Documento di ePolicy
I.C. BRANDIZZO

VIA ALBA 10 - 10032 - BRANDIZZO
Torino (TO) - Piemonte
Data di approvazione: 21/04/2026 - 06:34

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.

Perché è importante dotarsi di una ePolicy

Attraverso l'adozione della presente ePolicy, il nostro Istituto si dota di uno strumento di riferimento operativo e educativo rivolto all'intera comunità scolastica, finalizzato a promuovere un utilizzo delle tecnologie digitali consapevole, critico e responsabile.

L'ePolicy rappresenta un quadro di indirizzo condiviso che orienta le azioni della scuola nell'ambito della cittadinanza digitale, favorendo la diffusione di una cultura dell'uso positivo e consapevole della rete. Essa individua principi, regole e buone pratiche utili a valorizzare le opportunità offerte dalle tecnologie digitali e, al contempo, a prevenire e gestire i rischi connessi all'utilizzo di Internet e degli strumenti digitali.

Il documento fornisce pertanto linee guida per la promozione del benessere digitale, definendo modalità di utilizzo delle TIC negli ambienti scolastici e ponendo le basi per azioni formative, educative e di sensibilizzazione rivolte a studenti, docenti, personale amministrativo e famiglie.

Le tecnologie digitali costituiscono infatti importanti strumenti di conoscenza, comunicazione, partecipazione e apprendimento per i giovani; tuttavia, il loro utilizzo può esporre a rischi quali comportamenti offensivi, fenomeni di derisione, contatti inappropriati o altre forme di abuso online. Per questo motivo risulta fondamentale promuovere una cultura della sicurezza e della tutela dei minori, garantendo il diritto degli studenti ad essere protetti e accompagnati nell'uso della rete.

Da diversi anni l'Istituto Comprensivo Gianni Rodari di Brandizzo partecipa al progetto Generazioni Connesse, iniziativa cofinanziata dalla Commissione Europea e promossa dal MIM con il supporto del Safer Internet Centre e finalizzata alla diffusione di strategie, pratiche educative e strumenti utili a rendere il web un ambiente più sicuro per bambini e ragazzi.

La partecipazione al progetto ha consentito all'Istituto di elaborare la prima ePolicy d'Istituto nell'anno scolastico 2017–2018, successivamente aggiornata nell'anno scolastico 2021–2022 e ulteriormente revisionata nel corrente anno scolastico (2025-2026).

Il presente documento si rivolge pertanto a tutti i membri della comunità scolastica – studenti, famiglie, docenti e personale – con l'obiettivo di promuovere un approccio sicuro e responsabile alle tecnologie digitali e di sviluppare una maggiore consapevolezza delle opportunità e dei possibili rischi connessi all'utilizzo della rete.

La presente ePolicy definisce il quadro di riferimento dell'Istituto per la promozione di un uso consapevole, responsabile e sicuro delle tecnologie digitali all'interno della comunità scolastica. Il documento intende stabilire principi, regole e procedure finalizzati a garantire un utilizzo corretto delle risorse digitali nei contesti educativi e didattici, nel rispetto dei diritti e dei doveri di tutti i soggetti coinvolti.

In particolare, la presente ePolicy disciplina:

· l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC) negli ambienti scolastici e nelle attività didattiche, promuovendone un impiego responsabile e consapevole;

· l'impiego degli strumenti di Intelligenza Artificiale a supporto dei processi di insegnamento e apprendimento, nel rispetto dei principi etici, educativi e delle normative vigenti;

· la tutela della privacy e la protezione dei dati personali degli studenti, delle famiglie e del personale scolastico;

· le azioni di prevenzione, monitoraggio e contrasto delle situazioni problematiche connesse all'uso delle tecnologie digitali;

· le procedure di segnalazione e presa in carico dei casi individuati all'interno della scuola;

· le modalità di gestione degli interventi educativi e di supporto, che l'Istituto attiva in collaborazione con le famiglie e con gli enti competenti, a tutela degli studenti coinvolti, sia in qualità di vittime sia di spettatori o responsabili.

L'ePolicy si configura pertanto come uno strumento educativo e organizzativo volto a promuovere una cultura della cittadinanza digitale responsabile e a garantire un ambiente scolastico sicuro, inclusivo e rispettoso dei diritti di tutti.

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.

Ruoli e responsabilità all'interno del nostro I.C.

Affinché la **ePolicy** possa rappresentare uno strumento realmente efficace e operativo, è necessario che tutti i componenti della comunità scolastica – ciascuno in relazione al proprio ruolo – contribuiscano attivamente alla sua attuazione, diffusione e promozione.

La responsabilità educativa relativa all'uso consapevole delle tecnologie digitali è infatti **condivisa** tra scuola, famiglie, studenti e territorio.

IL DIRIGENTE SCOLASTICO

Il Dirigente Scolastico svolge un ruolo di *indirizzo*, *coordinamento* e *supervisione* nell'attuazione della ePolicy e nella promozione di un utilizzo sicuro e responsabile delle tecnologie digitali all'interno dell'Istituto.

In particolare:

- è responsabile della gestione e della tutela dei **dati sensibili e dei dati relativi alla sicurezza** dell'Istituto;
- garantisce la tutela della **privacy e dell'immagine** di tutti i membri della comunità scolastica;
- assicura la presenza di un sistema di **monitoraggio e controllo della sicurezza online** negli ambienti scolastici;
- attiva le procedure previste in caso di **violazione delle norme relative all'utilizzo delle TIC**;
- presiede e coordina il **Team per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo**;
- collabora con i docenti referenti e con i Consigli di classe nella gestione dei casi più complessi legati all'uso improprio delle tecnologie.

Nello specifico il Dirigente Scolastico:

- definisce e integra nel **Piano Triennale dell'Offerta Formativa (PTOF)** e nel **Patto Educativo di Corresponsabilità** (D.P.R. 235/2007) le linee di indirizzo dedicate alla prevenzione e al contrasto del bullismo e del cyberbullismo;
- promuove l'adozione e l'aggiornamento del **Regolamento d'Istituto**, prevedendo disposizioni chiare relative all'uso corretto delle tecnologie digitali;
- garantisce una comunicazione trasparente e costante con le famiglie anche attraverso gli strumenti digitali

istituzionali;
- promuove iniziative formative e di sensibilizzazione in collaborazione con enti, istituzioni, forze dell'ordine e servizi territoriali;
- garantisce la sicurezza della navigazione in rete integrando aspetti tecnici, normativi ed educativi;
- nomina formalmente uno o più docenti **referenti per il bullismo e il cyberbullismo**, su indicazione del Collegio dei Docenti;
- favorisce la stipula di protocolli di collaborazione con i servizi territoriali per il supporto agli studenti coinvolti in situazioni di rischio.

L'ANIMATORE DIGITALE E IL TEAM DIGITALE

L'Animatore Digitale rappresenta una figura di riferimento nel processo di innovazione e digitalizzazione dell'Istituto, favorendo l'integrazione tra **innovazione tecnologica, didattica e cittadinanza digitale**.

In collaborazione con il Team per l'Innovazione Digitale:

- promuove la diffusione di competenze relative alla **scuola digitale** e all'utilizzo consapevole delle tecnologie;
- supporta il personale scolastico nell'utilizzo delle TIC e nella comprensione degli aspetti connessi alla **privacy e alla protezione dei dati personali**;
- monitora le modalità di utilizzo delle tecnologie digitali e della rete all'interno dell'Istituto;
- propone l'introduzione di **pratiche innovative e migliorative** e contribuisce all'aggiornamento dei regolamenti d'Istituto;
- promuove percorsi di **formazione e aggiornamento** rivolti a docenti, studenti e personale ATA;
- collabora alla gestione delle modalità di accesso sicuro alla rete d'Istituto attraverso sistemi di autenticazione e credenziali protette.

L'Animatore Digitale partecipa inoltre:

- alle attività del **Team Digitale**;
- alle iniziative di prevenzione e contrasto del cyberbullismo, su indicazione del Dirigente Scolastico;
- alla diffusione della cultura digitale attraverso progetti interdisciplinari e collaborazioni con esperti esterni.

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO E IL TEAM ANTIBULLISMO

In conformità con quanto previsto dalla **Legge 71/2017**, l'Istituto individua uno o più docenti referenti per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo.

Tali figure:

- progettano, coordinano e monitorano le iniziative di prevenzione;
- coordinano il **Team Antibullismo**;
- collaborano con il Dirigente Scolastico e con i Consigli di classe nella gestione delle situazioni problematiche;
- fungono da raccordo tra scuola, famiglie, servizi territoriali e altre agenzie educative;
- monitorano e rilevano eventuali criticità legate all'uso delle tecnologie digitali;
- contribuiscono alla revisione e all'aggiornamento della **ePolicy**;
- relazionano periodicamente al Dirigente Scolastico sulle attività svolte;
- promuovono la conoscenza delle procedure di intervento previste dalla scuola;
- partecipano a percorsi di aggiornamento e formazione sui temi della sicurezza online.

I/LE DOCENTI

I docenti svolgono un ruolo fondamentale nella promozione di una **cultura della cittadinanza digitale responsabile**.

In particolare:

- curano la propria formazione sull'utilizzo delle tecnologie digitali e della rete;
- integrano, ove possibile, contenuti di **educazione digitale** nei percorsi disciplinari;
- accompagnano e supportano gli studenti nelle attività didattiche che prevedono l'utilizzo di dispositivi digitali;
- favoriscono lo sviluppo delle **competenze digitali** degli studenti e un utilizzo consapevole della rete;
- utilizzano esclusivamente i **canali istituzionali della scuola** per le comunicazioni con studenti e famiglie;
- garantiscono la riservatezza dei dati personali nel rispetto della normativa vigente;
- segnalano tempestivamente eventuali problematiche o episodi di uso improprio delle tecnologie;
- collaborano con i referenti e con il Dirigente nella gestione delle situazioni critiche;
- custodiscono e non divulgano le **credenziali di accesso alla rete d'Istituto**.

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

Il personale ATA contribuisce al buon funzionamento dell'Istituto anche sotto il profilo della **sicurezza digitale e della tutela degli studenti**.

In particolare:

- conosce e rispetta le disposizioni contenute nella ePolicy;
- contribuisce, per quanto di competenza, alla vigilanza sugli studenti;
- garantisce la riservatezza dei dati personali trattati;
- non divulga le credenziali di accesso alla rete d'Istituto;
- segnala eventuali comportamenti non adeguati o situazioni problematiche.

Il **Direttore dei Servizi Generali e Amministrativi (DSGA)**, in particolare:

- assicura, nei limiti delle risorse disponibili, il supporto tecnico necessario al corretto funzionamento delle dotazioni tecnologiche;
- garantisce il funzionamento dei principali **canali di comunicazione digitale della scuola** tra istituto, personale e famiglie.

GLI STUDENTI E LE STUDENTESSE

Gli studenti sono chiamati a partecipare attivamente alla costruzione di una **cittadinanza digitale consapevole e responsabile**.

Con il supporto dei docenti:

- utilizzano le tecnologie digitali nel rispetto delle indicazioni fornite dagli insegnanti;
- adottano comportamenti corretti e rispettosi anche nelle comunicazioni online;
- comprendono l'importanza delle **buone pratiche di sicurezza in rete**;
- segnalano tempestivamente eventuali malfunzionamenti delle attrezzature o contenuti inappropriati;
- partecipano alle attività educative e ai progetti di prevenzione del bullismo e del cyberbullismo, anche attraverso percorsi di **peer education**.

I GENITORI O GLI ADULTI DI RIFERIMENTO

I genitori o gli adulti di riferimento svolgono un ruolo essenziale nel **Patto Educativo di Corresponsabilità** con la scuola.

In base alla normativa vigente, essi sono chiamati a:

- collaborare con la scuola nella sensibilizzazione dei figli sull'uso sicuro della rete;
- condividere e sostenere le regole stabilite dall'Istituto;

- vigilare sull'utilizzo di Internet e dei dispositivi digitali da parte dei minori;
- partecipare alle iniziative formative e informative promosse dalla scuola;
- collaborare con l'Istituto nella prevenzione e nella gestione delle situazioni problematiche.

ENTI ESTERNI, ISTITUZIONI E ASSOCIAZIONI

Gli enti e le associazioni che collaborano con l'Istituto contribuiscono alla promozione di una **cultura della sicurezza e della cittadinanza digitale**.

Nell'ambito delle attività realizzate in collaborazione con la scuola:

- condividono e rispettano i principi e le disposizioni della presente ePolicy;
- promuovono comportamenti responsabili nell'uso delle tecnologie digitali;
- garantiscono la sicurezza degli studenti durante le attività svolte;
- operano nel rispetto della normativa vigente in materia di **protezione dei dati personali**, in conformità al **Regolamento UE 2016/679** e alla normativa nazionale.

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.

La trasversalità della **ePolicy** rende necessaria la sua integrazione all'interno dei principali documenti che regolano il funzionamento e l'organizzazione dell'Istituto Scolastico Gianni Rodari.

Il **Regolamento d'Istituto**, quale principale riferimento normativo per la vita della comunità scolastica, deve essere aggiornato al fine di recepire i principi della ePolicy, richiamando in modo esplicito le norme comportamentali e le procedure relative all'utilizzo delle **Tecnologie dell'Informazione e della Comunicazione (TIC)** negli ambienti scolastici.

Anche il **Patto Educativo di Corresponsabilità** tra scuola e famiglia deve essere integrato con specifici riferimenti alla ePolicy, evidenziando, da un lato, l'impegno dell'Istituto a promuovere iniziative di informazione e formazione rivolte ai genitori/adulti di riferimento sui temi della sicurezza digitale e della cittadinanza digitale e, dall'altro, la responsabilità degli stessi nel partecipare attivamente a tali momenti formativi e nel condividere con la scuola le azioni educative finalizzate a un utilizzo consapevole delle tecnologie.

Il **Piano Triennale dell'Offerta Formativa (PTOF)**, quale documento fondamentale che definisce l'identità culturale e progettuale dell'Istituto, deve inoltre includere le progettualità e le azioni educative connesse al percorso di **media education**, di educazione alla cittadinanza digitale e di prevenzione dei rischi legati all'uso della rete, in coerenza con gli obiettivi della ePolicy.

Così come il PTOF rappresenta il risultato di un processo di partecipazione e condivisione tra tutte le componenti della comunità scolastica – Dirigente Scolastico, docenti, personale, studenti, famiglie e territorio – anche il **Patto di Corresponsabilità** esprime l'assunzione di impegni educativi condivisi da parte di tutti i soggetti coinvolti nella comunità educante.

In tale prospettiva, tutti i soggetti che, a diverso titolo, entrano in relazione educativa con gli studenti e le studentesse – personale scolastico, esperti esterni, enti e associazioni del territorio – sono tenuti ad adottare comportamenti coerenti con i principi educativi e con le disposizioni contenute nella presente ePolicy.

In particolare, essi sono chiamati a mantenere un **elevato profilo personale e professionale**, improntato al rispetto, alla responsabilità e alla tutela del **superiore interesse del minore**, ascoltando e prendendo in seria considerazione le opinioni e le eventuali preoccupazioni espresse dagli studenti e dalle studentesse.

Non sono in alcun modo consentiti comportamenti irrispettosi, offensivi o lesivi della **dignità, della privacy e degli spazi personali** degli studenti e delle studentesse, né atteggiamenti che possano tollerare o favorire comportamenti illegali, abusivi o comunque tali da mettere a rischio la sicurezza e il benessere dei minori.

Tutti i soggetti esterni che collaborano con l'Istituto sono inoltre tenuti a conoscere e rispettare le disposizioni previste dal Regolamento d'Istituto in merito all'utilizzo dei **dispositivi digitali personali** (smartphone, tablet, computer) e delle strumentazioni tecnologiche messe a disposizione dalla scuola, evitando qualsiasi utilizzo improprio o non conforme alle finalità educative delle attività svolte con gli studenti.

Particolare attenzione deve essere posta al rispetto della **normativa sulla protezione dei dati personali**, soprattutto quando riguarda soggetti minorenni. Non è pertanto consentita la diffusione o la condivisione non autorizzata di fotografie, immagini, video o altri materiali che ritraggano studenti e studentesse, né lo scambio di contatti personali (numeri telefonici, indirizzi e-mail, chat o profili di social network) al di fuori dei canali istituzionali e delle procedure autorizzate.

Le organizzazioni e le associazioni che collaborano con l'Istituto, nel prendere parte alle attività educative rivolte agli studenti, dichiarano di **conoscere e condividere i principi della presente ePolicy**, impegnandosi a promuovere comportamenti responsabili e sicuri nell'utilizzo della rete e delle tecnologie digitali.

Tali soggetti sono inoltre chiamati a segnalare tempestivamente ai docenti referenti e al Dirigente Scolastico eventuali situazioni problematiche, comportamenti scorretti o casi di uso improprio delle tecnologie digitali e della rete, prestando particolare attenzione alle eventuali segnalazioni o preoccupazioni espresse dagli studenti e dalle studentesse.

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.

Condivisione e comunicazione della ePolicy all'interno della comunità scolastica dell'Istituto Gianni Rodari di Brandizzo

Il documento di **ePolicy** viene condiviso con l'intera comunità educante, ponendo al centro il benessere e la tutela degli studenti e delle studentesse e valorizzando il ruolo e le responsabilità di tutti i soggetti coinvolti nel processo educativo.

È fondamentale che ciascun componente della comunità scolastica – dirigenti, docenti, personale, studenti e famiglie –

contribuisca alla **diffusione e alla promozione dei principi contenuti nella ePolicy**, favorendo una cultura dell'uso consapevole, responsabile e sicuro delle tecnologie digitali.

La ePolicy viene resa nota e condivisa con la comunità scolastica attraverso diverse modalità, tra cui:

- la **pubblicazione del documento sul sito istituzionale dell'Istituto**;
- il **Patto Educativo di Corresponsabilità**, sottoscritto dalle famiglie all'inizio dell'anno scolastico;
- momenti di informazione e confronto negli **organi collegiali della scuola**.

Il documento viene approvato dal **Collegio dei Docenti** e dal **Consiglio di Istituto**. Una versione sintetica e semplificata delle principali regole relative all'uso delle tecnologie digitali viene inoltre esposta negli spazi dell'Istituto in cui sono presenti computer o dispositivi collegati alla rete Internet.

Gli studenti e le studentesse sono informati del fatto che l'utilizzo delle tecnologie digitali e della rete negli ambienti scolastici avviene sotto la **supervisione dei docenti**, nel rispetto delle regole stabilite dall'Istituto e delle finalità educative delle attività didattiche.

La scuola si impegna a promuovere azioni di **informazione, sensibilizzazione e formazione** rivolte a tutta la comunità scolastica, attraverso iniziative dedicate a studenti, docenti e famiglie, anche con il coinvolgimento di esperti esterni e di enti del territorio.

1. Condivisione e comunicazione della ePolicy agli studenti e alle studentesse

Gli studenti e le studentesse vengono informati sulle regole che disciplinano l'utilizzo della rete e dei dispositivi digitali all'interno della scuola. Essi sono consapevoli che l'accesso a Internet e l'uso delle tecnologie digitali negli ambienti scolastici avvengono **sotto la guida e la supervisione dei docenti** e esclusivamente per finalità didattiche ed educative.

L'Istituto promuove inoltre attività educative e laboratoriali, incontri, progetti e iniziative finalizzate a sviluppare negli studenti una maggiore consapevolezza delle **opportunità e dei rischi connessi all'uso della rete**, favorendo lo sviluppo delle competenze di cittadinanza digitale.

2. Condivisione e comunicazione della ePolicy al personale scolastico

Le disposizioni adottate dall'Istituto in materia di **sicurezza digitale e utilizzo responsabile delle tecnologie** vengono condivise con il personale scolastico nell'ambito degli organi collegiali e attraverso la pubblicazione del presente documento.

Al fine di favorire una più ampia diffusione delle regole relative alla sicurezza online, una sintesi delle principali indicazioni operative viene resa disponibile negli ambienti scolastici dotati di accesso alla rete Internet, quali aule e laboratori.

3. Condivisione e comunicazione della ePolicy alle famiglie

Le famiglie vengono informate sulle linee guida adottate dall'Istituto per promuovere un **utilizzo sicuro e responsabile delle tecnologie digitali e della rete**, attraverso la condivisione della ePolicy pubblicata sul sito istituzionale della scuola.

Al fine di rafforzare la collaborazione educativa tra scuola e famiglia, l'Istituto promuove inoltre **incontri informativi e momenti di confronto** dedicati ai temi della cittadinanza digitale, della sicurezza online e dell'uso consapevole delle tecnologie, durante i quali viene presentata e approfondita la presente ePolicy.

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

1.5 – I Piani di Azione dell'ePolicy – I.C. Gianni Rodari di Brandizzo

L'Istituto di Brandizzo, in coerenza con le Linee Guida ministeriali e nell'ambito del percorso promosso dal progetto *Generazioni Connesse*, ha definito un piano triennale di azioni strategiche finalizzate alla piena attuazione dell'ePolicy d'Istituto.

I Piani di Azione rappresentano lo strumento operativo attraverso il quale la scuola promuove, sviluppa e monitora iniziative volte alla diffusione di una cultura digitale consapevole, sicura e responsabile, coinvolgendo l'intera comunità scolastica.

All'interno dei Piani sono esplicitati obiettivi, impegni e responsabilità che l'Istituto assume in relazione a:

- la rilevazione dei bisogni formativi di docenti, studenti e famiglie;
- la progettazione e realizzazione di percorsi informativi e formativi strutturati;
- l'integrazione dell'ePolicy nei documenti ufficiali dell'Istituto (Regolamento d'Istituto, PTOF, Patto di corresponsabilità);
- il monitoraggio sistematico delle azioni intraprese e la valutazione dei risultati, con particolare attenzione ai principi di accessibilità e inclusione.

I Piani di Azione si articolano in:

- **azioni standard**, comuni alle scuole aderenti al progetto;
- **azioni contestualizzate**, definite sulla base delle specificità dell'Istituto, del contesto territoriale e delle collaborazioni attive con enti e realtà locali.

Primo anno di attuazione – Azioni previste

Modulo I – Comunicazione e diffusione dell'ePolicy e formazione della comunità scolastica

- Organizzazione di eventi di presentazione del progetto *Generazioni Connesse* rivolti a studenti, docenti e genitori;
- Realizzazione di un incontro specifico di presentazione e approfondimento dell'ePolicy destinato ai docenti;

- Partecipazione a iniziative e progetti promossi dal territorio sui temi della cittadinanza digitale.

Modulo II – Analisi dei bisogni

- Rilevazione del fabbisogno formativo del personale docente sui temi dell'educazione civica digitale e della cittadinanza digitale.

Modulo III – Integrazione normativa

- Inserimento e armonizzazione dei contenuti dell'ePolicy nei principali documenti regolamentari dell'Istituto (Regolamento d'Istituto, PTOF, Regolamento disciplinare).

Modulo IV – Prevenzione e segnalazione

- Definizione di procedure chiare e accessibili per la segnalazione di episodi critici o comportamenti a rischio, utilizzando un linguaggio adeguato anche agli studenti;
- Attivazione di un sistema strutturato di raccolta dati e monitoraggio delle segnalazioni, finalizzato alla trasparenza, alla prevenzione e al miglioramento continuo.

Secondo anno di attuazione – Consolidamento delle pratiche

Modulo I – Formazione della comunità scolastica

- Realizzazione di laboratori didattici sulle tematiche del bullismo e del cyberbullismo;
- Organizzazione di incontri con le famiglie per rafforzare l'alleanza educativa scuola–famiglia e condividere strategie di prevenzione e intervento;
- Promozione di eventi di diffusione e conoscenza dell'ePolicy rivolti a studenti e genitori.

Modulo II – Educazione civica digitale per studenti e famiglie

- Introduzione sperimentale, in classi pilota, del kit didattico del progetto *Generazioni Connesse* quale supporto metodologico per l'educazione digitale;
- Rilevazione sistematica dei comportamenti, delle abitudini e dei bisogni degli studenti in relazione all'uso delle tecnologie;
- Attivazione di moduli formativi dedicati agli studenti mediante l'utilizzo della piattaforma *Generazioni Connesse*;
- Realizzazione di una sezione dedicata del sito web d'Istituto contenente materiali informativi, documenti e risorse utili sui temi del bullismo e del cyberbullismo, accessibile a tutta la comunità scolastica.

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

Utilizzo delle risorse della piattaforma Generazioni Connesse

Nell'ambito del percorso di implementazione della **ePolicy**, l'Istituto Comprensivo Gianni Rodari intende valorizzare e integrare in modo sistematico le risorse messe a disposizione dalla piattaforma **Generazioni Connesse**, adattandole al contesto educativo dell'Istituto, alle caratteristiche della popolazione studentesca e ai bisogni formativi espressi dal territorio.

In particolare, l'Istituto prevede di utilizzare e personalizzare alcune delle principali risorse didattiche e formative offerte dalla piattaforma, integrandole nei percorsi educativi e nelle attività di formazione rivolte alla comunità scolastica.

1. Kit didattico

Il **Kit Didattico** sarà introdotto progressivamente in alcune classi come strumento metodologico per affrontare tematiche legate alla **cittadinanza digitale**, alla sicurezza in rete, al rispetto della privacy e alla prevenzione dei fenomeni di bullismo e cyberbullismo.

I docenti coinvolti provvederanno ad adattare i materiali alle diverse **fasce d'età degli studenti**, integrandoli all'interno dei percorsi di **Educazione Civica** e delle attività di educazione alla cittadinanza digitale previste dal curricolo d'Istituto.

2. Area formazione

L'Istituto promuove l'utilizzo dell'**Area Formazione** della piattaforma Generazioni Connesse come strumento di aggiornamento e crescita professionale per il personale scolastico e come supporto per attività di sensibilizzazione rivolte alla comunità educante.

In particolare si prevede di:

- promuovere la formazione dei docenti sui contenuti fondamentali della ePolicy e sui temi della sicurezza online, anche attraverso percorsi digitali disponibili sulla piattaforma o con il supporto di esperti esterni, con l'obiettivo di coinvolgere almeno il **60% del corpo docente entro il secondo anno di attuazione** del piano;
- organizzare momenti di informazione e sensibilizzazione rivolti alle **famiglie**, utilizzando i materiali formativi messi a disposizione dalla piattaforma;
- coinvolgere gli **studenti e le studentesse** in percorsi educativi guidati, da realizzare sia in presenza sia online, coordinati dai docenti referenti per la cittadinanza digitale.

3. Canale YouTube

I contenuti video pubblicati sul canale YouTube di **Generazioni Connesse** saranno utilizzati come materiali di supporto alle attività didattiche e come stimolo per momenti di confronto e riflessione in classe.

I video potranno essere impiegati nell'ambito di **discussioni guidate, laboratori, lavori di gruppo e attività di approfondimento**, nonché durante eventi informativi e incontri rivolti alle famiglie sui temi della sicurezza online e della cittadinanza digitale.

4. Canali social

I canali social ufficiali di **Generazioni Connesse** (tra cui TikTok, Instagram e Facebook) saranno segnalati a studenti e famiglie come **fonti informative affidabili e autorevoli** per approfondire i temi trattati nell'ambito dei percorsi di educazione digitale.

Alcuni contenuti selezionati potranno inoltre essere presentati in classe per avviare momenti di riflessione critica sull'uso consapevole dei **social media**, favorendo lo sviluppo di competenze di cittadinanza digitale responsabile.

Monitoraggio e valutazione delle azioni previste

L'Istituto Comprensivo Gianni Rodari prevede di accompagnare l'attuazione delle azioni descritte nella presente sezione con attività di **monitoraggio e valutazione periodica**, al fine di verificarne l'efficacia e garantire un progressivo miglioramento delle pratiche educative legate alla cittadinanza digitale.

Il monitoraggio delle attività sarà coordinato dal **Team digitale** e dai **docenti referenti per il bullismo e il cyberbullismo**, in collaborazione con il Dirigente Scolastico e con gli organi collegiali della scuola.

In particolare verranno presi in considerazione alcuni **indicatori di attuazione**, tra cui:

- il numero di **docenti coinvolti nei percorsi formativi** promossi attraverso l'Area Formazione della piattaforma Generazioni Connesse;
- il numero di **classi che utilizzano il Kit Didattico** nei percorsi di Educazione Civica e di educazione alla cittadinanza digitale;
- la partecipazione di **studenti e famiglie** agli incontri informativi e alle iniziative di sensibilizzazione promosse dall'Istituto;
- la realizzazione di **attività didattiche e laboratoriali** finalizzate alla prevenzione dei rischi della rete e alla promozione di comportamenti responsabili online.

I risultati del monitoraggio saranno condivisi periodicamente negli **organi collegiali della scuola** e potranno costituire la base per eventuali aggiornamenti della ePolicy e per l'implementazione di nuove azioni educative.

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.

Rischi online, sensibilizzazione e prevenzione

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

- mettere in atto comportamenti digitali potenzialmente dannosi per sé stesso o per gli altri;
- essere vittima di comportamenti lesivi;
- assistere, in qualità di spettatore, a tali dinamiche.

In relazione a tali rischi, l'Istituto adotta un approccio educativo integrato fondato su azioni di **sensibilizzazione** e **prevenzione**, rivolte all'intera comunità scolastica.

Sensibilizzazione

Le attività di sensibilizzazione vengono avviate a partire dalla scuola primaria, con particolare riferimento alle classi quarte e quinte, e proseguono lungo tutto il percorso della scuola secondaria di primo grado.

L'obiettivo non è soltanto informativo, ma principalmente educativo: promuovere negli studenti consapevolezza, senso critico e responsabilità nell'uso delle tecnologie digitali. In tale prospettiva, vengono affrontate le seguenti tematiche:

- uso consapevole e abuso di Internet;
- dipendenza da dispositivi digitali, in particolare dallo smartphone;
- utilizzo responsabile dei social network.

Prevenzione

Parallelamente alle azioni di sensibilizzazione, l'Istituto promuove interventi di prevenzione volti allo sviluppo delle competenze digitali e relazionali, con particolare attenzione a:

- la tutela della privacy personale e altrui;
- la conoscenza e il rispetto delle regole di comportamento (netiquette) nella navigazione in rete e nella pubblicazione/condivisione di contenuti;

- la riflessione sui comportamenti online, evidenziando come l'apparente anonimato possa favorire atteggiamenti scorretti o lesivi;
- l'approfondimento dei rischi connessi a un uso non consapevole delle tecnologie digitali, nonché delle possibili conseguenze civili e penali derivanti da comportamenti inappropriati.

Coinvolgimento della comunità scolastica

Al fine di rafforzare l'efficacia delle azioni educative, l'Istituto promuove il coinvolgimento attivo dell'intera comunità scolastica attraverso:

- incontri formativi con le Forze dell'Ordine sui temi della sicurezza in rete;
- la partecipazione degli studenti della scuola secondaria di primo grado al progetto **"Un patentino per lo smartphone"**, in collaborazione con l'ASL TO4;
- l'organizzazione di momenti informativi rivolti a genitori e alunni, a partire dalla scuola primaria, con il supporto dei materiali del progetto *Generazioni Connesse*;
- la partecipazione al **Safer Internet Day**, quale occasione di riflessione condivisa sull'uso sicuro e responsabile della rete;
- la realizzazione di percorsi di educazione all'affettività e alla cittadinanza, in un'ottica di prevenzione dei comportamenti a rischio anche nel contesto digitale.

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.

L'Istituto Comprensivo di Brandizzo riconosce l'innovazione didattica e la cittadinanza digitale come pilastri del proprio piano formativo. Per tale ragione, il Curricolo Digitale non è inteso come una disciplina isolata, ma come un percorso trasversale che integra le risorse nazionali e internazionali con l'identità progettuale della scuola.

- **Riferimento ai Framework Europei (DigComp 2.2):** L'Istituto adotta il framework europeo **DigComp 2.2** per definire e monitorare le competenze digitali di studenti, docenti e personale. Questa cornice permette di strutturare percorsi che vanno oltre l'uso tecnico degli strumenti, focalizzandosi sulla gestione delle informazioni, la creazione di contenuti e, soprattutto, la sicurezza e il benessere online.

- **Integrazione con l'Educazione Civica (L. 92/2019):** In coerenza con il PTOF, il curricolo di **Cittadinanza Digitale** è parte integrante dell'insegnamento dell'Educazione Civica. Le attività didattiche sono progettate per trasformare i principi della presente e-Policy in comportamenti quotidiani, rendendo gli studenti protagonisti consapevoli delle dinamiche di rete.

- **Progetti Qualificanti dell'Istituto:** Il curricolo trova attuazione pratica attraverso iniziative specifiche già consolidate nel piano triennale:

    - **Progetto "Un patentino per lo smartphone":** un percorso mirato a fornire agli alunni della scuola secondaria le basi giuridiche, etiche e tecniche per un uso responsabile del dispositivo mobile.

    - **Lotta alle Fake News:** laboratori dedicati allo sviluppo dello spirito critico e alla verifica delle fonti (fact-checking) per contrastare la disinformazione.

    - **Prevenzione del Cyberbullismo:** l'adesione alla rete **"#NoBullismo – La Rete siamo Noi"** e l'organizzazione di spettacoli teatrali antibullismo, che utilizzano linguaggi espressivi per sensibilizzare sui rischi della prevaricazione online.

- **Metodologie e Strumenti:** Grazie alla dotazione di **Aule 3.0, laboratori STEM e oltre 200 dispositivi (PC e Tablet)**, il curricolo digitale si avvale di metodologie attive quali la *Flipped Classroom* e il *Project-Based Learning*. In ogni classe è previsto un appuntamento didattico specifico, calibrato sull'età, che utilizza i kit ministeriali (es. Generazioni Connesse) per approfondire le finalità della e-Policy.

- **Coinvolgimento delle Famiglie:** L'Istituto promuove azioni di sensibilizzazione rivolte ai genitori, affinché la cultura della prevenzione e dell'uso positivo delle tecnologie trovi continuità nel contesto domestico, creando un'alleanza educativa solida tra scuola e famiglia.

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.

Materiali e strumenti utilizzati dall'Istituto

L'Istituto si avvale di materiali didattici e risorse educative finalizzate a promuovere negli studenti un uso consapevole, sicuro e responsabile delle tecnologie digitali.

I docenti possono utilizzare, in particolare, il **Kit Didattico del progetto *Generazioni Connesse***, integrandolo con ulteriori risorse digitali selezionate, per affrontare in classe tematiche quali:

- la sicurezza in rete;
- la tutela dei dati personali e della privacy;
- l'uso corretto e responsabile dei social network;
- la prevenzione del bullismo e del cyberbullismo.

Le attività didattiche sono progettate secondo **metodologie attive e partecipative** e prevedono momenti di riflessione, discussioni guidate, lavori di gruppo e percorsi di approfondimento. Tali approcci favoriscono lo sviluppo delle competenze di **cittadinanza digitale** e promuovono il rispetto delle regole della comunicazione online.

I materiali e gli strumenti utilizzati vengono sistematicamente integrati nella programmazione didattica e nei percorsi di educazione civica, contribuendo alla formazione di studenti consapevoli, responsabili e capaci di un utilizzo critico delle tecnologie digitali.

Materiali e strumenti utilizzati dall'Istituto

L'Istituto si avvale di materiali didattici e risorse educative finalizzate a promuovere negli studenti un uso consapevole, sicuro e responsabile delle tecnologie digitali.

I docenti possono utilizzare, in particolare, il **Kit Didattico del progetto *Generazioni Connesse***, integrandolo con ulteriori risorse digitali selezionate, per affrontare in classe tematiche quali:

- la sicurezza in rete;
- la tutela dei dati personali e della privacy;
- l'uso corretto e responsabile dei social network;
- la prevenzione del bullismo e del cyberbullismo.

Le attività didattiche sono progettate secondo **metodologie attive e partecipative** e prevedono momenti di riflessione, discussioni guidate, lavori di gruppo e percorsi di approfondimento. Tali approcci favoriscono lo sviluppo delle competenze di **cittadinanza digitale** e promuovono il rispetto delle regole della comunicazione online.

I materiali e gli strumenti utilizzati vengono sistematicamente integrati nella programmazione didattica e nei percorsi di educazione civica, contribuendo alla formazione di studenti consapevoli, responsabili e capaci di un utilizzo critico delle tecnologie digitali.

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.

La protezione dei dati personali costituisce un diritto fondamentale (Art. 8 Carta dei diritti UE; Art. 16 TFUE). L'IC Brandizzo opera nel pieno rispetto del **GDPR (Regolamento UE 2016/679)** e del **D.Lgs. 196/2003**, riconoscendo la delicatezza del trattamento di dati sensibili in ambito educativo.

- **Organizzazione:** L'Istituto ha definito un organigramma privacy e nominato un Responsabile della Protezione dei Dati (DPO/RPD). I dati sono gestiti tramite registri di trattamento costantemente aggiornati.

- **Informativa e Trasparenza:** Come previsto dal PTOF, la scuola adotta procedure di dematerializzazione sicura (PEO, PEC, protocollo informatico) e assicura che ogni raccolta dati (iscrizioni, attività didattiche) sia accompagnata da informative chiare per le famiglie.

- **Sicurezza dei dati:** L'Istituto si impegna a formare il personale (ATA e Docenti) sulla gestione dei flussi documentali e sulla protezione dei dati degli alunni, considerandola non solo un obbligo di legge, ma un elemento essenziale del "benessere a scuola" promosso nel piano triennale.

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.

La P.U.A. dell'IC Brandizzo è il documento cardine che regola l'accesso alla rete scolastica, integrante il Documento Programmatico sulla Sicurezza (DPS). Essa mira a bilanciare le potenzialità della didattica digitale con la mitigazione dei rischi.

- **Uso Consapevole:** In linea con il progetto **"Un patentino per lo smartphone"** citato nel PTOF, la P.U.A. non è solo sanzionatoria ma educativa. L'uso della rete è finalizzato alla ricerca di materiali consoni allo stile educativo della scuola.
- **Divieti Operativi:** È fatto divieto di utilizzare la rete scolastica per attività illecite, gioco d'azzardo online, violazione del diritto d'autore o diffusione di contenuti che ledano la dignità della persona.
- **Prevenzione Rischi:** Coerentemente con il progetto **"#NoBullismo – La Rete siamo Noi"**, la P.U.A. definisce le regole per prevenire il cyberbullismo, promuovendo il rispetto reciproco anche negli spazi virtuali e l'uso critico delle fonti per contrastare le *fake news*.

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.

L'IC Brandizzo recepisce le indicazioni del Ministero dell'Istruzione (dieci punti per il BYOD), integrando l'uso dei dispositivi personali nelle attività didattiche quotidiane per favorire l'inclusione e l'innovazione.

- **Finalità Didattica:** L'uso di smartphone, tablet o PC personali in classe è consentito esclusivamente sotto la supervisione del docente e per finalità di apprendimento, come previsto dalle metodologie attive (Flipped Classroom, laboratori STEM) descritte nel PTOF.

- **Regolamentazione Condivisa:** L'Istituto promuove un dialogo costante tra docenti, studenti e famiglie per definire regole condivise che trasformino il dispositivo da elemento di distrazione a strumento di cittadinanza attiva.

- **Equità e Inclusione:** L'uso del BYOD è supportato dalla dotazione tecnologica dell'Istituto (oltre 200 dispositivi tra PC e Tablet e Aule 3.0), garantendo che nessun alunno sia escluso dalle attività digitali qualora non possieda un dispositivo proprio.

- **Sicurezza e Responsabilità:** Ogni utente che accede alla rete dell'Istituto con un proprio dispositivo è tenuto al rispetto della privacy altrui, con particolare divieto di effettuare riprese o fotografie senza esplicita autorizzazione didattica.

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.

Procedure di segnalazione e gestione dei casi nel nostro Istituto

Il personale docente dell'Istituto, qualora rilevi il sospetto o la certezza che uno/a studente/essa sia coinvolto/a, in qualità di vittima o autore, in **episodi di cyberbullismo, sexting o adescamento online**, fa riferimento a procedure condivise e definite, attivando la rete di supporto interna alla comunità scolastica.

Situazioni di disagio possono emergere attraverso segnali indiretti, quali atteggiamenti di insofferenza nei confronti dei pari, dinamiche di esclusione o isolamento, oppure tramite segnalazioni dirette da parte degli studenti stessi, anche in relazione a fatti avvenuti al di fuori del contesto scolastico.

La crescente diffusione dei social network tra bambini e adolescenti espone gli studenti al rischio di condividere contenuti personali o sensibili in modo non protetto. Le attività di confronto e riflessione svolte in classe sui rischi del web e sulle esperienze digitali favoriscono l'emersione di situazioni potenzialmente critiche, che richiedono attenzione da parte dei docenti.

Nel rispetto delle norme vigenti, il personale scolastico può intervenire sui dispositivi in uso all'interno dell'ambiente scolastico; eventuali interventi su dispositivi personali degli studenti sono subordinati all'esplicita autorizzazione delle famiglie.

Sono oggetto di segnalazione tutte le situazioni riconducibili a:

- episodi di bullismo e cyberbullismo, intesi come comportamenti intenzionali e ripetuti finalizzati a offendere, minacciare, diffamare o danneggiare una persona o un gruppo, sia in presenza sia online;
- utilizzi inappropriati della rete, quali l'accesso a contenuti non idonei all'età, la frequentazione di siti d'odio o altre esperienze digitali a rischio.

I docenti di classe provvedono a informare tempestivamente il Referente d'Istituto per il bullismo e il cyberbullismo, il quale, a sua volta, coinvolge il Dirigente Scolastico. Quest'ultimo, in relazione alla gravità dei fatti, attiva le procedure previste, inclusa la convocazione delle famiglie degli studenti interessati.

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.

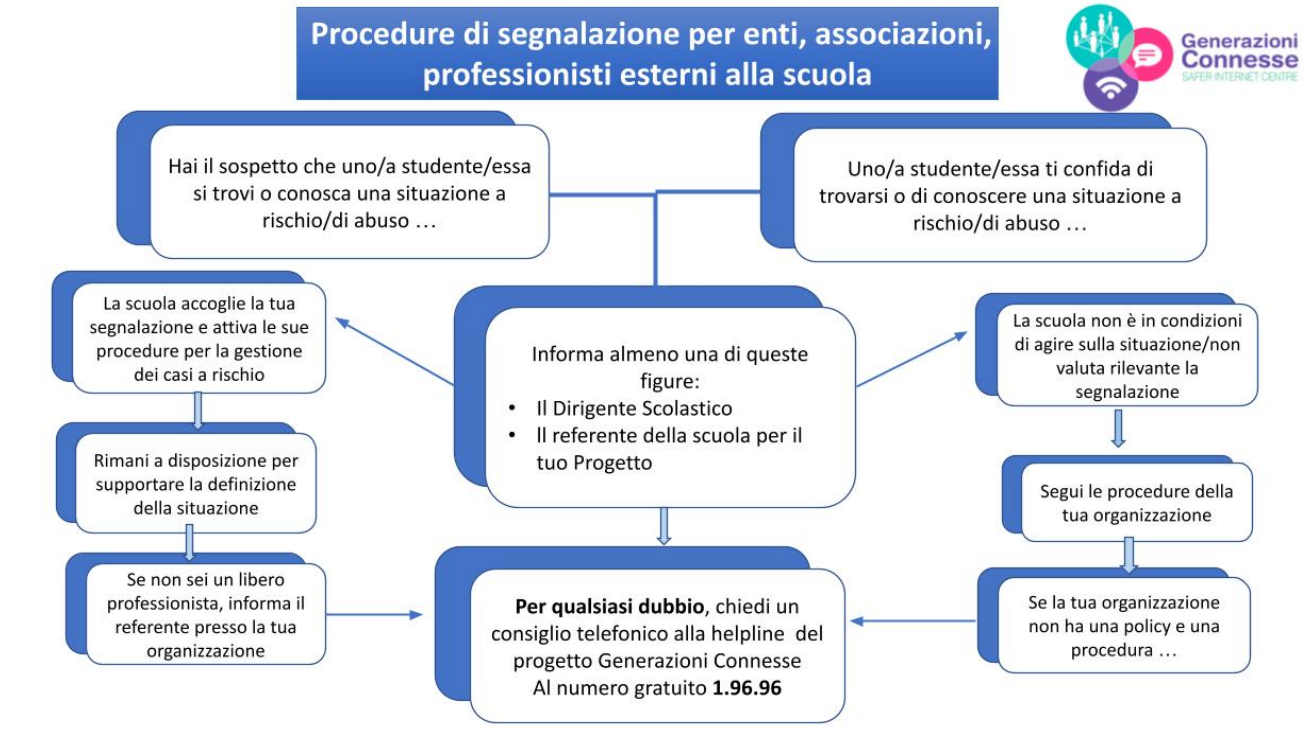
Strumenti a disposizione di studenti/esse

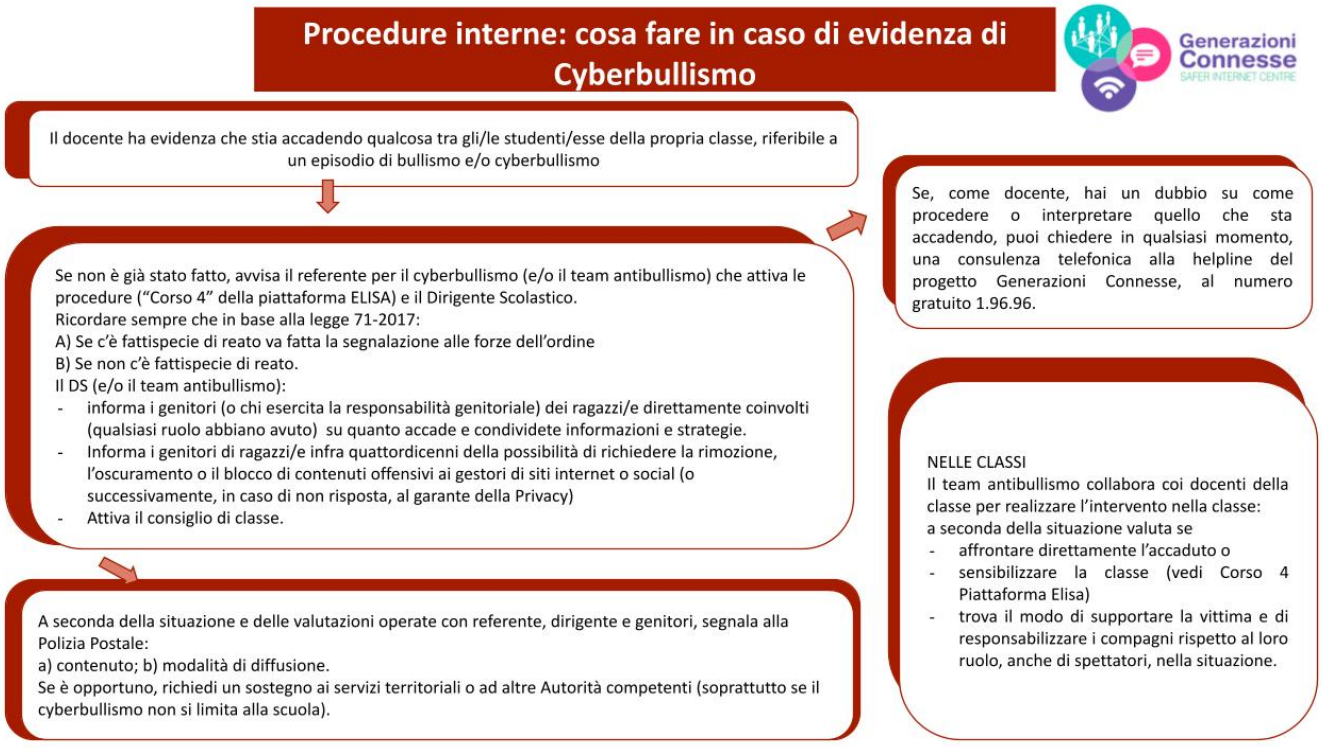
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

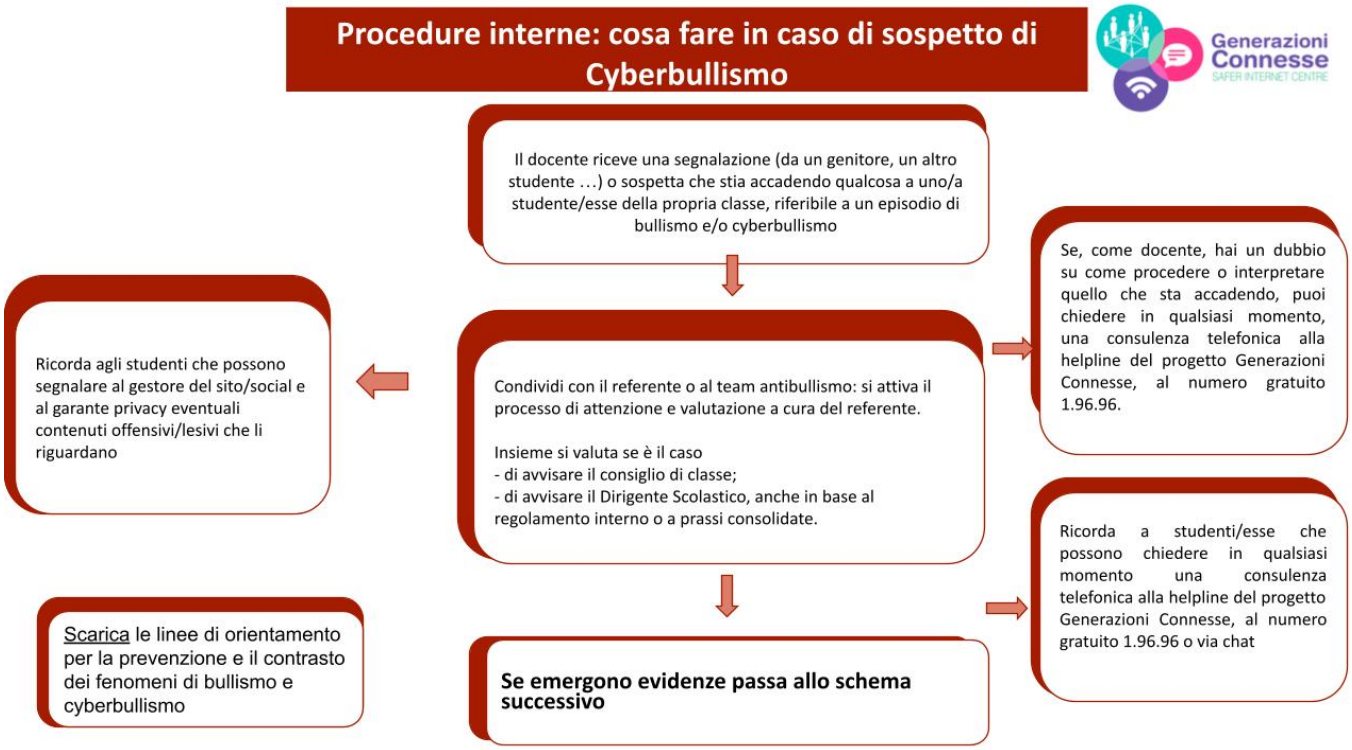
In particolare, sarebbe utile che la scuola attivi un sistema di segnalazione utile anche al monitoraggio dei fenomeni dal quale partire per integrare azioni didattiche preventive e giornate di sensibilizzazione, insieme agli Enti/Servizi presenti sul territorio di riferimento. Importante, altresì, immaginare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

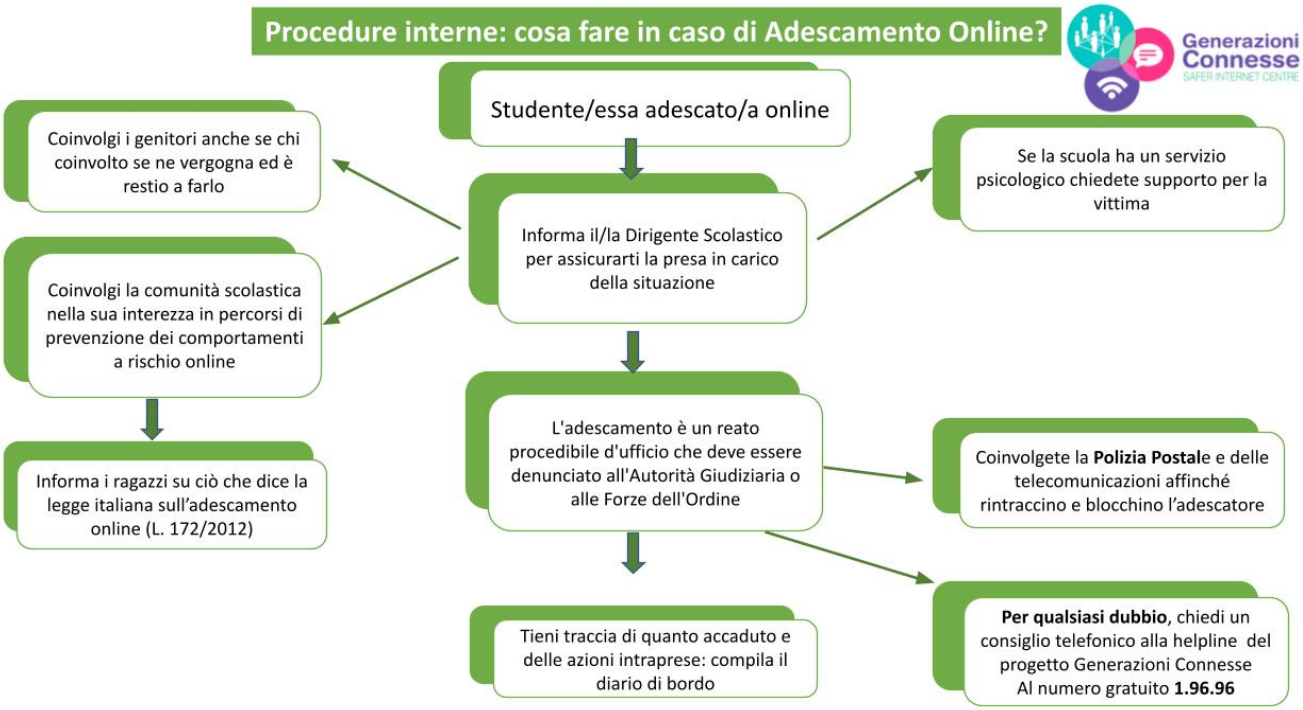
Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle Linee di Orientamento per la prevenzione e il contrasto 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.

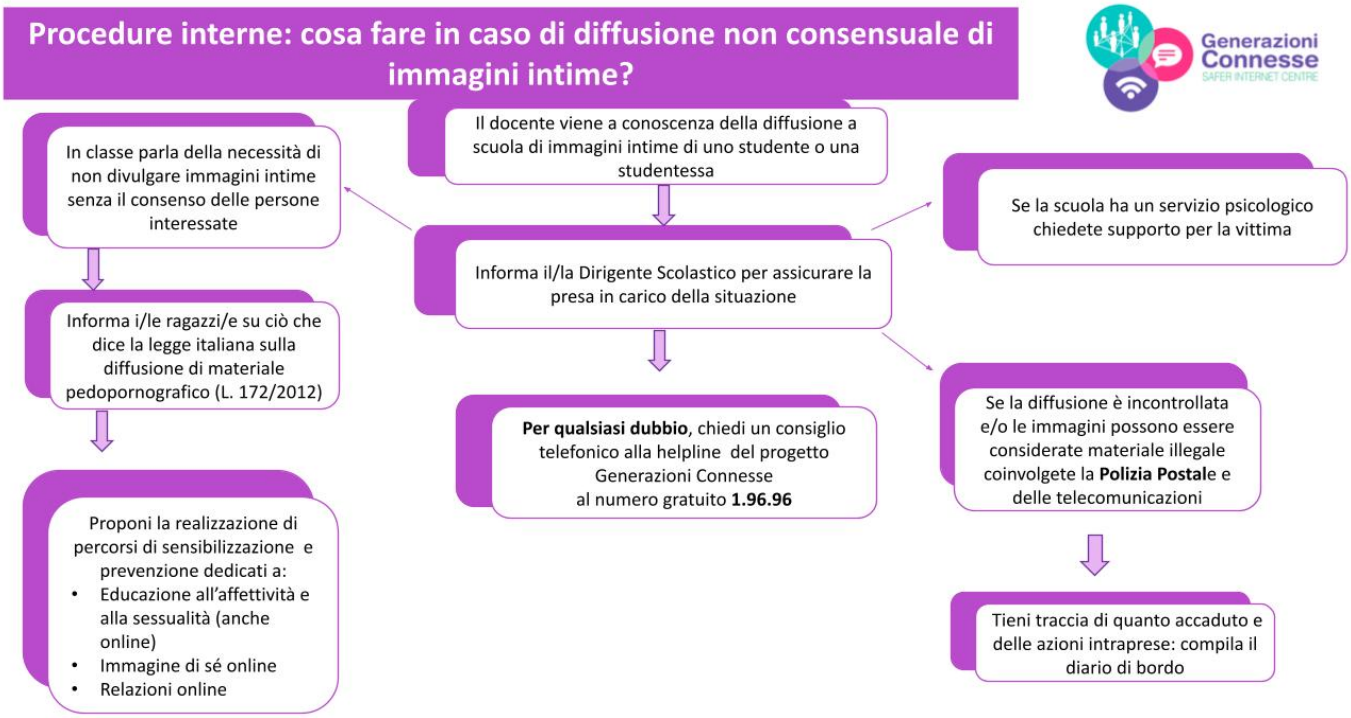
Procedure


Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola
Generazioni Connesse SAFER INTERNET CENTRE
Hai il sospetto che uno/a studente/essa si trovi o conosca una situazione a rischio/di abuso …
Uno/a studente/essa ti confida di trovarsi o di conoscere una situazione a rischio/di abuso …
La scuola accoglie la tua segnalazione e attiva le sue procedure per la gestione dei casi a rischio
Rimani a disposizione per supportare la definizione della situazione
Se non sei un libero professionista, informa il referente presso la tua organizzazione
Informa almeno una di queste figure:
• Il Dirigente Scolastico
• Il referente della scuola per il tuo Progetto
La scuola non è in condizioni di agire sulla situazione/non valuta rilevante la segnalazione
Segui le procedure della tua organizzazione
Se la tua organizzazione non ha una policy e una procedura …
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse Al numero gratuito 1.96.96


Procedure interne: cosa fare in caso di evidenza di Cyberbullismo
Generazioni Connesse SAFER INTERNET CENTRE
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
Generazioni Connesse SAFER INTERNET CENTRE
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
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.
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.
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano
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
Scarica le linee di orientamento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo
Se emergono evidenze passa allo schema successivo


Procedure interne: cosa fare in caso di Adescamento Online?
Generazioni Connesse SAFER INTERNET CENTRE
Studente/essa adescato/a online
Coinvolgi i genitori anche se chi coinvolto se ne vergogna ed è restio a farlo
Se la scuola ha un servizio psicologico chiedete supporto per la vittima
Informa il/la Dirigente Scolastico per assicurarti la presa in carico della situazione
Coinvolgi la comunità scolastica nella sua interezza in percorsi di prevenzione dei comportamenti a rischio online
L'adescamento è un reato procedibile d'ufficio che deve essere denunciato all'Autorità Giudiziaria o alle Forze dell'Ordine
Coinvolgete la Polizia Postale e delle telecomunicazioni affinché rintraccino e blocchino l'adescatore
Informa i ragazzi su ciò che dice la legge italiana sull'adescamento online (L. 172/2012)
Tieni traccia di quanto accaduto e delle azioni intraprese: compila il diario di bordo
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse Al numero gratuito 1.96.96



Protocollo d'azione per la gestione dei casi di bullismo e cyberbullismo

Il nostro Istituto adotta un protocollo d'azione strutturato, articolato in fasi, finalizzato alla tempestiva individuazione, gestione e monitoraggio dei casi di bullismo e cyberbullismo.

Fase 1 – Segnalazione

La fase di segnalazione ha lo scopo di attivare un processo di **attenzione** e di successiva **valutazione** in presenza di un presunto caso di bullismo o cyberbullismo.

La segnalazione può essere effettuata da un **qualsiasi membro della comunità scolastica**: vittima, compagni, genitori, docenti o personale ATA.

Chiunque raccolga una segnalazione è tenuto a **informare tempestivamente** il Referente d'Istituto per il bullismo e il cyberbullismo, o un componente del Team dedicato, utilizzando l'apposita **Scheda di Segnalazione** allegata al presente documento.

Al fine di garantire la tracciabilità del processo, è prevista la compilazione del **Diario di bordo**, nel quale vengono registrati gli eventi e le azioni intraprese.

Fase 2 – Analisi e valutazione dei fatti

Ricevuta la segnalazione, il Team bullismo e cyberbullismo informa il Dirigente Scolastico e avvia tempestivamente la **fase di analisi e valutazione dei fatti**, in collaborazione con il docente coordinatore di classe e, se necessario, con il Consiglio

di classe o il Team docenti (per la scuola primaria).

L'obiettivo è raccogliere **informazioni dettagliate** sull'accaduto al fine di:

- definire la tipologia dell'evento;
- valutarne la gravità;
- individuare le modalità di intervento più adeguate.

A tal fine, il Team procede con **colloqui e interviste** ai soggetti coinvolti (segnalante, vittima, eventuali testimoni, docenti), raccoglie le diverse versioni dei fatti e acquisisce eventuali prove o documentazione utile.

Al **termine** della raccolta delle informazioni:

- se i fatti non risultano riconducibili a episodi di bullismo o cyberbullismo, l'intervento prosegue nell'ambito dell'ordinaria azione educativa;
- se i fatti risultano confermati, il Team formalizza l'apertura del caso e definisce, in accordo con il Dirigente Scolastico, le azioni da intraprendere.

Fase 3 – Scelta dell'intervento e gestione del caso

Sulla base della valutazione effettuata, il Team, in collaborazione con il Dirigente Scolastico e il Consiglio di classe/Team docenti, individua gli **interventi più adeguati**, calibrati sulla specificità del caso.

In linea generale, le **azioni** previste comprendono:

- tutela e supporto della vittima, al fine di garantirne la protezione e prevenire sentimenti di colpa o isolamento;
- convocazione della famiglia della vittima per la condivisione dei fatti e la definizione di strategie di supporto;
- convocazione della famiglia dell'autore degli atti, con illustrazione dei fatti, eventuale comunicazione delle sanzioni disciplinari e definizione di interventi educativi e di supporto;
- eventuale attivazione di percorsi di supporto personalizzato (sportello di ascolto, interventi psico-educativi);
- convocazione straordinaria del Consiglio di classe o Team docenti per la definizione degli interventi educativi e relazionali (lavoro sul gruppo classe, mediazione, gestione delle relazioni);
- individuazione e applicazione di eventuali provvedimenti disciplinari, privilegiando, ove possibile, misure di carattere educativo e riparativo;
- comunicazione formale alle famiglie delle decisioni assunte;
- eventuale segnalazione alle autorità competenti nei casi in cui si configurino ipotesi di reato.

Fase 4 – Monitoraggio

Al termine dell'intervento, il Team bullismo e cyberbullismo, in collaborazione con i docenti e gli altri soggetti coinvolti, attiva un **processo di monitoraggio continuo**, finalizzato a:

- verificare l'efficacia delle azioni intraprese;
- osservare eventuali cambiamenti nei comportamenti dei soggetti coinvolti;
- accertare la cessazione delle situazioni di disagio per la vittima;
- favorire la presa di consapevolezza da parte dell'autore degli atti.

Le modalità di gestione e monitoraggio sono **differenziate in base alla gravità del caso**: nelle situazioni meno complesse può essere sufficiente un intervento educativo a livello di gruppo classe; nei casi più rilevanti si attivano percorsi strutturati e prolungati nel tempo.