



I.T.S. "C. ANDREOZZI" - AVERSA
Prot. 0003282 del 14/03/2024
IV (Uscita)



Documento di ePolicy

CETD21000R

I.T.S.-SETTORE EC. E TEC. "C. ANDREOZZI"

VIALE EUROPA 269 - 81031 - AVERSA - CASERTA (CE)

Anna Lisa Marinelli

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 curriculum

1. Curriculum 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.

Il nostro istituto con questo documento ePolicy 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 a Internet. Il Documento di e-policy - "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.

Il Dirigente Scolastico

- garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica.
- promuove la cultura della sicurezza online e, ove possibile, dà il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo,
- gestisce ed interviene nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

L'Animatore digitale

- supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale".
- fa parte della Commissione bullismo e cyberbullismo.

Il Referente bullismo e cyberbullismo

- coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo ai sensi della legge n. 71/2017, art.4;
- si avvale della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio;
- gestisce in collaborazione con la DS, con i docenti della Commissione, con i coordinatori di classe, i casi di bullismo e cyberbullismo.

I Docenti

- segnalano alla DS e alla Referente qualunque problematica relativa a casi di cyberbullismo o di uso non corretto dei dispositivi digitali.
- nell'ambito delle discipline di insegnamento promuovono una cultura del rispetto e un uso corretto delle tecnologie digitali

Il personale Amministrativo, Tecnico e Ausiliario (ATA)

- proprio perchè a contatto quotidiano con studenti e studentesse, vigila e segnala a DS e al referente i comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.

Gli Studenti e le Studentesse

- devono attenersi al Regolamento d'Istituto in particolare per quanto riguarda le regole di utilizzo dei cellulari e in generale nell'uso delle TIC;
- devono segnalare se loro stessi sono oggetto di atti persecutori/bullistici/cyberbullistici o se ne sono stati spettatori o ne sono stati informati;
- devono contribuire attivamente ai momenti di formazione previsti e possono cooperare con proposte e suggerimenti, alla realizzazione di attività e iniziative per la promozione di un uso consapevole e corretto delle TIC anche attraverso percorsi di peer education.

I Genitori

- devono relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete;
- comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet;
- condividere e accettare quanto scritto nell'ePolicy dell'Istituto

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).

Tutto il personale esterno che collabora con l'Istituto per la realizzazione di attività didattiche e/o educative viene informato dell'esistenza del documento di ePolicy dell'Istituto con le procedure in esso contenute per la segnalazione di eventuali episodi e/o comportamenti scorretti da parte di studenti e studentesse o di personale dell'Istituto.

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/le 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.

Il documento dell'ePolicy di istituto viene pubblicato nel sito internet della scuola. Inoltre si prevedono momenti specifici di divulgazione e comunicazione a tutti i soggetti interessati: docenti, studenti e studentesse, genitori.

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.

La scuola gestisce le infrazioni all'ePolicy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni. Nelle attività scolastiche ed extra-scolastiche gli studenti assumono i comportamenti richiesti dalle norme giuridiche, dallo Statuto delle studentesse e degli studenti e dal Regolamento di Istituto. I provvedimenti disciplinari hanno finalità educativa, tendono al rafforzamento del senso di responsabilità e al ripristino di rapporti corretti all'interno della scuola e sono ispirati, per quanto possibile, al principio della riparazione del danno. Inoltre le infrazioni alla ePolicy e, più in generale, all'uso scorretto dei cellulari, e di qualsiasi strumento informatico all'interno dell'Istituto, nonché tutti i comportamenti bullistici e cyberbullistici sono sanzionati nel Regolamento di istituto che è stato recentemente aggiornato .

In particolare si farà riferimento a:

- Patto educativo di corresponsabilità
- Regolamento di Istituto
- Tutto il personale è tenuto a collaborare con il Dirigente Scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo, gestionale, disciplinare, amministrativo, penale, a seconda del tipo e della gravità delle infrazioni commesse.

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.

Si fa riferimento ai documenti di cui sopra, che vengono allegati alla ePolicy d'Istituto.

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.

L' ePolicy verrà aggiornata quando si verificheranno 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. L'aggiornamento e l'eventuale implementazione del documento di ePolicy sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore digitale, del Referente del bullismo e cyberbullismo, e dagli Organi collegiali. L'attività di monitoraggio avrà il fine di rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di Internet. Il monitoraggio on-line sarà rivolto anche ai docenti, al fine di valutare l'impatto della ePolicy e la necessità di eventuali miglioramenti.

Il nostro piano d'azioni

PIANO D' AZIONE 2023/2024

Azioni da svolgere entro un'annualità scolastica:

Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti

Informare i docenti anche nell'ambito di un'attività collegiale

Informare i componenti del Consiglio di istituto

Azioni da svolgere nei prossimi 3 anni:

- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti

Capitolo 2 - Formazione e curriculum

2.1. Curriculum 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 curriculum digitale.

Il curriculum predisposto è articolato per aree delle competenze e le competenze specifiche da raggiungere. Le competenze verranno poi inserite nelle uda programmate dai singoli docenti e dai consigli di classe.

Per quanto concerne l'"**Alfabetizzazione su informazioni e dati**", saranno organizzate attività volte a potenziare le capacità e competenze nel saper ricercare e filtrare dati, informazioni e i contenuti digitali, nel saper valutare e gestire dati, informazioni e contenuti digitali.

Rispetto alla competenza di "**Comunicazione e collaborazione**", si pianificheranno azioni volte a potenziare azioni volte a sviluppare la capacità degli studenti nell'interazione con i gruppi dei pari con l'uso delle tecnologie digitali, in modo da favorire le competenze necessarie per condividere informazioni i

ed esercitare la cittadinanza attraverso le tecnologie digitali. Durante queste attività conosceranno la Netiquette e avranno modo di imparare a gestire l'identità digitale. Per quanto riguarda la "**Creazione di contenuti digitali**", saranno sviluppate azioni formative su come costruire, interrogare e rielaborare i contenuti digitali. Conosceranno anche il Copyright e le licenze. In merito alla "**Sicurezza**" si organizzeranno incontri per imparare a proteggere i dispositivi, i dati personali e la privacy, la salute e il benessere in Rete. Per la competenza "**Risolvere problemi**" saranno strutturati segmenti didattici per saper utilizzare in modo creativo le tecnologie digitali, e saper comprendere le diverse competenze digitali.

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.

La maggior parte dei docenti ha in attivo percorsi formativi sull'utilizzo delle tecnologie digitali a supporto della didattica. Tutti i docenti interessati saranno indirizzati a corsi che prevedono l'utilizzo di strumenti tecnologici per creare ambienti di apprendimento inclusivi e creativi. Inoltre, saranno strutturati percorsi formativi sull'uso corretto e consapevole della Rete e del potenziale delle tecnologie digitali a supporto dello studio e sulla strutturazione di percorsi educativi-didattici rivolti agli studenti. Per la formazione dei docenti si farà anche leva sulle azioni formative proposte dall'Animatore digitale e su quelle offerte dalla piattaforma Generazioni connesse e altre iniziative offerte dalla piattaforma Elisa, dal MIM e dall'USR. Durante l'a.s. 2023-2024 un gruppo di docenti delle classi prime ha frequentato il corso

Unplugged, per la prevenzione alle dipendenze promosso da formatori dell'ASL di Caserta.

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.

Saranno proposti percorsi formativi sulla sicurezza in rete e sulla gestione dei dati e informazioni che circolano in rete per rendere i docenti validi supporti per gli studenti. Sarà predisposto un canale nella piattaforma Microsoft Teams, in cui i docenti potranno condividere i materiali del corso e le buone pratiche messe in atto. Tutto il materiale sulla sicurezza online deve essere condiviso anche con gli studenti e le famiglie.

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.

Saranno organizzati incontri a sostegno della genitorialità attiva su tematiche legate all'uso della rete e dei problemi legati all'uso non corretto delle tecnologie digitali da parte non solo dei giovani ma di tutti. In particolare saranno messi a conoscenza dei rischi della rete, legati alle comunità virtuali: cyberbullismo, sexting e gli adolescenti, l'addescamento online, la pedopornografia e la dipendenza da internet e dal gioco online. Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi.

Il nostro piano d'azioni

PIANO D' AZIONI 2023/2024)

Scegliere almeno 1 di queste azioni

x Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.

x 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.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.

x Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

x Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

Scegliere almeno 1 di queste azioni

x Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.

- 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.

x Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.

x Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze 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.

All'atto dell'iscrizione il nostro istituto fornisce ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori, quali l'utilizzo di foto, video ed altri materiali audiovisivi contenenti l'immagine e/o il nome del proprio figlio/a all'interno di attività educative e didattiche per scopi documentativi, formativi ed informativi durante gli anni di frequenza nella scuola. Si evidenzia che le immagini e le riprese audiovisive realizzate dalla scuola, nonché gli elaborati prodotti dagli studenti durante le attività scolastiche, potranno essere utilizzati esclusivamente per documentare e divulgare le attività scolastiche tramite il sito web dell'Istituto.

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.

L'accesso a Internet è consentito all'interno dell'Istituto per l'esercizio di attività didattica attraverso reti wireless e wired l'accesso degli studenti ai dispositivi della scuola deve avvenire sempre in presenza del docente il quale segnalerà al responsabile dei laboratori eventuali disservizi e malfunzionamenti. Il docente è responsabile del comportamento degli alunni, degli strumenti e del software che utilizzano in sua presenza. L'accesso al sistema informatico per la didattica è consentito al personale previa assegnazione di credenziali formate da nome utente e una password. I docenti accedono alla propria sezione del registro elettronico con credenziali personali. L'account di posta elettronica è quello personale usato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. Tutti i docenti dell'Istituto e gli studenti possiedono un account generato dalla scuola per consentire l'accesso alla piattaforma Microsoft Teams, questo consente ai destinatari di utilizzare le funzionalità dell'ambiente online, per il lavoro collaborativo nelle classi.

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.

Le nuove tecnologie facilitano e migliorano la comunicazione: per questo all'interno dell'Istituto Carlo andreoZZi si utilizzano diversi strumenti di comunicazione online. A tale proposito è importante effettuare una distinzione preliminare fra comunicazione interna e comunicazione esterna. La scuola utilizza diversi strumenti di comunicazione

on-line, sia per far circolare all'interno della scuola informazioni di servizio o contenuti importanti fra i diversi attori scolastici (docenti, studenti, genitori, collaboratori scolastici ecc.), sia per raggiungere target esterni, al fine di valorizzare e promuovere le attività portate avanti dall'Istituto (rivolgendosi ad esempio a istituzioni, famiglie, studenti non ancora iscritti, associazioni ecc.). Fra gli strumenti di comunicazione esterna, troviamo il sito web della scuola dove è possibile trovare i principali documenti della scuola: PTOF, Regolamento d'Istituto, pubblicizzazione di eventi, circolari ed avvisi, documentazione di attività curricolari ed extracurricolari ecc.che viene continuamente aggiornato.I profili sui social network: Facebook, Instagram. La comunicazione esterna dell'Istituto è progettata ed implementata anche con il supporto degli studenti che producono contenuti multimediali da diffondere attraverso i vari canali in uso (video, foto, post sui social, articoli per il sito ecc.). Fra gli strumenti di comunicazione interna, invece, troviamo il Registro elettronico Argo con tutte le sue funzionalità, la posta elettronica ordinaria, applicativi e piattaforme di lavoro condiviso e collaborativo come Microsoft Teams che sono utilizzati anche per facilitare e rendere più partecipata la didattica e la comunicazione a scuola. Gli strumenti di messaggistica istantanea, come Whatsapp, sono utilizzati solo per le comunicazioni informali tra docenti.

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.

Come da Regolamento d'Istituto, agli studenti è fatto assoluto divieto di usare il cellulare durante le ore di lezione, se non per scopi esclusivamente didattici autorizzati

dal docente. Lo stesso divieto si estende al personale docente: è consentito l'uso di dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili. L'Istituto Andreozzi, aderendo al progetto Generazioni Connesse, si impegna a sensibilizzare, formare e responsabilizzare tutti i soggetti che partecipano al processo educativo e didattico. L'utilizzo delle tecnologie e dei dispositivi anche personali va mediato e calibrato, anche al fine di favorire negli studenti lo sviluppo di un pensiero critico. L'ePolicy, documento di indirizzo e programmazione interno al progetto, viene redatto per perseguire tali obiettivi, per potenziare le competenze di cittadinanza digitale e per favorire un utilizzo costruttivo e consapevole del proprio dispositivo (azione #15 del PNSD - Scenari innovativi per lo sviluppo di competenze digitali applicate).

Il nostro piano d'azioni

IL NOSTRO PIANO D' AZIONE

da sviluppare nell'arco dell'anno scolastico 2023/2024

- organizzare un evento volto a formare personale docente e non docente dell'Istituto sui temi dell'accesso a Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity);
- organizzare un evento volto a formare gli studenti/esse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity);
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

AZIONI DA SVILUPPARE NEL CORSO DEI TRE ANNI SCOLASTICI SUCCESSIVI:

- organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso a Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity);
- organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso a Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity);
- effettuare un' analisi sull' utilizzo dei dispositivi personali a scuola da parte degli altri studenti e studentesse;
- organizzare incontri per la consultazione degli studenti sulle indicazioni/regolamenti inerenti l'uso dei dispositivi digitali personali ;
- organizzare uno o più eventi o attività volti a formare gli studenti e

le studentesse del nostro istituto sul tema delle tecnologie digitali e della protezione dei dati 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.

Le tecnologie digitali e la rete internet ha trasformato radicalmente le dinamiche relazionali e quelle identitarie, si è assistito a un nuovo utilizzo di linguaggi e modi di comunicazione. Ormai sono diventati strumenti privilegiati nella comunicazione e nella relazione; e risultano essere un valido supporto nello studio e nella ricerca di informazioni e per tale necessitano di una conoscenza anche in termini di sicurezza e

coretto utilizzo per il benessere proprio e di chi interagisce con noi. I giovani possono facilmente correre rischi in un uso inconsapevole della rete, tra quelli più noti abbiamo: l'adescamento online, il cyberbullismo, il sexting, la violazione della privacy, la pornografia, la pedopornografia, il gioco d'azzardo o gambling, internet addiction, videogiochi online,, nonché esposizione a contenuti dannosi o inadeguati come i contenuti razzisti, comportamenti alimentari scorretti, atteggiamenti violenti e prevaricatori su persone fragili etc. Inoltre, sarà previsto un incontro per far conoscere alla comunità scolastica l'e-policy. Per favorire atteggiamenti responsabili e sviluppare le competenze necessarie per utilizzare il potenziale delle tecnologie digitali è necessario promuovere azioni formative volte alla sensibilizzazione e protezione in termini di cittadinanza digitale. Al fine di sensibilizzare le studentesse e gli studenti l'istituto Carlo Andreozzi propone degli incontri formativi rivolti a tutte le classi dell'istituto durante i quali saranno fatti conoscere i rischi della rete, con il supporto di filmati e testimonianze di storie reali reperite in internet e quelle offerte dalla piattaforma generazioni connesse. Le attività saranno integrate nelle unità di apprendimento delle singole discipline e in quelle interdisciplinari elaborate dal consiglio di classe. Per prevenire e contrastare i fenomeni devianti legati all'uso inconsapevole della rete e delle nuove tecnologie si creeranno momenti di incontro con esperti dell'ASL e della Polizia Postale, e si coinvolgeranno anche le famiglie. Inoltre sarà favorita una didattica che vede la collaborazione tra pari.

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).

Il cyberbullismo è un atto offensivo, minatorio e prevaricatorio condotto attraverso l'utilizzo dei social network. Il fatto che si consumi in internet, in un ambiente riconosciuto non reale dai ragazzi, gli dà anche una veste ludica e per questo viene sottovalutato, ma le conseguenze possono essere estreme come il suicidio. Il tema è senz'altro importante e per questo le attività riconducibili all'educazione civica danno spazio anche alla discussione del tema in tutte le classi.

Il nostro istituto nella prevenzione al fenomeno del cyberbullismo opera e le allinea le sue attività formative rispetto a quanto previsto dalla Legge 71/2017 e dalle Linee di orientamento. In merito ha già aggiornato il nostro Regolamento di Istituto e ha attivato incontri di sensibilizzazione con esperti esterni.

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.

Gli "hate speech" consistono in un odio o intolleranza verso un gruppo o una persona identificata, e si attua principalmente con l'uso di internet. Per far conoscere questi rischi della rete sarà favorito un utilizzo responsabile delle tecnologie digitali e in questo caso far conoscere ai giovani come agire per arginare gli stereotipi (razza, genere, disabilità) su cui poggiano le forme di hate speech. Inoltre sarà incentivata una partecipazione attiva e consapevole in rete per depotenziare gli stereotipi che alimentano gli hate speech, in merito si predisporranno attività didattiche che vedono i nostri studenti impegnati in campagne di sostegno alla lotta agli stereotipi su cui poggiano gli hate speech con l'uso dei media digitali e i social network. Le attività avranno anche la finalità di favorire la formazione di cittadini attivi e consapevoli.

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?

Il nostro Istituto organizzerà attività che avranno lo scopo di favorire il benessere psico-fisico di chi utilizza la Rete e le nuove tecnologie digitali. Saranno proposte azioni formative incentrate su giochi virtuali con l'utilizzo dei dispositivi elettronici dotati di

connessione internet; inoltre, saranno organizzati incontri con esperti per affrontare la questione della dipendenza da internet e dal gioco online. Saranno favoriti anche interventi educativi durante i quali le studentesse e gli studenti conosceranno il potenziale delle tecnologie digitali e dell'uso corretto della Rete.

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 medialmente 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.

Il sexting è un fenomeno molto diffuso in Rete, ma non tutti i giovani e le loro famiglie ne conoscono la portata e per questo il nostro istituto si impegnerà nella disposizione di incontri per presentare questo rischio della Rete anche per far conoscere alle studentesse e agli studenti i rischi penali a cui si va incontro una diffusione di materiale dal contenuto sessualmente esplicito. Si cercherà la collaborazione di esperti di diritto penale.

4.6 - Adescamento online

Il **grooming** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenzialmente 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.

Il nostro istituto si propone di mettere in campo azioni formative rivolte a un uso prudente e consapevole della Rete. Saranno organizzati corsi di formazione rivolti ai docenti per tenerli aggiornati sui rischi della Rete in modo tale da poter fornire i loro studenti degli strumenti opportuni per poter navigare con sicurezza in Rete. Le studentesse e gli studenti saranno indirizzati alla prudenza, sarà detto di non fornire dati e informazioni personali, di uscire da chat e siti con contenuti inadatti e di non incontrare persone conosciute in Internet senza averne prima parlato con i genitori. Saranno messe in campo attività sulle fake news, sui siti e sulle email poco attendibili in modo da sviluppare negli studenti la capacità di valutare criticamente ciò che incontrano durante la navigazione, poiché non tutte le informazioni online sono vere e affidabili.

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](#).

La nostra scuola avvierà azioni di sensibilizzazione e formazione per prevenire i fenomeni di pedopornografia, anche con la collaborazione di esperti: psicologo e forze dell'ordine. Le attività avranno l'obiettivo di rendere gli studenti consapevoli di eventuali rischi che si possono correre nella divulgazione a soggetti terzi di immagine intime online. Inoltre si organizzeranno incontri e parteciperà ai eventi sull'educazione all'affettività, già da quest'anno avviati. Infatti l'8 marzo 2024 gli alunni delle classi prime sono stati coinvolti nell'incontro "Quando l'emozioni ci rendono più forti". Educare all'affettività è il primo passo per prevenire qualsiasi forma di devianza giovanile. Saranno organizzati eventi formativi sul tema della pedopornografia rivolti sia agli studenti sia alle loro famiglie per far comprendere anche i possibili risvolti giuridici se si collabora alla diffusione di immagine intime. Le attività rientrano nelle regolari attività di studio, programmati dai docenti, perché i nostri alunni studiano materie giuridiche, e quindi imparano le nozioni di base sul diritto all'immagine e sulle responsabilità penali e civili conseguenti alla loro diffusione.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024).**Scegliere almeno 1 di queste azioni:**

Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/le 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.

Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

Promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.

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/le studenti/studentesse.

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

Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

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

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).**Scegliere almeno 1 di queste azioni:**

Organizzare uno o più incontri di sensibilizzazione sui rischi online e un

utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

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.

x 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.

x Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

Promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.

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.

Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

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/le studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online:** se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenni 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.

Tt

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](tel: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.

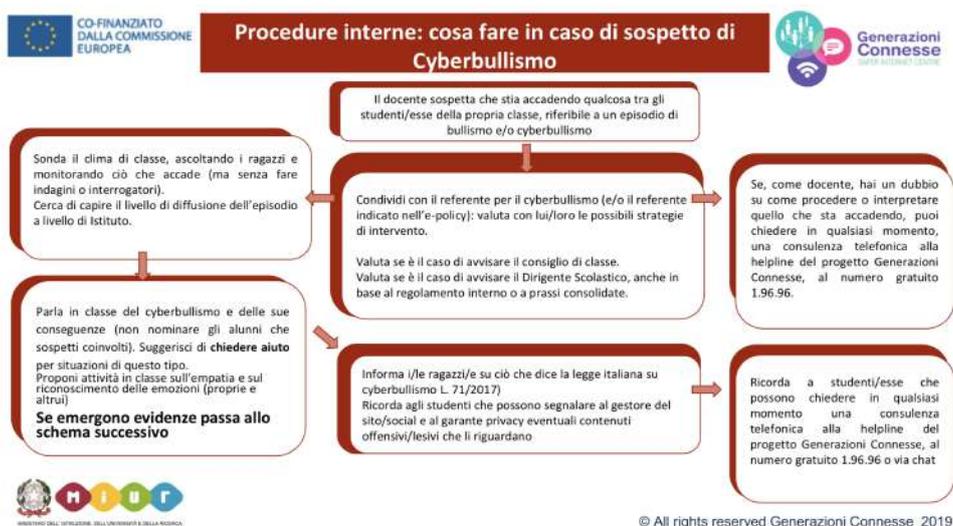
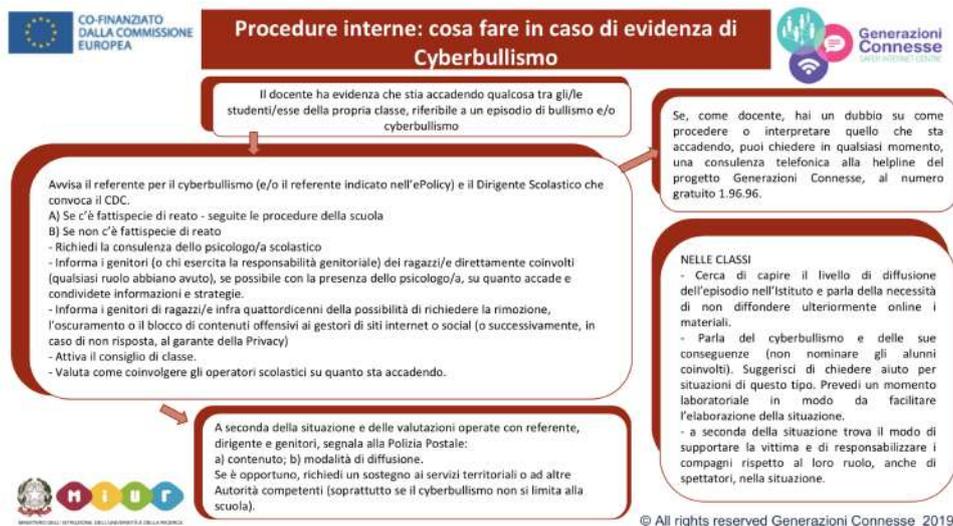
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare 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; raccolgono 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.

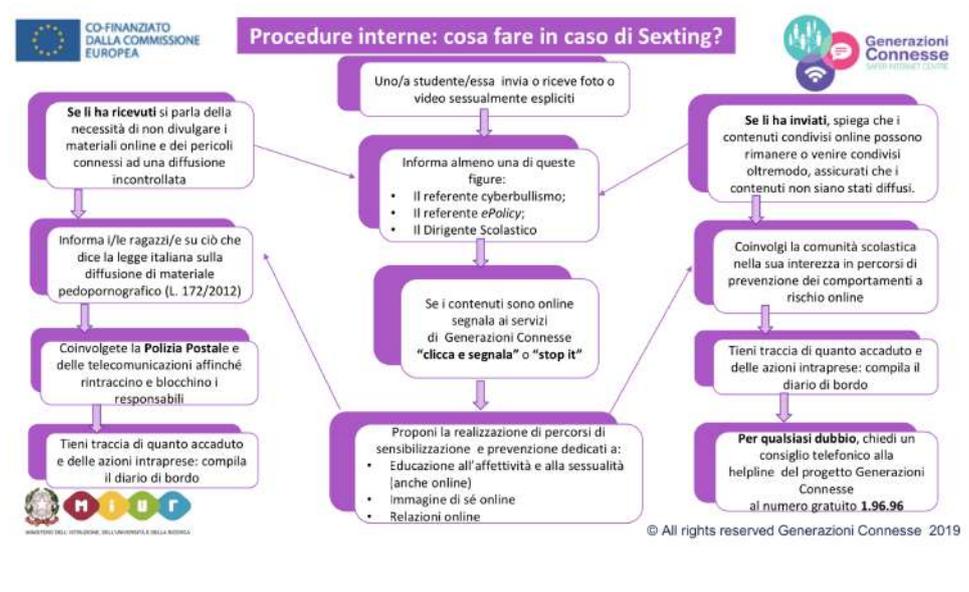
- **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

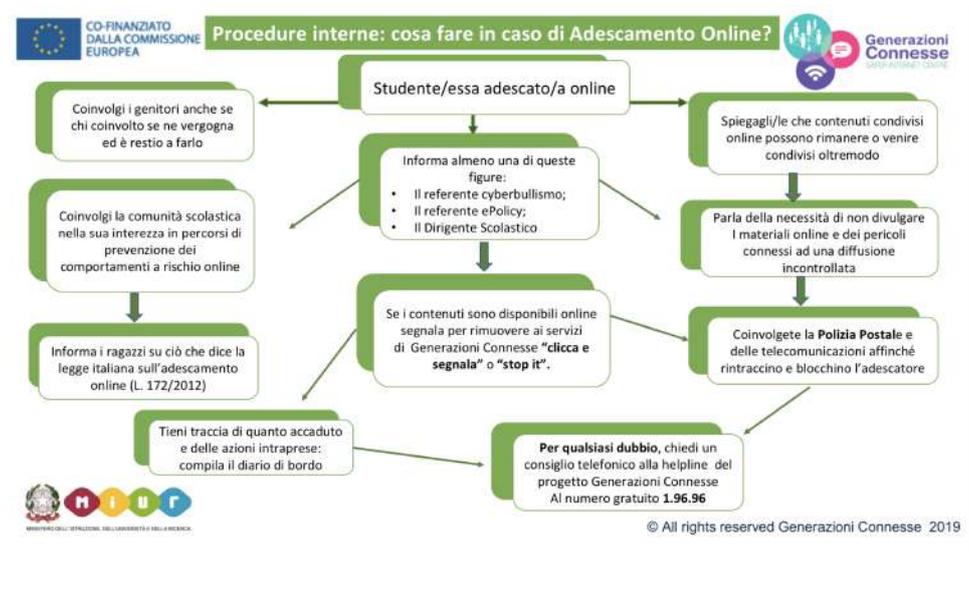
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



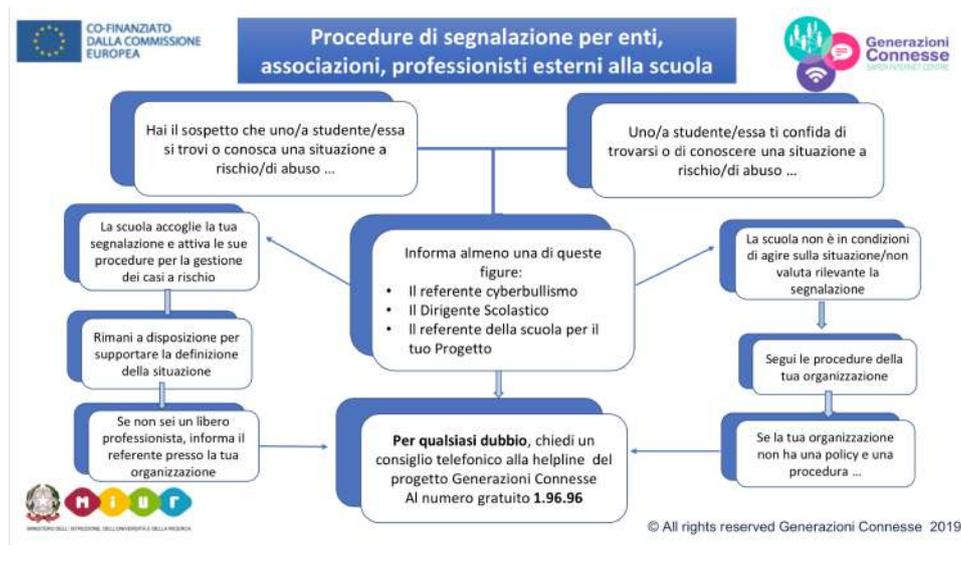
Procedure interne: cosa fare in caso di sexting?



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](#)

Si utilizzeranno i materiali offerti dalla piattaforma Generazioni connesse.

Il nostro piano d'azioni

Le azioni saranno condivise con la comunità scolastica, alla quale sarà presentata il documento di ePolicy. Il Regolamento di Istituto sarà integrato con documento di ePolicy. Come già si è detto nei capitoli precedenti saranno avviate azioni di formazione, sensibilizzazione e prevenzione rivolte sia al personale scolastico, sia agli alunni, sia alle famiglie. Saranno attivati rapporti di collaborazione con esperti di problematiche giovanili, di dipendenze e benessere e con le Forze dell'ordine.

