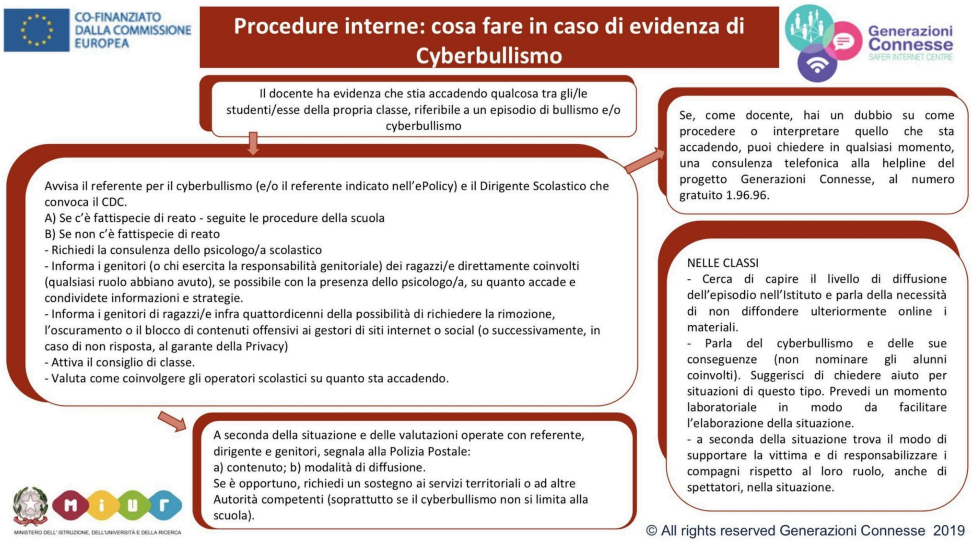
informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.

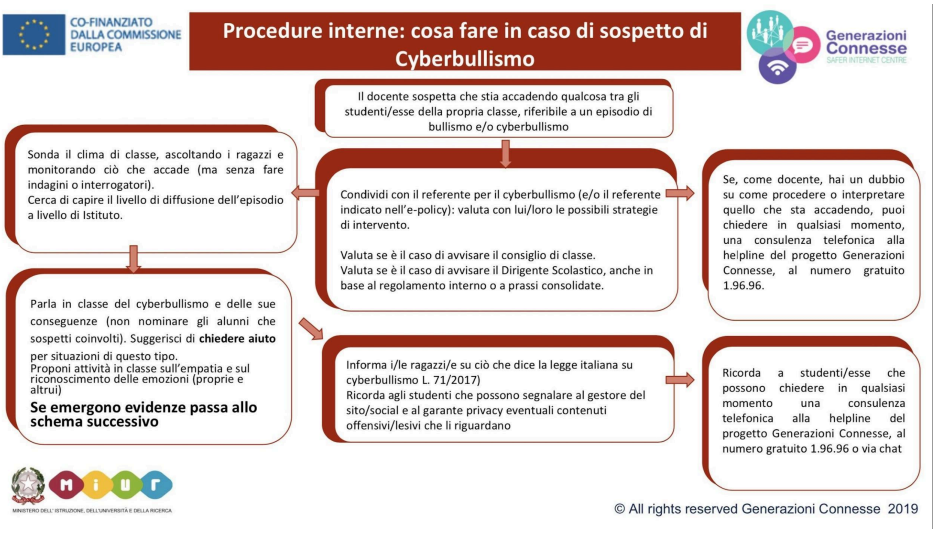
- Tribunale per i Minorenni: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4 - Allegati con le procedure

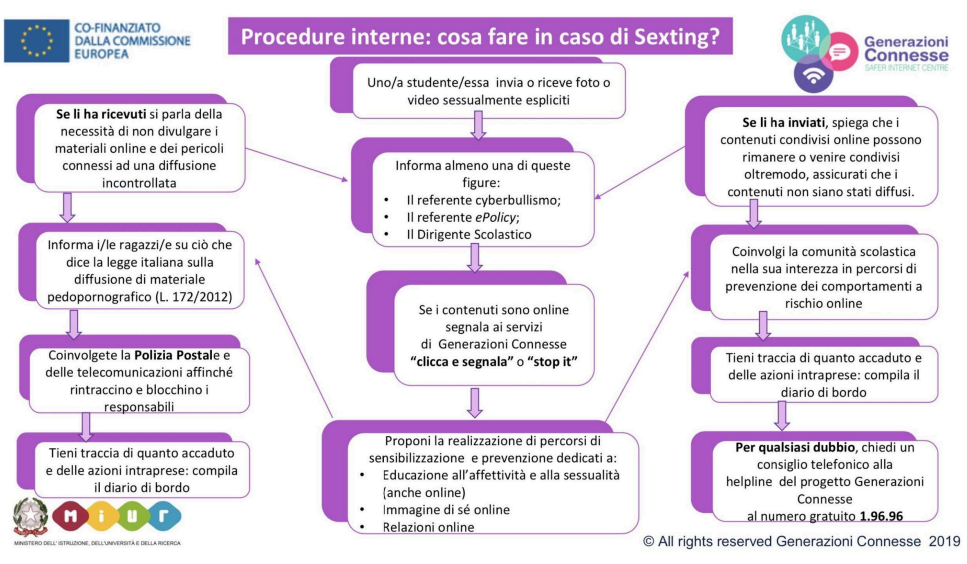
Si riportano di seguito gli schemi delle diverse procedure da seguire in caso di episodi di cyberbullismo, sexting, adescamento online e le eventuali modalità di segnalazione ad enti esterni.

Procedure interne: cosa fare in caso di sospetto di**Cyberbullismo?**

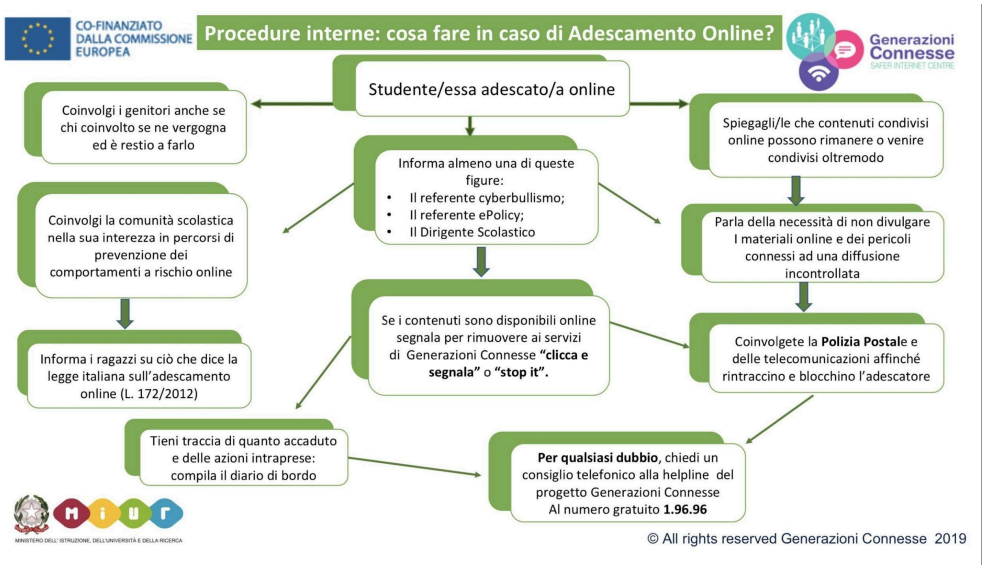




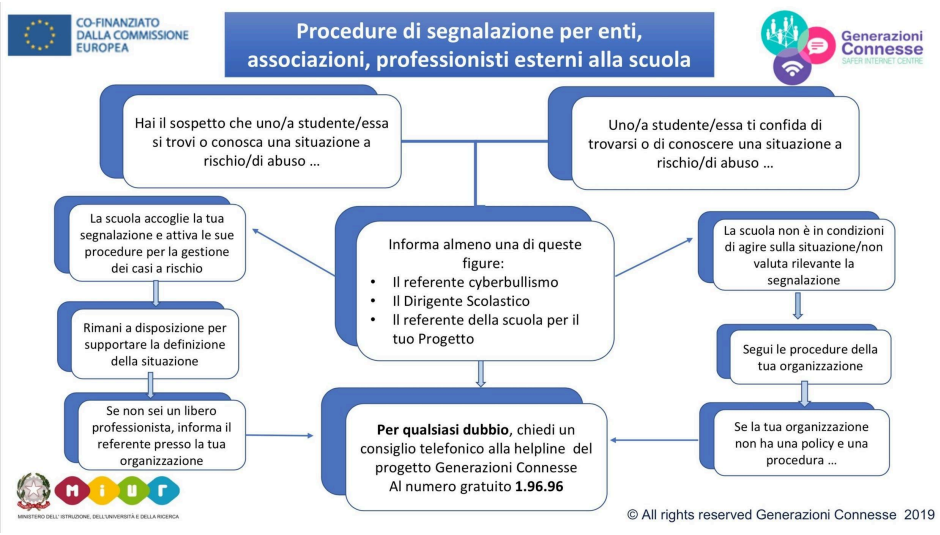
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola



Siti utili

iGloss@ 1.0 l’ABC dei comportamenti devianti online

Elenco reati procedibili d’ufficio

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
  - Allegato 8 ePolicy: Modulo per la segnalazione delle situazioni di rischio
  - Allegato 9 ePolicy: Diario di Bordo

Il presente documento è stato approvato dal Consiglio di Istituto in data 24/05/2024.

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

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

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'E-policy 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

MINISTERO DELLA PUBBLICA ISTRUZIONE
Istituto Comprensivo Statale
"CASTELDACCIA"
Via Carlo Cattaneo N.80 – 90014 CASTELDACCIA (PA)
C.F.: 90007610828 – Cod. Min.: PAIC84200X
☎ 091-954299 – Fax 091-9100217

Agli assistenti amministrativi ATA

Al DSGA

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

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 atti ità 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 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 atti ità:

Area didatti a:

- **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 didatti he.**

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

- **atti ità di protocollazione e smistamento alle aree competenti degli atti in ingresso all'Istituto, siano essi recapitati in forma cartacea che elettronica (PEC, mail, eccetera);**
- **atti ità di protocollazione ed invio ai destinatati 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'atti ità 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 legitti i, ed utilizzarli solo per operazioni di trattamento compatibili con le finalità connesse all'atti ità 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 Protezioni 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 atti ità che comporti il trattamento dei dati personali.**

MISURE OPERATIVE SPECIFICHE ALL'UTILIZZO DI TECNOLOGIE INFORMATICHE

- **scegliere per i diversi software gestionali (area personale, area didatti a, 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**

didatti a, 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 documenti 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 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"
Via Carlo Cattaneo N.80 – 90014 CASTELDACCIA (PA)
C.F.: 90007610828 – Cod. Min.: PAIC84200X
☎ 091-954299 – Fax 091-9100217

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 atti ità 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 atti ità 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 Protezioni 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"
Via Carlo Cattaneo N.80 – 90014 CASTELDACCIA (PA)
C.F.: 90007610828 – Cod. Min.: PAIC84200X
☎ 091-954299 – Fax 091-9100217

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 atti ità 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 atti ità:

- **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 legitti i;**
- **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 legitti amente 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 atti ità 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 atti ità 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@arub

apec.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"
Via Carlo Cattaneo N.80 – 90014 CASTELDACCIA (PA)
C.F.: 90007610828 – Cod. Min.: PAIC84200X
☎ 091-954299 – Fax 091-9100217

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 atti ità 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 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:

- **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 atti ità 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 legitti i, ed utilizzarli solo per operazioni di trattamento compatibili con le finalità connesse all'atti ità 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 Protezioni 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@arub
apec.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



MINISTERO DELLA PUBBLICA ISTRUZIONE
Istituto Comprensivo Statale
"CASTELDACCIA"
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:

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 pixellizzazione 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 qualifica 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 _____

MINISTERO DELLA PUBBLICA ISTRUZIONE
Istituto Comprensivo Statale ad indirizzo musicale
"*CASTELDACCIA* "
Via Carlo Cattaneo N.80 – 90014 CASTELDACCIA (PA)
C.F.: 90007610828 – Cod. Min.: PAIC84200X 091-954299– Fax 091-9100217
e-mail paic84200x@istruzione.it

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

1. L'Istituto mette a disposizione per l'a.s. 2023/2024 ai propri docenti, studenti e personale ATA 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.
2. Si esclude espressamente l'applicazione del presente regolamento alle sedute degli organi collegiali (OO.CC.) aventi carattere deliberativo di cui al D.Lgs. 297/1994, compresi gli scrutini.
3. 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.
4. Il regolamento si applica a tutti gli utenti titolari di un account.
5. 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.
6. 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 personale A.T.A. 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.:

1. 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.
2. Gli account fanno parte del dominio di cui l'Istituto è proprietario indicato nel paragrafo "definizioni".
3. Nel caso di smarrimento della password, l'utente potrà rivolgersi direttamente all'Amministratore della piattaforma scolastica.
4. 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.

5. 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.
6. L'utente si impegna a collegarsi 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.
7. L'utente s'impegna ad utilizzare l'account esclusivamente per le finalità indicate al precedente Art. 3.
8. 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.
9. 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.
10. 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.
11. È vietato immettere in rete materiale che violi diritti d'autore, o altri diritti di proprietà intellettuale o industriale o che costituisca concorrenza sleale.
12. L'utente s'impegna a non procedere all'invio massivo di mail non richieste (spam).
13. 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.
14. 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

MINISTERO DELLA PUBBLICA ISTRUZIONE
Istituto Comprensivo Statale ad indirizzo musicale
"*CASTELDACCIA* "
Via Carlo Cattaneo N.80 – 90014 CASTELDACCIA (PA)
C.F.: 90007610828 – Cod. Min.: PAIC84200X 091-954299 –
Fax 091-9100217 e-mail paic84200x@istruzione.it

Spett.le
Prof.ssa Lorena Ragusa
C.F. RGSLRN76P62G273Q

ALLEGATO 1 AL REGOLAMENTO PIATTAFORMA GOOGLE WORKSPACE FOR EDUCATION

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, negandolo 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. 10 ore a euro 19,25

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

MINISTERO DELLA PUBBLICA ISTRUZIONE
Istituto Comprensivo Statale ad indirizzo musicale
"CASTELDACCIA"
Via Carlo Cattaneo N.80 – 90014 CASTELDACCIA (PA)
C.F.: 90007610828 – Cod. Min.: PAIC84200X 091-954299 –
Fax 091-9100217 e-mail paic84200x@istruzione.it

Alle famiglie coinvolte

ALLEGATO 2 AL REGOLAMENTO PIATTAFORMA GOOGLE WORKSPACE FOR EDUCATION

DISPOSIZIONI OPERATIVE E INFORMATIVA DATI PERSONALI

Google workspace for education

FAMIGLIE E STUDENTI

per l'utilizzo dei tool di didattica digitale (eLearning))

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 è assolutamente vietato divulgarlo 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.

Luogo e Data _____

Il Dirigente Scolastico

MINISTERO DELLA PUBBLICA ISTRUZIONE
Istituto Comprensivo Statale ad indirizzo musicale
"*CASTELDACCIA* "
Via Carlo Cattaneo N.80 – 90014 CASTELDACCIA (PA)
C.F.: 90007610828 – Cod. Min.: PAIC84200X 091-954299 –
Fax 091-9100217 e-mail paic84200x@istruzione.it

Alle famiglie coinvolte
Ai docenti

ALLEGATO 3 AL REGOLAMENTO PIATTAFORMA GOOGLE WORKSPACE FOR EDUCATION

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 (eLearning)**

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 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.

  c). Nella Programmazione di Scuola Primaria, le riunioni di due ore, martedì dalle 14.30 alle 16.30, vengono svolte on line o in presenza in accordo a quanto previsto dal piano delle attività e comunicate col dirigente scolastico.

  (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 e-lettronico 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 insegnan 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 terapisti, 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.

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.

Luogo e Data _____

Il Dirigente Scolastico

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

MINISTERO DELLA PUBBLICA ISTRUZIONE

Istituto Comprensivo Statale ad indirizzo musicale

"*CASTELDACCIA* "

Via Carlo Cattaneo N.80 – 90014 CASTELDACCIA (PA)

C.F.: 90007610828 – Cod. Min.: PAIC84200X 091-954299 – Fax 091-9100217

e-mail paic84200x@istruzione.it

Descrizione dell'episodio o del problema		
Soggetti coinvolti	Vittima/e: 1…….. … Classe: …. 2…….. … Classe: ….	Autore/autrice e sostenitori: 1…….. … Classe: …. 2…….. … Classe: …. 3……..

	3…….. … 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/persone è sostenuto chi ha compiuto l'azione? Quanti compagni supportano la vittima o potrebbero farlo?	
Gli insegnanti sono intervenuti in qualche modo ?		

La famiglia o altri adulti hanno cercato di intervenire ?		
Chi è stato informato della situazione?	□ coordinatore di classe data: □ consiglio di classe data: □ dirigente scolastico data: □ la famiglia della vittima/e data:	□ la famiglia del bullo/i data: □ le forze dell'ordine data: □ altro, specificare:

MODULO PER IL FOLLOW-UP DEI CASI

	AZIONI INTRAPRESE	La situazione è
Aggiornamento 1		□ migliorata □ invariata □ peggiorata Come:
Aggiornamento 2		□ migliorata □ invariata □ peggiorata Come:
Aggiornamento 3		□ migliorata □ invariata □ peggiorata Come:
Aggiornamento 4		□ migliorata □ invariata □ peggiorata Come:
Aggiornamento 5		□ migliorata □ invariata □ peggiorata Come:

CO-FINANZIATO DALLA COMMISSIONE EUROPEA

Allegato 9 ePolicy . Diario di Bordo dei casi

Generazioni Connesse

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?		