# 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.

Le "competenze digitali" sono 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).

In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a 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

1. **Presentazione dell'ePolicy**
    1. Scopo dell'ePolicy
    2. Ruoli e responsabilità
    3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
    4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
    5. Gestione delle infrazioni alla ePolicy
    6. Integrazione dell'ePolicy con regolamenti esistenti
    7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
2. **Formazione e curricolo**
    1. Curricolo sulle competenze digitali per gli studenti
    2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
    3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
    4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
    1. Protezione dei dati personali
    2. Accesso ad Internet
    3. Strumenti di comunicazione online
    4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
    1. Sensibilizzazione e prevenzione
    2. Cyberbullismo: che cos'è e come prevenirlo
    3. Hate speech: che cos'è e come prevenirlo
    4. Dipendenza da Internet e gioco online
    5. Sexting
    6. Adescamento online
    7. Pedopornografia
5. **Segnalazione e gestione dei casi**
    1. Cosa segnalare
    2. Come segnalare: quali strumenti e a chi
    3. Gli attori sul territorio per intervenire
    4. Allegati con le procedure

## 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.

### 1.1 - 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**

**3.3 Strumenti di comunicazione online**

**3.4 Strumentazione personale**

**4. Rischi on line: conoscere, prevenire e rilevare**

1. **Sensibilizzazione e prevenzione**
2. **Cyberbullismo: che cos'è e come prevenirlo**
3. **Hate speech: che cos'è e come prevenirlo**
4. **Dipendenza da Internet e gioco online**
5. **Sexting**
6. **Adescamento online**
7. **Pedopornografia**

5. **Segnalazione e gestione dei casi**

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

**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, s'impegni nell'attuazione e promozione di essa.

**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;**<br>**- Titolarità sul del trattamento dei dati (PPO);**<br>**- Garantire che la scuola utilizzi un Internet Service filtrato approvato, conforme ai requisiti di legge vigenti ;**<br>**- Essere a conoscenza delle procedure da seguire in caso di infrazione della e-Safety Policy;**<br>**- Ruolo di primo piano nello stabilire e rivedere la e-Safety Policy;**<br>**-Ricevere relazioni di monitoraggio periodiche della sicurezza online da parte del responsabile;**<br>**- 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;**<br>**- Promuovere la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica;**<br>**- Garantire che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente per la sicurezza online;**<br>**- Garantire che sia tenuto un registro di incidenti di sicurezza online;**<br>**- Facilitare la formazione e la consulenza per tutto il personale;**<br>**- Coordinare con le autorità locali e le agenzie competenti;**<br>**- Controllare la condivisione di dati personali;**<br>**- Controllare l'accesso a materiali illegali / inadeguati;**<br>**- Controllare probabili azioni di cyberbullismo.** |

| | |
|---|---|
| **Funzione strumentale per le Nuove tecnologie** | **- Coadiuvare il DSGA nella redazione dell'inventario della dotazione tecnologia scolastica;**<br>**- Coadiuvare il DS nelle comunicazioni con il MIUR inerenti il monitoraggio dei beni inventariati a servizio delle aule laboratoriali;**<br>**- 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;**<br>**- Riportare al DS e al DSGA e alla figura di riferimento per il Pronto Soccorso Tecnico eventuali comunicazioni di danneggiamento/furto/malfunzionamento delle attrezzature;**<br>**- Redigere la procedura di utilizzo degli strumenti in dotazione alle aule e vigila sulla mancata osservazione della stessa;**<br>**- Eseguire interventi formativi per i docenti all'uso delle aule informatiche e della strumentazione esistente e ne garantisce l'abilitazione;**<br>**- Comunicare al DS e al DSGA l'elenco dei docenti abilitati all'uso delle aule informatiche;**<br>**- Comunicare ai docenti e agli studenti le procedure per il corretto utilizzo degli strumenti;**<br>**- Coadiuva il Responsabile della Gestione del Firewall nella gestione del Firewall della scuola per la parte di rete didattica;**<br>**- Redigere un report annuale che includa le azioni svolte nell'ambito del proprio incarico.** |
| **DPO (Data Protection Officer)** | **- Informare e fornire consulenza al titolare del trattamento;**<br>**- Sorvegliare l'osservanza del regolamento e di altre disposizioni dell'Unione o degli Stati membri, relative alla protezione dei dati;**<br>**- Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne l'attuazione;**<br>**- Cooperare con l'autorità di controllo;**<br>**- 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 suo Team** | **- Promuovere azioni di sensibilizzazione/formazione per un uso consapevole delle nuove tecnologie e della rete;**<br>**- Promuovere l'uso delle nuove tecnologie nella didattica;**<br>**- Verifica attraverso survey periodici le necessità formative dei docenti;**<br>**- Coordinare la partecipazione ad eventi inerenti lo sviluppo delle competenze digitali degli utenti della scuola;**<br>**- Mettere in atto norme, procedure e regolamenti per il corretto uso delle tecnologie al servizio della didattica;** |
| **Amministratore Firewall** | **- 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 e i docenti.** |

| | |
|---|---|
| **Gli insegnanti** | **- 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;**<br>**- Supervisionare e guidare gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono la tecnologia online;**<br>**- Mettere in atto i passaggi riportati nella procedura per il trattamento di casi sospetti/evidenti legati al cyberbullismo**<br>**- Mettere in atto norme, procedure e regolamenti per il corretto uso delle tecnologie al servizio della didattica**<br>**- Comprendere e contribuire a promuovere politiche di sicurezza ;**<br>**- Essere consapevoli dei problemi di sicurezza online connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili;**<br>**- Monitorare l'uso di dispositivi tecnologici in dotazione alle proprie aule e attuare politiche e le procedure scolastiche per quanto riguarda questi dispositivi;**<br>**- 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 per il 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;**<br>**- Coadiuvare i referenti nel mettere in atto i passaggi riportati nella procedura per il trattamento di casi evidenti/sospetti legati al Cyberbullismo;**<br>**- Coadiuvare l'AD e i referenti al Cyberbullismo nella realizzazione di iniziative di formazione/informazione atte a prevenire un uso scorretto della rete e azioni di Cyberbullismo.** |
| **Commissione Regolamento Istituto** | - Aggiornare e pubblicare Regolamento e la e-Safety Policy sul sito della scuola<br>- Diffondere la e-Safet policy attraverso power point o interventi informativi e quanto attiene il Regolamento di Istituto<br>- Gestisce il Piano di Azione previsto dalla E-policy |
| **OPT (Operatore Psicopedagogico Territoriale)** | **- Fornisce supporto alle attività del Team e del DS**<br>**- 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 ;**<br>**- Essere consapevoli dei problemi di sicurezza online connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili;**<br>**- Usare comportamenti sicuri, responsabili e professionali nell'uso della tecnologia;**<br>**- Segnalare alterazioni negli strumenti assegnati alle aule e attuare politiche e le procedure scolastiche per quanto riguarda questi dispositivi;**<br>**- Segnalare qualsiasi abuso sospetto o problema ai responsabili della sicurezza online;** |

| | |
|---|---|
| **Gli alunni** | **- Leggere, comprendere, ed accettare la e-Safety Policy;**<br>**- Avere una buona comprensione delle capacità di ricerca e la necessità di evitare il plagio e rispettare normative sul diritto d'autore;**<br>**- Capire l'importanza di segnalare abusi, o l'uso improprio o l'accesso a materiali inappropriati;**<br>**- Sapere quali azioni intraprendere se si è vittime o testimoni o se si individuano situazioni di vulnerabilità nell'uso della tecnologia online;**<br>**- Conoscere e capire la politica relativa all'uso dei telefoni cellulari, fotocamere digitali e dispositivi portatili;**<br>**- Conoscere e capire la politica della scuola sull'uso di immagini e il cyberbullismo;**<br>**- Capire l'importanza di adottare buone pratiche di sicurezza online quando si usano le tecnologie digitali fuori dalla scuola;**<br>**- 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.** |
| **I genitori** | **- 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;**<br>**- Leggere, comprendere e controfirmare il suddetto accordo;**<br>**- 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 di 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).

### 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 presa**

**visione e adesione).**

---

# *1.4 - Condivisione e comunicazione dell'ePolicy 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;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

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.

### 1.4 - 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.

**1.5 - Gestione delle infrazioni alla ePolicy**

**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 E FIGURE COINVOLTE**

| | | |
|---|---|---|
| **Atteggiamenti intimidatori verso gli altri (reali e virtuali)** | **Richiamo annotazione sul registro di classe<br>Incontri con gli alunni coinvolti<br>Discussione condivisa in classe<br>Informare coinvolgere genitori<br>Responsabilizzare gli alunni coinvolti<br>Rinegoziare le regole condivise** | **Dirigente Scolastico<br>Referente Docenti<br>Genitori<br>Psicopedagogisti** |
| **Danni e sottrazione materiale altrui** | **Richiamo e annotazione sul registro<br>Incontri con gli alunni coinvolti<br>Convocazione dei genitori e riparazione del danno** | |

| | |
|---|---|
| **Danni alle strutture/attrezzature scolastiche** | **Richiamo e annotazione sul registro<br>Condurre gli alunni alla riflessione sull'accaduto<br>In caso di danni a persone o cose, comunicazione ai genitori per il risarcimento stabilito** |

**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 ad 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'ePolicy con Regolamenti esistenti*

Il Regolamento dell'Istituto Scolastico 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.

### 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 ePolicy 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 saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

### 1.7 - 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 avverrà attraverso la progettazione e implementazione di un curricolo digitale.

#### 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.

**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 avverrà 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.

**2.3 - 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'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

### 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 lo scorso 19 settembre.

In questo paragrafo dell'ePolicy 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 ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali.

### 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 lo scorso 19 settembre.**

**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 liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali.**

**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.**

**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 il personale esterno è tenuto a conservare in modo adeguato tali documenti consegnandoli al docente di riferimento dell'attività condotta che a sua volta ne curerà l'archiviazione secondo quanto previsto per i docenti.**

---

# *3.2 - Accesso ad Internet*

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *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.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *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.*

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE

relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

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.

### 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.**

**(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.

### 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.**

### 3.3.1 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 (Allegato 2). Per la raccolta delle autorizzazioni si rimanda al punto 3.3.2 "Piattaforme didattiche e Google Workspace for Education".**

### 3.3.2 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 nomeutente 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.**

**I docenti prendono visione dell'Informativa sull'Uso di Google Workspace for education e del relativo Regolamento d'uso, pubblicati sul sito della scuola.**

**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 e l'elenco degli account con password, da cambiare dopo il primo accesso.**

**Il modulo firmato sarà consegnato in segreteria prima dell'inizio delle attività didattiche secondo le modalità riportate nell'avviso sul sito della scuola. La segreteria alunni comunicherà l'elenco degli studenti autorizzati ai coordinatori delle classi.**

**Nel caso in cui l'Istituto decida di attivare i servizi aggiuntivi della**

**Piattaforma Google Workspace for education, i genitori dovranno sottoscrivere la dichiarazione liberatoria sull'utilizzo di tali servizi compilando il modulo di consenso disponibile su Argo e consegnandolo ai docenti coordinatori che lo conserveranno presso gli uffici della segreteria alunni in apposite cartelle. Resta inteso che l'attivazione dell'account studente effettuata il primo anno non necessita di ulteriore autorizzazione negli anni successivi. Per l'attivazione e la gestione della piattaforma sono stati stilati i seguenti documenti:**

- **Allegato 2 Informativa all'uso di Google Workspace for Education**
- **Allegato 3 Dichiarazione liberatoria all'uso dei servizi aggiuntivi di Google Workspace for education.**

**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. L'accesso a tali piattaforme potrebbe essere regolato da sistemi di autenticazione che richiedono l'autorizzazione da parte dei genitori, garantendo la massima trasparenza e sicurezza (Allegato 3 - Modulo di autorizzazione all'uso di piattaforme didattiche). In questi casi le autorizzazioni saranno consegnate in cartaceo al docente interessato che le raccoglierà e le consegnerà alla segreteria alunni dove verranno archiviate unitamente ai documenti degli alunni della classe.Resta inteso che l'attivazione dell'account studente effettuata il primo anno non necessita di ulteriore autorizzazione negli anni successivi.**

**3.3.3 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.**

**3.3.4 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 hanno consegnato il relativo modulo di sottoscrizione di liberatoria (Allegato 4 - Modulo consenso uso credenziali ARGO FAMIGLIA). Il modulo sarà anche disponibile sul sito della scuola e potrà essere consegnato in segreteria nei giorni antecedenti l'inizio delle attività didattiche secondo modalità riportate in circolare e nella sez. avvisi.**

### 3.3.5 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 i cui genitori hanno preventivamente autorizzato la scuola all'uso delle immagini dei propri figli attraverso la compilazione dell'apposito modulo autorizzativo (Allegato 5 - Modulo consenso informato foto e video). I moduli firmati saranno raccolti e conservati dalla segreteria alunni secondo le modalità riportate nell'avviso pubblicato con circolare e sul sito della scuola nei gironi precedenti l'inizio delle attività didattiche. L'autorizzazione deve essere rinnovata annualmente.**

**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 la presenza dei consensi informati all'uso dell'immagine da parte del genitore/tutore dello studente minorenne che viene ritratto nella presentazione pubblicata.**

---

# *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 ***ePolicy*** 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 - 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*

**Piano di 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.*

#### 4.1 - 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. 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).

### 4.2 - 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 seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

### 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.

*L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale?*

**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.

**4.5 – 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.

### 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.**

### 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.

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 la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per

segnalare la presenza di materiale pedopornografico online.

### 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 la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.**

**Vi suggeriamo, inoltre, i seguenti servizi:**

**- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;**

**- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.**

---

# *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;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

### 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.

### 5.3. - 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.**

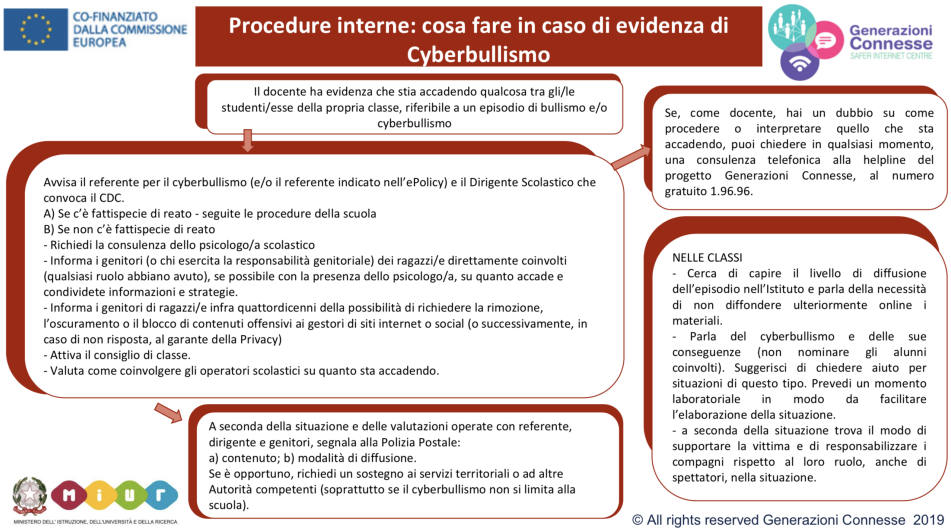
- **Tribunale per i Minorenni: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.**

---

# *5.4. - Allegati con le procedure*

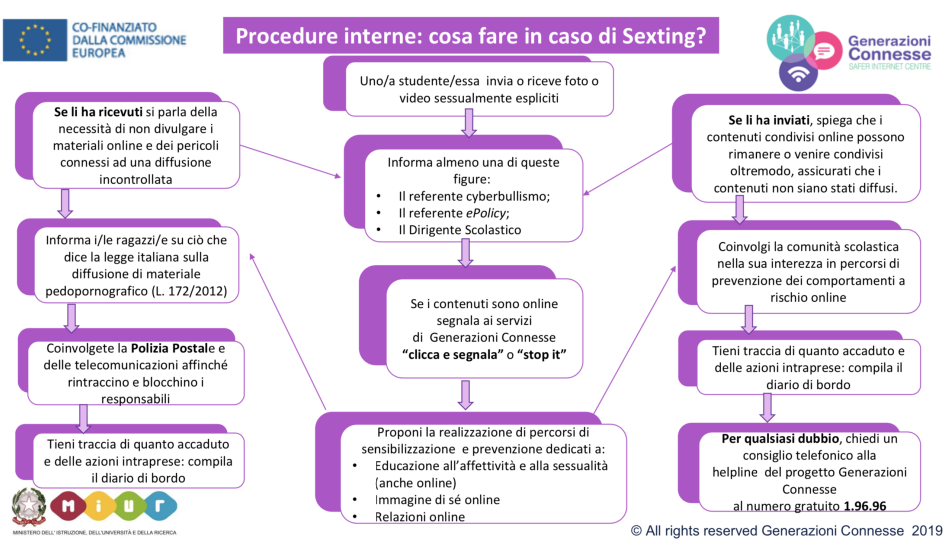
## Procedure interne: cosa fare in caso di sospetto di

# Cyberbullismo?

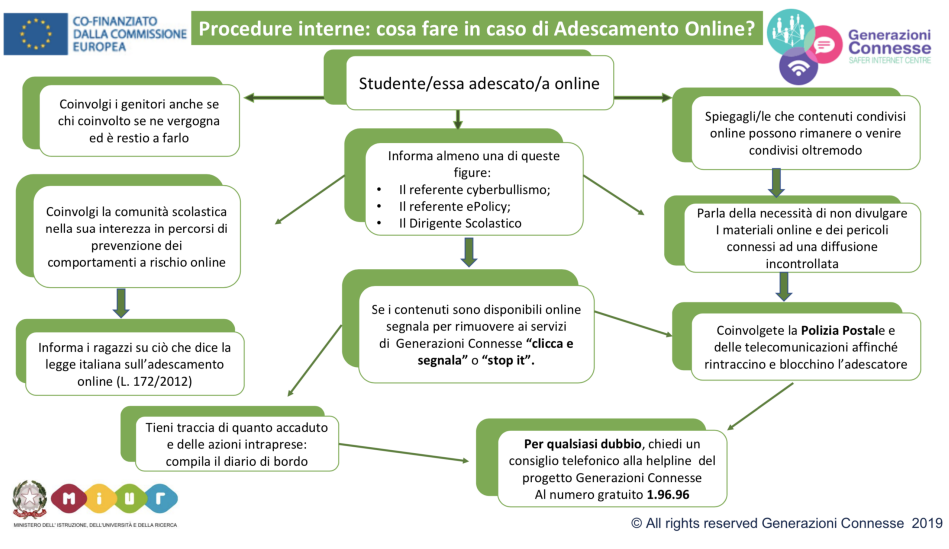




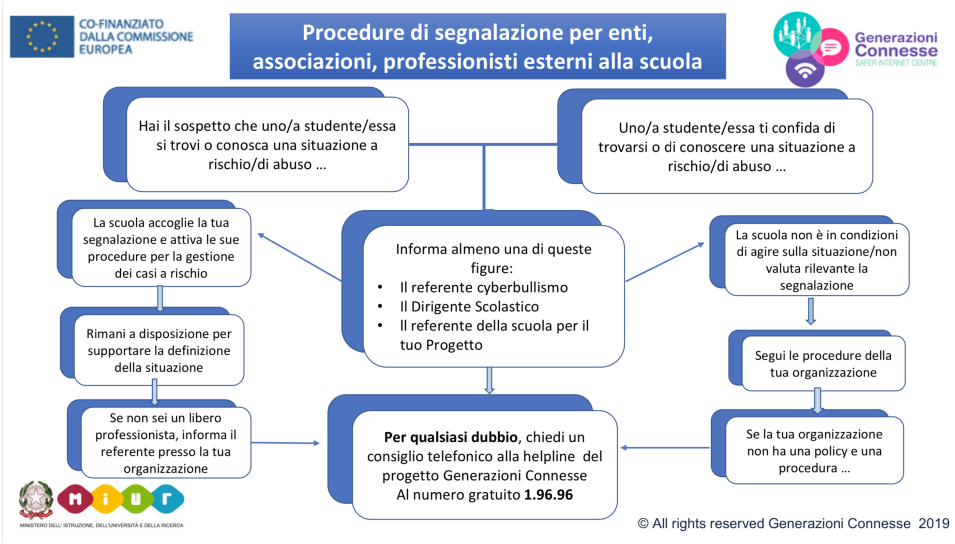
# Procedure interne: cosa fare in caso di sexting?




# Procedure interne: cosa fare in caso di adescamento online?




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

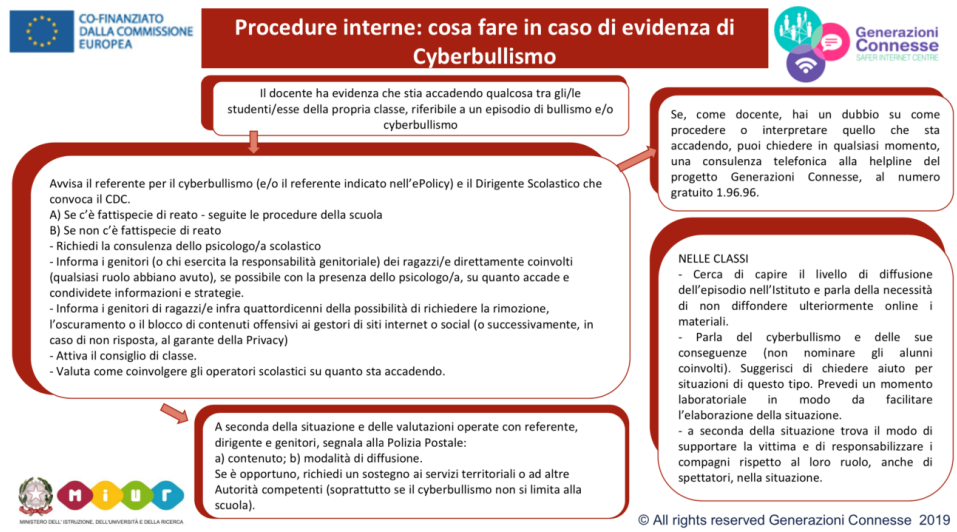



---

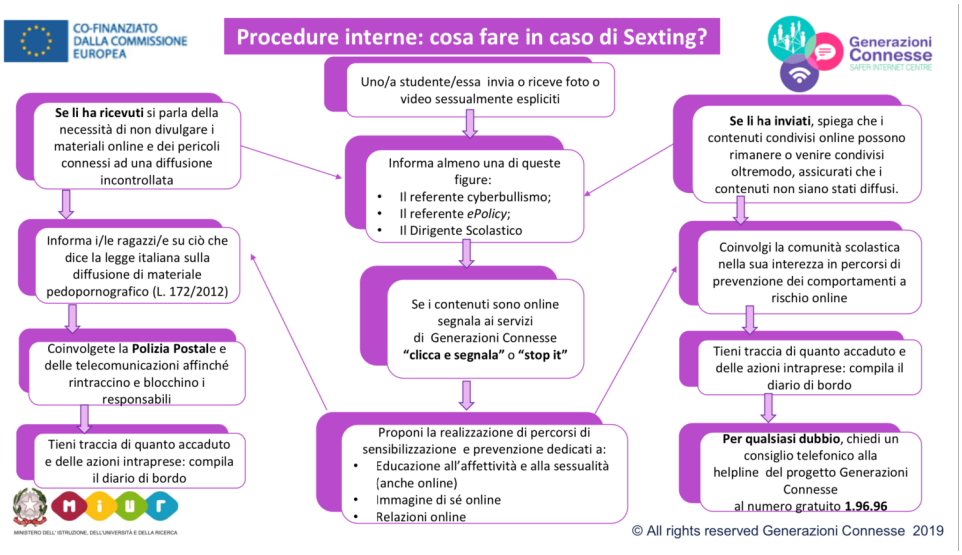
# Altri allegati

- Scheda di segnalazione
- Diario di bordo
- iGloss@ 1.0 l'ABC dei comportamenti devianti online
- Elenco reati procedibili d'ufficio

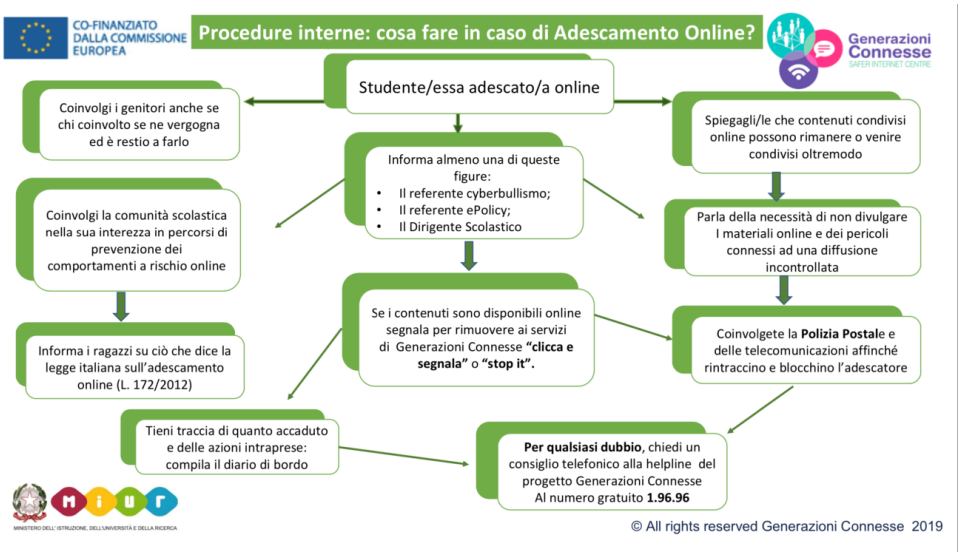
### Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?




## Procedure interne: cosa fare in caso di sexting?

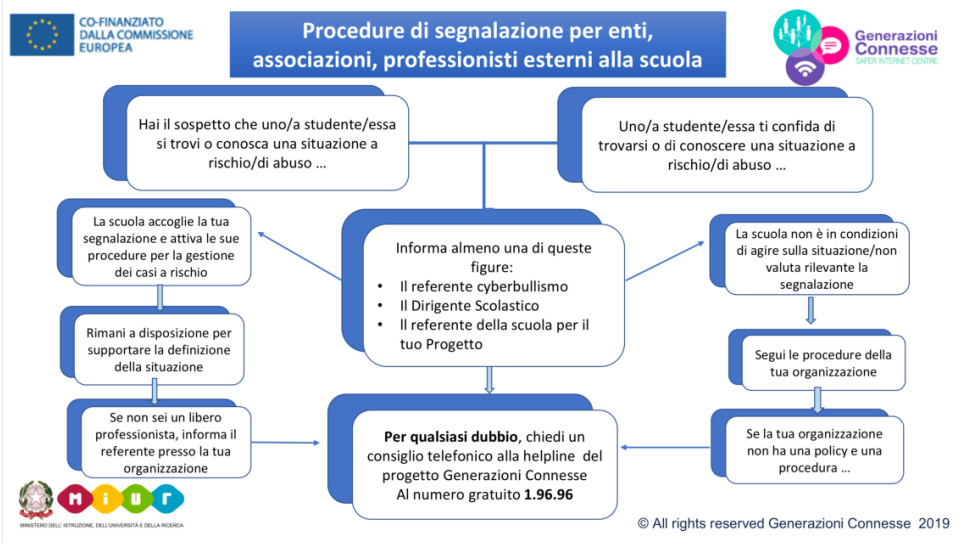



## Procedure interne: cosa fare in caso di adescamento online?




---

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




---

## Altri allegati

- **Informativa e Dichiarazione di presa visione e adesione all'informativa sull'Epolicy dell'IC Casteldaccia e Modulo segnalazione di situazioni a rischio (Allegato 1)**
- **Informativa all'uso di Google Workspace for education (Allegato2)**
- **Modulo per il consenso delle Piattaforme didattiche digitali/app/tools diverse da Google Workspace ed email dei genitori (Allegato3)**
- **Modulo Consenso Uso Credenziali Argo Famiglia (Allegato4)**
- **Modulo Consenso informato Foto e Video (Allegato5)**
- **Modulo per la segnalazione delle situazioni di rischio (Allegato6)**
- **Diario di Bordo (Allegato7)**
- **Elenco reati procedibili d'ufficio**

**Allegato 1**

**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"**

**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-Safety: Informativa all'uso di Google Workspace for education