Documento di ePolicy
I.C. DI BUDRIO

VIA GIOVANNI XXIII 2 - 40054 - BUDRIO
Bologna (BO) - Emilia-Romagna
Data di approvazione: 03/11/2025 - 19:54

Cap 1 - Lo scopo della ePolicy

1.1 Scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

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

Capitolo 2 - Sensibilizzazione e prevenzione

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

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

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

Capitolo 4 - Segnalazione e gestione dei casi

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

1.1 Scopo dell'ePolicy

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

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

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

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

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

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

Le tecnologie dell'informazione e della comunicazione (TIC) sono strumenti essenziali per l'apprendimento e la didattica. Adottare un'**ePolicy** non è un semplice adempimento burocratico, ma una scelta strategica per garantire un ambiente educativo sicuro e rispettoso nell'uso della tecnologia.

Principi e Regole

In un'epoca in cui la vita di studenti, docenti e genitori è strettamente legata al digitale, l'uso di Internet, social media e intelligenza artificiale richiede regole chiare. L'Istituto Comprensivo di Budrio si fonda su principi di **rispetto reciproco**, **riservatezza** e **trasparenza**.

- **Rispetto e Condivisione delle Regole:** Tutta la comunità scolastica si impegna a collaborare per prevenire e contrastare comportamenti intimidatori o violenti. Per questo, è fondamentale conoscere e rispettare il **PTOF**, il **Regolamento d'Istituto**, il **Patto di Corresponsabilità** e la presente ePolicy.

- **Riservatezza:** Il personale scolastico si impegna a non divulgare dati personali o notizie riservate. Allo stesso modo, gli studenti sono tenuti a rispettare la riservatezza altrui, non diffondendo senza consenso foto, video o altre informazioni.

- **Trasparenza:** La scuola garantisce la massima trasparenza delle sue attività, facilitando l'accesso alle informazioni tramite il **Registro Elettronico** e il sito web. Gli studenti hanno il diritto di conoscere in modo chiaro i criteri e le modalità di valutazione.

Comunicazione e Collaborazione

La comunicazione tra docenti, studenti e famiglie avviene principalmente tramite il Registro Elettronico, il sito web la posta elettronica e Classroom

Obiettivi e Fondamenti dell'ePolicy

L'adozione di un'ePolicy rappresenta un investimento per la crescita digitale della scuola. Il presente documento mira a:

- Promuovere le **competenze digitali**.

- Garantire la **sicurezza online** e il **rispetto della privacy**.

- Prevenire e contrastare il **cyberbullismo**, l'**hate speech** e la **dipendenza da internet**.
- Definire norme per la gestione delle infrastrutture e degli strumenti digitali.

L'ePolicy si basa su normative nazionali ed europee, tra cui il **GDPR**, la **legge sul cyberbullismo** e le linee guida del **MIUR**. È coerente con il **PTOF** e il **Piano di Miglioramento** dell'Istituto.

La scuola collabora attivamente con enti esterni come università, Enti Locali e associazioni per realizzare percorsi educativi e formativi condivisi, valorizzando la co-progettazione e la prevenzione dei rischi online.

Il nostro piano d'Azioni

Azioni da svolgere entro i prossimi tre anni scolastici:

- Riconferma del gruppo di lavoro E-policy, così costituito: referente per la prevenzione del bullismo e del cyberbullismo, PTOF, FS e TIC
- Aggiornamemento periodico del monitoraggio dell'efficacia dell'E-policy attraverso sondaggio rivolto a tutte le componenti dell'Istituto
- Formazione del personale docente e non docente sui reati on-line e sulla privacy
- Revisione del Regolamento d'Istituto
- Implementazione della dotazione tecnica delle classi, per quanto concerne LIM, PC, tablet (anche in comodato d'uso agli studenti) con particolare attenzione nei confronti degli allievi con BES, nei limiti delle dotazioni finanziarie dell'Istituto e dei fondi dedicati
- Aggiornamento del documento E-policy

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

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

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

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

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

IL DIRIGENTE SCOLASTICO

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

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

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

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

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

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

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

In coerenza con le Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo del Ministero dell'Istruzione (D.M. n. 18 del 13/1/2021, agg. 2021 – nota prot. 482 del 18-02-2021), il Team ha le funzioni di coadiuvare il Dirigente Scolastico, coordinatore del Team nella scuola, nella definizione degli interventi di prevenzione e nella gestione dei

casi di bullismo e cyberbullismo che si possono presentare. Promuove inoltre la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale e comunica ad alunni, famiglie e tutto il personale scolastico dell'esistenza del team, a cui poter fare riferimento per segnalazioni o richieste di informazioni sul tema.

Il Team ha il compito di:

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

I/LE DOCENTI

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

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

RESPONSABILE DELLA PROTEZIONE DEI DATI

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

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

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

GLI STUDENTI E LE STUDENTESSE

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

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

I GENITORI/ADULTI DI RIFERIMENTO

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

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

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

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

L'Istituto ha delineato un Piano di Formazione che si focalizza su competenze digitali, didattica innovativa e uso consapevole delle tecnologie. Per raggiungere questi obiettivi, sono state previste diverse modalità di coinvolgimento, tra cui laboratori, workshop, e corsi specifici sull'uso delle piattaforme digitali. Queste iniziative si integrano pienamente con le priorità del Piano Nazionale di Formazione (PNF) e sono allineate con il Piano Triennale dell'Offerta Formativa (PTOF).

La formazione non si limita ai soli docenti: anche il personale ATA è incluso, con moduli dedicati all'autonomia scolastica, alla sicurezza, alla privacy e al supporto tecnico per le attività digitali.

L'efficacia delle azioni intraprese sarà costantemente monitorata attraverso un bilancio annuale che verrà redatto dal dal Team del Bullismo e dal Dirigente Scolastico. Tale bilancio, affiancherà la revisione del PTOF e del Rapporto di Autovalutazione (RAV). I risultati di questo monitoraggio verranno poi discussi e analizzati in Collegio dei Docenti e in Consiglio d'Istituto, permettendo un aggiornamento del documento e la pianificazione di futuri interventi formativi.

1.3 Integrazione ePolicy nei documenti scolastici

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

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

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

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

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

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

Inizio di ogni anno scolastico, agli studenti e alle studentesse viene letto il Regolamento d'Istituto e il Patto di Corresponsabilità, entrambi arricchiti con riferimenti al documento di ePolicy. Questi documenti, insieme all'ePolicy stessa, sono sempre disponibili sul sito web ufficiale della scuola per la consultazione.

Il PTOF 2025-2028 verrà aggiornato per includere specifici riferimenti, collegamenti e integrazioni con l'ePolicy, la piattaforma Generazioni Connesse e il Curricolo Digitale.

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

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

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

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

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

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

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

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

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

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

Canali e Strumenti Chiave per la diffusione del documento ePolicy:

- **Sito Web Istituzionale:** L'ePolicy completa sarà sempre disponibile in una sezione dedicata del sito della scuola.
- **Incontri Informativi:** la scuola organizzerà sessioni periodiche, online o in presenza, per presentare l'ePolicy, discuterne le implicazioni e raccogliere feedback.
- **Protocolli d'Intesa:** Ogni accordo di collaborazione richiamerà esplicitamente l'adesione alla presente ePolicy.

Contenuti Essenziali delle Informative

Le comunicazioni agli attori esterni dovranno coprire i seguenti punti:

- **Obiettivi e Principi:** Visione e valori alla base dell'ePolicy.
- **Ambiti di Applicazione:** Contesti e attività a cui si applica il documento.
- **Ruoli e Responsabilità:** Chiari compiti di scuola e partner.
- **Linee Guida per le Attività:** Come progettare e realizzare iniziative in conformità con l'ePolicy, con focus su privacy e sicurezza.
- **Consenso Informato:** Procedure per la raccolta dei consensi dei genitori/tutori.
- **Procedure di Segnalazione:** Come agire in caso di comportamenti non conformi o rischi.

1.5 - I Piani di Azione dell'ePolicy

I piani di azione rappresentano il **programma triennale** di obiettivi che la scuola intende realizzare per promuovere la conoscenza delle regole e dei protocolli di intervento che sono stati adottati con il documento di ePolicy nella comunità scolastica.

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

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

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

1° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

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

MODULO II

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

MODULO III

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

MODULO IV

- Definizione, a partire da quanto definito nell'ePolicy, delle procedure di segnalazione anche con linguaggio child/youth friendly perché possano essere accessibili a studenti e studentesse;

- Realizzare una reportistica delle segnalazioni ricevute e dei relativi esiti.

2° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

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

MODULO II

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

---

Infrastrutture e Didattica Digitale

L'Istituto comprensivo di Budrio è all'avanguardia nell'integrazione delle tecnologie didattiche. Tutti gli ambienti e le aule sono equipaggiate di LIM, PC, Tablet, e registratori audio, inoltre sono disponibili laboratori multimediali con connessione Wi-Fi in tutta la struttura. Questi strumenti sono alla base di un ambiente di apprendimento flessibile, pensato per favorire la didattica laboratoriale e interdisciplinare, in linea con le direttive del PNRR e i programmi STEM.

La scuola, inoltre, mira a potenziare le competenze digitali attraverso percorsi specifici di didattica, formazione e orientamento per gli studenti per una didattica accessibile e inclusiva.

Pianificazione delle Azioni

Obiettivi a breve termine (entro un anno scolastico):

Valutazione delle competenze: Analizzare il fabbisogno formativo degli studenti e dei docenti in merito alle competenze digitali e all'integrazione delle TIC nella didattica.

Sensibilizzazione: Organizzare un evento di presentazione del progetto "**Generazioni Connesse**" per studenti e docenti.

Obiettivi a medio termine (entro i prossimi tre anni):

Formazione continua: Organizzare e promuovere corsi di formazione per i docenti sull'uso e l'integrazione delle **TIC** e dell'**Intelligenza Artificiale (IA)** nella didattica.

Coinvolgimento della comunità: Organizzare incontri con esperti di competenze digitali, aperti a docenti, studenti e genitori.

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

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

Per garantire la massima accessibilità, il link e le risorse della piattaforma Generazioni Connesse sono ora parte integrante del PTOF e del Regolamento d'Istituto, oltre a essere pubblicati sul sito web ufficiale della nostra scuola.

La presentazione del kit didattico della piattaforma avverrà a inizio anno scolastico 2025/2026, in un incontro dedicato a studenti, docenti e genitori, guidato dal Team Bullismo e Cyberbullismo.

Cap 2 - Sensibilizzazione e prevenzione

2.1 - Sensibilizzazione e prevenzione

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

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

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

I rischi online si configurano come la possibilità per il minore di:

• commettere azioni online che possano danneggiare sé stessi o altri o esserne vittima;

• osservare altri commettere azioni dannose per sé stessi o altri. È importante riconoscere tempestivamente questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e contenerli, ma è altrettanto rilevante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. Ciò è possibile solo lavorando su aspetti di ampio raggio che riducano i fattori di rischio e, di conseguenza, si traducano in una minore probabilità che i ragazzi si trovino in situazioni pericolose. È importante che gli studenti e le studentesse abbiano gli strumenti per riconoscere possibili situazioni di rischio e per segnalarle a 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.

AZIONI (da sviluppare nell'arco di tre anni scolastici 2025/2028).

- 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 formativi con il coinvolgimento di esperti per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti al personale docente.
- 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.

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

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

- 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 formativi con il coinvolgimento di esperti per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti al personale docente.
- 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.
- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.
- Potenziare l'attività dello Sportello d'Ascolto su queste tematiche.

2.2 - Il Curricolo Digitale

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

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

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

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

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

Il nostro Istituto si impegna a promuovere un **Curricolo Digitale** che accompagnerà nel percorso formativo studenti,docenti e famiglie strutturato sulle cinque aree chiave definite dall'Unione Europea:

- **Informazione:** Sviluppare la capacità di identificare, localizzare, recuperare, organizzare e analizzare le informazioni digitali con spirito critico, superando l'approccio "intuitivo".
- **Comunicazione:** Imparare a interagire e collaborare in ambienti digitali, connettendovi con gli altri e partecipando attivamente a comunità e reti online.
- **Creazione di contenuti:** realizzare e modificare contenuti digitali (testi, immagini, video), integrando e rielaborando conoscenze per produrre risultati creativi e innovativi.
- **Sicurezza:** Riflettere sulla protezione personale e dei dati, acquisendo consapevolezza sulle misure di sicurezza, sull'identità digitale e sui diritti di proprietà intellettuale.
- **Problem-solving:** Utilizzare gli strumenti digitali per identificare e risolvere problemi, contribuendo alla creazione di nuova conoscenza e supportando gli altri nell'uso delle tecnologie.

Strumenti per l'Apprendimento Digitale

Per raggiungere questi traguardi, la scuola mette a disposizione una gamma di strumenti:

- **Infrastrutture di base:** Rete Wi-Fi, registro elettronico e un ambiente di lavoro condiviso come **Google Suite**.
- **Piattaforme didattiche:** Software dedicati alla didattica collaborativa, alla creazione di mappe concettuali (**CMap**) e alla geometria dinamica (**Geogebra**) e all'IA.
- **Risorse multimediali:** Accesso a video didattici in rete (come quelli di **RAI Scuola**) e software per la produzione di documenti, fogli di calcolo e presentazioni.

Impegno della Comunità Scolastica

La promozione di una cittadinanza digitale responsabile è una priorità che richiede la collaborazione di tutti gli attori educativi:

- **Formazione dei docenti:** La scuola investe nella formazione continua degli insegnanti per un uso efficace e inclusivo delle TIC nella didattica, fornendo loro modelli positivi e aggiornati.
- **Sensibilizzazione delle famiglie:** Attraverso l'aggiornamento del **Patto di Corresponsabilità**, la scuola si impegna a informare le famiglie sulle attività digitali e a promuovere una collaborazione continua per un uso consapevole delle tecnologie, anche in prospettiva futura.

- **Prevenzione e sicurezza:** Organizziamo corsi e incontri con esperti qualificati come la **Polizia Postale, Carabinieri** per affrontare temi cruciali come il bullismo, il cyberbullismo, i rischi online e le normative legali. Inoltre, ci avvaliamo della collaborazione di professionisti del settore **psicologico** e **legale** per fornire un supporto completo e specializzato a studenti, docenti e famiglie.

Il nostro obiettivo è quello di costruire un ambiente digitale sicuro, ricco di opportunità e rispettoso, che prepari ognuno ad affrontare con successo le sfide del futuro.

2.3 - Il Kit Didattico

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

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

Il nostro Istituto si dota di un quadro operativo chiaro e aggiornato per l'educazione digitale, in quanto il kit si integra pienamente nelle azioni previste dalla nostra **ePolicy**. Il kit offre materiali pratici e strumenti teorici per promuovere una **cittadinanza digitale consapevole, critica e partecipativa** in tutti gli studenti e le studentesse.

Le aree tematiche e l'approccio inclusivo

Basato sul framework europeo **DigComp 2.2**, il kit sviluppa competenze digitali essenziali attraverso 5 aree tematiche:

- **Educazione ai media**
- **Cambiamento digitale**
- **Creatività**
- **Computazione**
- **Informazione**

Il kit include schede didattiche differenziate per i vari ordini di scuola e "pillole" teoriche per la formazione interna del personale. La sua struttura si allinea al modello **ICF-CY**, che garantisce un approccio inclusivo e accessibile per tutti, in linea

con la missione educativa della nostra scuola.

Il valore di questo strumento

Integrare questo kit nella nostra ePolicy significa non solo promuovere la sicurezza in rete, ma anche il **benessere digitale** e l'**autonomia critica** degli studenti. È un passo concreto che ci permette di essere in linea con le normative europee, garantendo un'educazione digitale completa e coerente.

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

3.1 - Protezione dei dati personali e GDPR

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

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

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

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

Il DPO.

Figura obbligatoria nella scuola, ha una conoscenza approfondita della normativa sulla privacy. Può essere interno o esterno all'Istituto scolastico.

Forma e fornisce consulenza all'istituto scolastico ed ai suoi dipensenti in merito agli adempimenti privacy; sorveglia che la scuola adempia agli obblighi normativi; organizza attività formative e di aggiornamento del personale; dà pareri alla scuola in materia di privacy; funge da punto di contatto tra la scuola e il Garante della Privacy.

Trattamento dei dati

Nel rispetto del GPDR l'Istituto informa sul Titolare del trattamento, del DPO, sulla finalità e la base giuridica del trattamento, i destinatari dei dati, il periodo di conservazione dei dati e i termini previsti per la loro cancellazione, i diritti degli interessati, dell'eventuale trasferimento di dati personali verso un paese terzo, sulle misure di sicurezza tecniche ed organizzative.

L'Istituro raccoglie tutte queste informazioni nel **registro dei trattamenti dei dati**.

L'Istituto integra l'organigramma di Istituto con **l'organigramma privacy**.

Violazione dei dati

In caso di violazione dei dati l'Istituto interviene immediatamente per interrompere la perdita dei dati aggiuntiva, informa immediatamente e senza ritardo il DS e il DPO, valuta l'entità della violazione, valura la necessità di procedere alla notifica della violazione del Garante Privacy.

Privacy, scuola, consenso:

Il consenso privacy non è richiesto quando il trattamento dei dati è funzionale all'attività didattica e formativa per il perseguimento di specifiche finalità istituzionali.

Il consenso privacy è richiesto per attività non strettamente connesse a quelle diddattiche (ad. es. erogazione corsi di musica, lezioni di lingua straniera o attività sportive, teatrali e altro non previsto nel curricolo scolastico).

Azioni da svolgere nella prossima annualità e nei prossimi tre anni

L'Istituto si impegna ad organizzare attività formative ad hoc sulla normativa privacy a favore del personale interno alla scuola e a promuovere il continuo aggiornamento.

L'isituto promuove il corso obbligatorio di aggiornamento sulla normativa privacy.

3.2 - Strumenti di comunicazione online (PUA)

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

Il nostro istituto.

Nel rispetto del P.U.A., integrante il DPS; nel rispetto del GPDR; nel rispetto del diritto di accesso a Internet come dall'art. 2 della Dichiarazione dei diritti di Internet e del Regolamento UE del Parlamento Europeo del 2016 e seguenti, e in coerenza con il PNSD, l'Istituto garantisce l'accesso ad internet dotandosi di una strumentazione tecnologica diffusa capillarmente in tutti gli spazi. La connettività è garantita dalla fibra ottica in modalità via cavo e Wi-Fi ed offre la connessione ad internet per le attività sia didattiche sia amministrative.

Per l'accesso alla rete della scuola i dipendenti della scuola sono profilati con account personalizzati e accedono ai servizi tramite procedura di autenticazione personale che prevede l'utilizzo di password aventi caratteristiche adeguate. L'assistenza tecnica del server e delle apparecchiature informatiche è affidata ditta specializzata che provvede al controllo sul backup dei dati, all'aggiornamento dei sistemi operativi e degli antivirus installati sulle macchine e al controllo del funzionamento del firewall. La rete didattica, dotata di firewall dedicato, fornisce in sicurezza la connessione alle classi e ai vari laboratori.

Il firewall non permette l'accesso ai siti non attendibili e ai social. In tutti questi spazi l'utilizzo quotidiano del registro elettronico, attualmente Nuvola, è garantito da protezione dei dati, così come la normativa richiede. L'accesso alla strumentazione e alla connessione è consentito ai docenti solo ai fini didattici ed è normato da password gestite dal responsabile della rete

Gli studenti accedono alla rete sotto il controllo dei docenti e degli assistenti durante le attività didattiche.

La sensibilizzazione rispetto all'uso delle password viene fatta attraverso la diffusione di circolari circa l'utilizzo della strumentazione tecnologica da parte dei docenti.

In particolare gli assistenti tecnici informatici hanno cura di aggiornare periodicamente il software e il sistema operativo a garanzia della protezione da aggressioni esterne e dalle vulnerabilità che emergono nel tempo.

L'uso della tecnologia a scuola è regolamentato dai regolamenti approvati dal Consiglio di Istituto circa l'accesso alla Rete e ai dispositivi tecnologici e dal regolamento E-Policy.

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.

Gli strumenti che l'Istituto adotta sono: sito scolastico, Registro Elettronico, mail personali e/o istituzionali.

Sito scolastico

L'istituto ha nominato l'Animatore Digitale (docente interno per la redazione editoriale e la gestione delle pagine del sito della scuola (da convertire in icbudrio.edu.it.).

Il Dirigente Scolastico è garante del contenuto.

La scuola detiene i diritti d'autore dei documenti che si trovano sul proprio sito o di quei documenti per i quali è stato chiesto ed ottenuto il permesso dall'autore proprietario.

Le informazioni pubblicate sul sito della scuola relative alle persone da contattare rispettano le norme vigenti sulla privacy.

La scuola non pubblica sul proprio sito materiale prodotto dagli alunni senza il permesso dei loro genitori; inoltre, le fotografie degli stessi sono pubblicate previa liberatoria dei genitori o tutori.

La scuola ha già provveduto alla migrazione del sito da suffissi gov.it (non più validi per le istituzioni scolastiche secondo la determina n. 36 del 12 febbraio 2018) a suffissi edu.it.

La scuola valuta l'utilizzo del protocollo HTTPS (l'Hypertext Transfer Protocol Secure è un protocollo per la comunicazione su Internet che protegge l'integrità e la riservatezza dei dati scambiati online); l'utilizzo di un sistema di cifratura quando il trattamento di dati lo richiede (ovvero oscurare il dato per renderlo incomprensibile a coloro che non hanno i codici per accedervi, mediante la "crittografia" e, quindi, l'uso di un algoritmo di cifratura); un sistema di backup (sistema che permette di salvare regolarmente i dati, di ripristinare eventuali file modificati o rimossi per errore dalla rete, di garantire la presenza di una copia di sicurezza di tutti i file importanti).

La scuola offre all'interno del proprio sito web i seguenti servizi alle famiglie ed agli utenti esterni:

servizio del Registro on-line per comunicazione di voti e assenze e per prenotazione di colloqui individuali con i docenti;

- consultazione elenchi libri di testo
- consultazione Piano dell'Offerta Formativa
- consultazione Regolamento di Istituto
- consultazione Patto di Corresponsabilità
- consultazione Orario delle lezioni
- consultazione Organigramma d'Istituto.
- Registro elettronico - Attualmente piattaforma Nuvola

Docenti

Ad ogni docente è assegnata una login e password per la gestione del registro elettronico e posta elettronica dell'Istituto.

Ogni docente firma la presenza secondo l'orario scolastico e tiene aggiornato il registro personale.

Ogni docente chiude il Registro Elettronico al termine della lezione.

Ogni docente chiude su ogni postazione la casella di posta utilizzata sia quella personale sia quella messa a disposizione dell'Istituto.

L'Istituto non risponde dell'alterazione di eventuali dati.

Famiglie

I genitori accedono al Registro Elettronico con un profilo assegnato dal sistema, per la comunicazione sull'andamento didattico-disciplinare dell'alunno, per la prenotazione dei colloqui e per prendere atto della programmazione didattica.

Dirigente, Collaboratori, Segreteria

La comunicazione formale con le famiglie avviene tramite l'invio delle mail istituzionale della scuola alle mail personali dei genitori.

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.

Azioni da svolgere nella prossima annualità e nei prossimi tre anni

La scuola organizza uno o più eventi o attività volti a formare il personale docente e non docente dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.

Organizza uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity).

3.3 - BYOD

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

Strumentazione personale

Per gli studenti

L'Istituto si attiene alla normativa vigente, rispettando i dieci punti del MIUR sull'uso degli strumenti personali a scuola. Il tablet, in particolare, può essere utilizzato come alternativa ai libri di testo, ma solo in modalità offline.

Non è consentito, secondo la norma di legge, l'uso del telefono cellulare come dispositivo didattico.

Eccezione sono gli alunni con BES o DSA, per i quali la scuola garantisce il supporto tecnologico idoneo, ma su richiesta dell'interessato: a loro è consentito l'uso della strumentazione personale con l'accesso alla rete wifi dell'istituto.

Per i docenti

Durante le ore delle lezioni non è consentito l'utilizzo del cellulare se non per finalità strettamente didattica.

È consentito l'uso di altri dispositivi elettronici personali sempre solo a scopo didattico ed integrativo di quelli scolastici disponibili. Durante il restante orario di servizio è permesso l'uso di portatili, tablet, per attività funzionali all'insegnamento; in entrambe le situazioni è garantito l'accesso alla rete wifi negli spazi comuni previsti dalla logistica della rete stessa.

Per il personale della scuola

Durante l'orario di servizio al personale scolastico è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente.

Azioni da svolgere nella prossima annualità e nei prossimi tre anni

Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse in accordo con la normativa vigente.

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

Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali

Cap 4 - Segnalazione e gestione dei casi

4.1 - Cosa Segnalare

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

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

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

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

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

Cyberbullismo: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/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, per quanto possibile, la rimozione del materiale on-line e il blocco della sua diffusione per mezzo dei dispositivi mobili.

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

Azioni da svolgere nella prossima annualità e nei prossimi tre anni

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 formativi con il coinvolgimento di esperti (ad esempio Polizia Postale) per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti al personale docente; promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale anche con esperti esterni; 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.; pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

4.2 - Quali strumenti e a chi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Gli insegnanti e i genitori, come studenti e studentesse, si possono rivolgere alla Helpline del progetto Generazioni Connesse, al numero gratuito 19696, attraverso la chat disponibile sul sito o tramite chat WhatsApp per ricevere supporto e

consulenza. Per tutti i dettagli, il riferimento è agli allegati con le procedure.

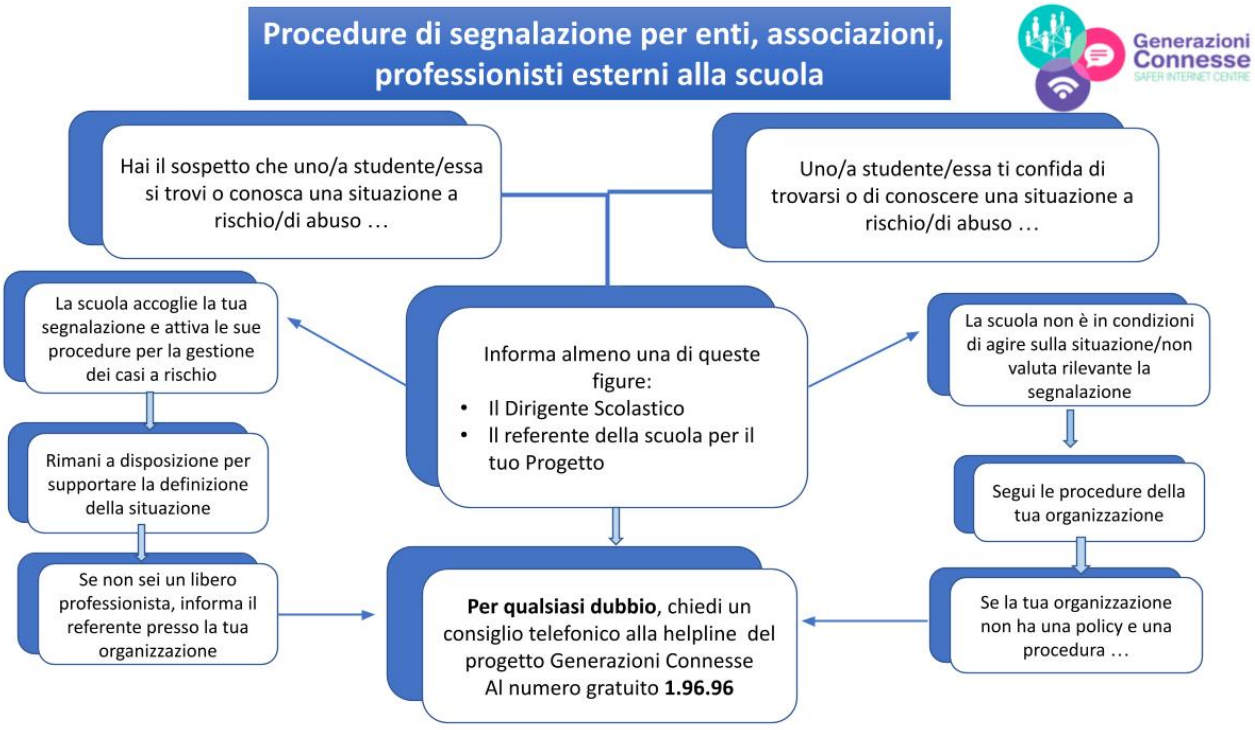
Strumenti a disposizione di studenti/esse

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

In particolare, sarebbe utile che la scuola attivi un sistema di segnalazione utile anche al monitoraggio dei fenomeni dal quale partire per integrare azioni didattiche preventive e giornate di sensibilizzazione, insieme agli Enti/Servizi presenti sul territorio di riferimento. Importante, altresì, immaginare e programmare percorsi di peer education per la prevenzione e il contrasto degli agiti.

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

Procedure



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

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

Se non è già stato fatto, avvisa il referente per il cyberbullismo (e/o il team antibullismo) che attiva le procedure ("Corso 4" della piattaforma ELISA) e il Dirigente Scolastico.
Ricordare sempre che in base alla legge 71-2017:
A) Se c'è fattispecie di reato va fatta la segnalazione alle forze dell'ordine
B) Se non c'è fattispecie di reato.
Il DS (e/o il team antibullismo):
- informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto) su quanto accade e condividete informazioni e strategie.
- Informa i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy)
- Attiva il consiglio di classe.

A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla Polizia Postale:
a) contenuto; b) modalità di diffusione.
Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).

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

NELLE CLASSI
Il team antibullismo collabora coi docenti della classe per realizzare l'intervento nella classe:
a seconda della situazione valuta se
- affrontare direttamente l'accaduto o
- sensibilizzare la classe (vedi Corso 4 Piattaforma Elisa)
- trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo

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

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

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

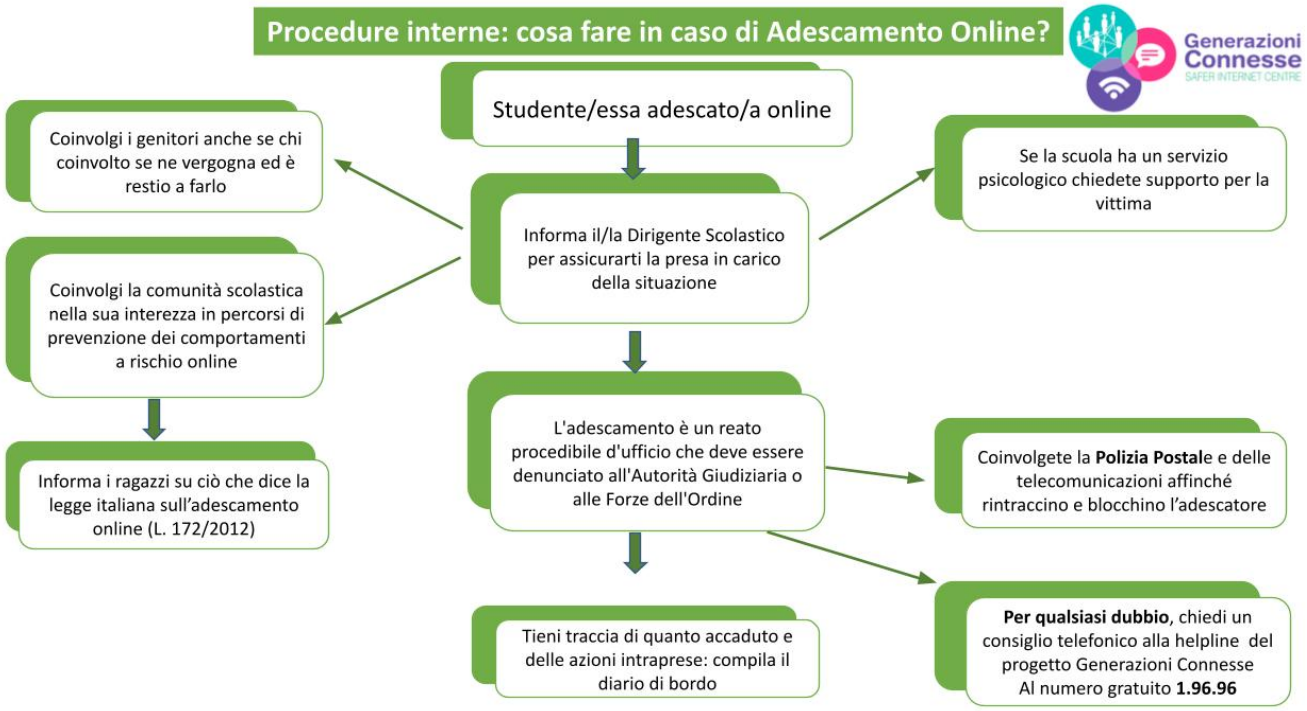
Se emergono evidenze passa allo schema successivo

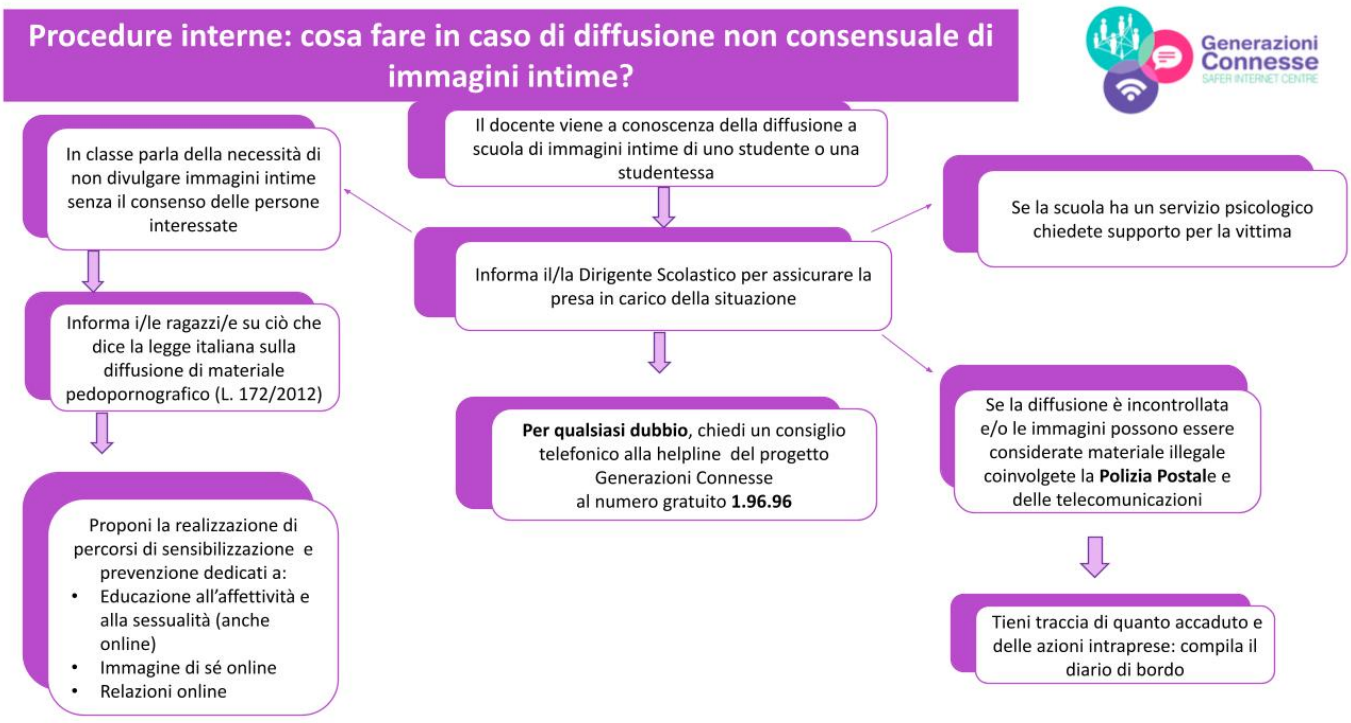
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

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

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

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





Azioni da svolgere nella prossima annualità e nei prossimi tre anni:

Riconferma l'apposita Commissione per il bullismo e il cyberbullismo.

Nomina il referente per il bullismo e cyberbullismo.

Potenzia l'attività dello Sportello d'Ascolto su queste tematiche.

Aggiorna il Regolamento d'Istituto nell'ottica dell'E-Policy.

Crea sul sito una sezione dedicata alle procedure di segnalazione di violazione e alla modulistica specifica, con indicazione dei principali Enti e Servizi a cui rivolgersi per assistenza e tutela.

Organizza periodicamente attività di formazione e divulgazione relativa alle procedure e alla documentazione per la gestione dei casi a favore del personale scolastico interno e delle famiglie.