Documento di ePolicy
I.I.S.S. Ezio Vanoni - Menaggio

VIA MALAGRIDA P. G. 3 - 22017 - MENAGGIO
Como (CO) - Lombardia
Data di approvazione: 27/05/2026 - 16:47

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.

Attraverso l'ePolicy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, per sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

L' ePolicy fornisce, quindi, linee guida per garantire il benessere in rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative ed educative su e con le tecnologie digitali, oltre che di sensibilizzazione ad un uso consapevole delle stesse.

Il nostro Istituto realizza interventi volti a migliorare l'efficienza e la sicurezza della strumentazione digitale e attiva un progetto di informazione e sensibilizzazione dei genitori e degli studenti sulle problematiche relative ad un uso poco consapevole o improprio delle TD e degli ambienti social, trattando anche il relativo fenomeno del cyberbullismo.

L'ePolicy nasce dunque anche con l'obiettivo di sistematizzare tale sensibilità educativa rendendo strutturali linee guida, regole, interventi formativi, informativi e di sensibilizzazione che riguardino tutti gli attori della scuola (studenti e studentesse, docenti, personale ATA, genitori), intesi come comunità.

La pervasività della tecnologia nella vita dentro e fuori scuola richiede infatti che tale comunità sia informata e conscia delle opportunità e dei rischi che dall'uso della tecnologia derivano.

In particolare il nostro Istituto, in relazione alle tematiche legate alle competenze digitali, all'uso delle stesse in ambiente scolastico, alla sicurezza in rete, si propone di:

- individuare linee guida e procedure per l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC);
- promuovere l'uso delle tecnologie digitali nella didattica;
- sensibilizzare gli attori della scuola ai rischi legati all'uso non consapevole e/o distorto delle tecnologie digitali, con particolare attenzione alla prevenzione del cyberbullismo e alla tutela delle vittime dello stesso;
- individuare linee guida e procedure per gestire casi di cyberbullismo e di *cybercrimes* in generale;
- consolidare il patto educativo di corresponsabilità tra scuola e famiglie.

Tali obiettivi sono in linea con le indicazioni offerte dalle *Linee di Orientamento per Azioni di prevenzione e Contrasto al Bullismo e al Cyberbullismo*, elaborate dal MIM in collaborazione con il *Safer Internet Center* per l'Italia.

Il presente documento sarà soggetto a revisioni ed aggiornamenti periodici e sottoposto all'attenzione dei competenti Organi Collegiali.

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

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

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

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

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

IL DIRIGENTE SCOLASTICO

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

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

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

L'animatore digitale e il Team per l'Innovazione digitale sono co-responsabili, con il referente ePolicy, dell'attuazione dei

piani di azione in particolare in riferimento alla formazione dei docenti. Sono inoltre responsabili del controllo all'accesso da parte degli studenti delle Tic

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

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

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

In coerenza con le Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo del Ministero dell'Istruzione (D.M. n. 18 del 13/1/2021, agg. 2021 – nota prot. 482 del 18-02-2021), il Team ha le funzioni di coadiuvare il Dirigente Scolastico, coordinatore del Team nella scuola, nella definizione degli interventi di prevenzione e nella gestione dei casi di bullismo e cyberbullismo che si possono presentare. Promuove inoltre la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale e comunica ad alunni, famiglie e tutto il personale scolastico dell'esistenza del team, a cui poter fare riferimento per segnalazioni o richieste di informazioni sul tema.

Il Team ha il compito di:

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

I/LE DOCENTI

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

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

RESPONSABILE DELLA PROTEZIONE DEI DATI

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

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

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

GLI STUDENTI E LE STUDENTESSE

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

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

I GENITORI/ADULTI DI RIFERIMENTO

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

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

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

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

L'efficacia del documento di ePolicy diventa significativa soltanto se prevede il coinvolgimento di tutti gli attori della scuola: studenti e studentesse, docenti, genitori, e personale ATA.

Il Dirigente Scolastico è garante della sicurezza, anche on-line, di tutti i membri della comunità scolastica e promuove la cultura della sicurezza e della prevenzione.

Nella promozione dell'uso consapevole della rete il **Dirigente Scolastico** deve:

- garantire una formazione adeguata del personale docente relativo all'uso delle TIC nella didattica;
- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di Internet siano integrate nel *curriculum* di studio e nelle attività didattiche ed educative delle classi; garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza online;
- seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola;
- garantire la corretta applicazione delle linee guida in materia di bullismo e cyberbullismo, nel rispetto dei diritti, della dignità e della privacy di ciascun componente dell'istituzione scolastica;
- individuare un referente del bullismo e cyberbullismo;
- coinvolgere, nella prevenzione e contrasto al fenomeno del bullismo, tutte le componenti della comunità scolastica;
- promuovere azioni di sensibilizzazione dei fenomeni del bullismo e del cyberbullismo nel territorio in rete con enti, associazioni, istituzioni locali ed altre scuole, coinvolgendo alunni, docenti, genitori ed esperti;
- favorire la discussione all'interno della scuola, attraverso i vari organi collegiali, creando i presupposti di regole condivise di comportamento per il contrasto e prevenzione dei fenomeni del bullismo e cyberbullismo.

L'animatore digitale è una figura di supporto a tutta la comunità scolastica relativamente alle tematiche dei rischi online, alla protezione dei dati personali.

Presenta al Dirigente Scolastico, all'inizio di ogni anno scolastico, un percorso di formazione per lo sviluppo delle competenze digitali, previste anche nell'ambito dell'educazione civica.

L'animatore digitale ha inoltre il compito di:

- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi online e alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di Internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite password e sensibilizzarli sulla necessità di cambiarle regolarmente;
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti alla "scuola digitale";
- è inoltre responsabile della compilazione del registro che riporta gli "incidenti online" avvenuti nella scuola.

Il Team per l'innovazione digitale non è al momento presente nell'Istituto.

Il **referente per il bullismo e il cyberbullismo** coordina e promuove iniziative specifiche per la prevenzione e il contrasto e vigila sulla corretta applicazione delle linee guida in materia di bullismo e cyberbullismo e in particolare:

- organizza attività di informazione-formazione rivolte ad alunni, studenti e personale scolastico, in materia di bullismo, cyberbullismo e cittadinanza digitale;
- organizza percorsi rieducativi per gli alunni che non hanno rispettato le norme previste dal presente documento;
- interviene in sostegno delle vittime di bullismo o cyberbullismo;
- collabora con i docenti e i Consigli di classe per la gestione dei casi e per le attività di prevenzione del bullismo e del cyberbullismo.

Il Team Antibullismo e il Team per l'Emergenza hanno le funzioni di coadiuvare il Dirigente Scolastico, che li coordina, nella definizione degli interventi di prevenzione e nella gestione dei casi di bullismo e cyberbullismo che si possono presentare. Nel nostro Istituto sono stati istituiti nell'a.s. 2025/2026.

Il Team Antibullismo:

- è composto dal Dirigente Scolastico, dal referente per il bullismo e il cyberbullismo, dall'animatore digitale, dai docenti del Team ePolicy;
- coadiuva il Dirigente Scolastico, coordinatore del Team, nella definizione degli interventi volti alla consapevolezza e alla prevenzione dei fenomeni di bullismo e cyberbullismo, a beneficio di genitori, studenti, personale tutto;
- promuove la redazione e l'applicazione della ePolicy;
- attiva il Team per l'Emergenza in caso di necessità;
- monitora e valuta le segnalazioni e le attività svolte.

Il Team per l'Emergenza:

- è composto dal Dirigente Scolastico, dal referente per il bullismo e il cyberbullismo. Può avvalersi del supporto del Coordinatore di classe, dello psicologo d'Istituto, dell'animatore digitale, di membri del Team ePolicy;
- interviene nelle situazioni evidenti di bullismo e cyberbullismo;
- può collaborare con soggetti esterni (per esempio le forze dell'ordine, i servizi sanitari) per un supporto integrato.

I **docenti** devono:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di Internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete, ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente; controllare l'uso delle tecnologie digitali, dispositivi mobili, fotocamere, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito); nelle lezioni e attività in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all'animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC.

Il **personale ATA** è responsabile del proprio utilizzo corretto e consapevole della tecnologia in ambito scolastico, con particolare riferimento alla protezione dei dati personali.

Gli **studenti e le studentesse** devono:

- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali, ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
- comprendere l'importanza di adottare buone pratiche di sicurezza online quando si utilizzano le tecnologie digitali per non correre rischi;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di Internet ai docenti e ai

genitori;
- segnalare tempestivamente casi di uso scorretto delle tecnologie digitali da parte di compagni singoli o in gruppo;
- segnalare alla scuola casi di bullismo o cyberbullismo, di cui sono vittime o spettatori;
- collaborare con la scuola nella diffusione dell'uso corretto delle tecnologie digitali.

Le **famiglie** si impegnano a:

- collaborare con la scuola nella promozione della cultura di un uso consapevole e corretto delle nuove tecnologie e della rete, del rispetto della dignità e della privacy di ciascuno;
- prevenire e intercettare situazioni legate ad un uso scorretto delle nuove tecnologie e alla loro segnalazione alla scuola;
- vigilare, nei limiti delle proprie competenze e possibilità, sui device dei propri figli al fine di prevenire ed intercettare situazioni di rischio;
- segnalare alla scuola casi di uso scorretto delle nuove tecnologie da parte di alunni singoli o in gruppo;
- segnalare alla scuola casi di bullismo o cyberbullismo.

Il nostro Istituto, al fine di rendere l'ePolicy uno strumento efficace per la tutela degli studenti e delle studentesse, ha individuato un insieme di regole o norme di comportamento da condividere con le organizzazioni/associazioni extrascolastiche e con gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti, laboratori e che erogano attività educative in ambito scolastico, sul breve e/o lungo periodo.

Tale codice di comportamento è specificato nell' **Informativa sintetica sull'ePolicy** destinata a tutti i soggetti esterni che si trovano ad operare all'interno dell'Istituto e che permette non solo di tutelare studenti e studentesse e la scuola stessa da comportamenti potenzialmente rischiosi messi in atto da soggetti esterni alla scuola, ma anche di porre in essere nuove modalità per rilevare, limitare e contrastare possibili pericoli legati a condotte educative non professionali.

Tale documento, inoltre, specifica anche il sistema di azioni e le procedure di segnalazione da seguire, qualora si verificassero problematiche derivanti da un utilizzo non corretto delle tecnologie digitali o quando, nei casi più estremi, si sospettassero forme di maltrattamento/abuso sia nel reale che nel virtuale, sia di tipo fisico che psicologico a danno di minori, affinché tutti gli attori educativi siano sensibilizzati e resi consapevoli dei rischi online.

Tutti i soggetti esterni dovranno prendere visione di tale informativa, condividerla e sottoscriverla preliminarmente all'avvio delle attività con gli studenti e le studentesse, in classe o fuori, in modo da garantire la massima tutela delle alunne e degli alunni.

Il documento, vincolante fra le parti, potrà essere monitorato, aggiornato ed integrato in caso di necessità.

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.

Il Regolamento di Istituto è in corso di revisione e aggiornamento; per quanto concerne l'ePolicy verrà integrato con aspetti riguardanti i diversi ruoli degli attori della scuola e le procedure da seguire in caso di segnalazione e/o infrazione.

Il Codice disciplinare degli studenti (allegato al Regolamento d'Istituto) nell'a.s. 2023-2024 è stato aggiornato in relazione alle diverse tipologie di infrazioni all'ePolicy ed è attualmente in vigore.

Il PTOF è stato rinnovato per il triennio 2025-2028. Nel documento è presente una sezione dedicata alla ePolicy con particolare riferimento all'attività del curricolo digitale verticale.

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.

L'Istituto intende dotarsi di una versione friendly del documento di ePolicy da condividere con famiglie e studenti. Tale documento tratterà i seguenti punti:

- scopo dell'ePolicy;
- ruoli e responsabilità;
- indicazioni sul curricolo digitale verticale e sull'uso del kit didattico;
- illustrazione delle regole per un uso consapevole della tecnologia a scuola;
- segnalazione e gestione dei casi

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

L'Istituto intende perseguire i seguenti piani d'azione, passibili di integrazione qualora necessario

1° anno:

- presentazione dell'ePolicy agli studenti delle classi prime;
- invio della versione friendly dell'ePolicy a tutti gli studenti dell'Istituto;
- presentazione della nuova redazione dell'ePolicy ai docenti dell'Istituto con particolare riferimento al kit didattico e alle novità rispetto al documento precedente;
- presentazione e diffusione della nuova redazione dell'ePolicy ai genitori in occasione degli incontri di orientamento (open day) e dell'elezione dei rappresentanti dei genitori;
- rilevazione del fabbisogno formativo dei docenti sui temi dell'educazione civica digitale in collaborazione con il referente per l'Ed. Civica, il referente per il bullismo e cyberbullismo, l'animatore digitale;
- rilevazione di interessi, bisogni e comportamenti delle famiglie sull'uso positivo del digitale;
- uso del kit didattico in aggiunta al materiale autoprodotto dalla scuola (attività didattiche utili a sviluppare competenze del curricolo digitale) come materiale utile alla realizzazione del curricolo digitale verticale;
- eventuale ulteriore integrazione dell'ePolicy nei documenti dell'Istituto;
- eventuale aggiornamento della Politica d'Uso accettabile e del regolamento BYOD;
- definizione delle procedure di segnalazione per studenti e studentesse e diffusione delle stesse;
- realizzazione di una reportistica delle segnalazioni ricevute e degli esiti delle stesse da presentare nel Collegio Docenti finale.

2° anno:

- presentazione dell'ePolicy agli studenti delle classi prime;
- uso del kit didattico in aggiunta al materiale autoprodotto dalla scuola (attività didattiche utili a sviluppare competenze del curricolo digitale) come materiale utile alla realizzazione del curricolo digitale verticale;
- rilevazione di interessi, bisogni, comportamenti, abitudini di studenti e studentesse sui temi dell'educazione civica digitale in collaborazione con il referente di ed. civica, il referente per il bullismo e il cyberbullismo, l'animatore digitale;
- realizzazione di una formazione rivolta agli studenti e alle studentesse attraverso il percorso previsto dal curricolo digitale verticale;
- realizzazione di una formazione rivolta alle famiglie anche attraverso il percorso previsto sulla piattaforma di Generazioni Connesse e sulla base delle rilevazioni dell'anno precedente.

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

Le risorse di Generazioni Connesse verranno utilizzate e promosse nella loro conoscenza e diffusione presso tutti gli attori della scuola.

Dal momento che l'Istituto, dall'a.s. 2022/2023, ha attuato le attività del curricolo digitale verticale, sono state nel tempo creati e raccolti sul Drive dìlstituto, una serie di stimoli didattici suddivisi per disciplina e specifiche competenze utili alla formazione degli studenti nell'ambito del digitale. Tali risorse verranno dunque integrate con quelle proposte da Generazioni Connesse, dal Dig.Comp 2.2 e sue successive evoluzioni, da Parole O_stili, da Co.Re.Com.

Cap 2 - Sensibilizzazione e prevenzione

2.1 - Sensibilizzazione e prevenzione

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

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

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

I **rischi online** rappresentano tutte le situazioni problematiche derivanti da un uso non consapevole e non responsabile delle tecnologie digitali da parte degli studenti, in particolare di quelli minorenni: *adescamento online, cyberbullismo, sexting, violazione della privacy, pornografia, pedopornografia, gioco d'azzardo o gambling, internet addiction, videogiochi online, esposizione a contenuti dannosi o inadeguati* (ad es. contenuti razzisti, che inneggiano al suicidio, che promuovono comportamenti alimentari scorretti, ecc.).

Vanno dunque promosse nei più giovani le necessarie conoscenze, competenze e capacità, al fine di una protezione adeguata, ma anche di un utilizzo consapevole che sappia sfruttare le potenzialità delle tecnologie digitali e gestirne le implicazioni.

La **sensibilizzazione** costituisce il primo passo verso un cambiamento positivo; si ritiene che ci si debba impegnare soprattutto su tre fronti perché possa avere una sua efficacia:

- la consapevolezza dello *status quo*;
- la motivazione al cambiamento;
- la scelta delle azioni da porre in essere al fine di produrre il cambiamento.

Le **azioni di sensibilizzazione** che il nostro Istituto intende intraprendere prevedono di:

- attivare percorsi/incontri educativi sui rischi della rete sia per gli studenti che per i genitori, avvalendosi del personale della scuola con competenze specifiche, ma anche di personale esterno alla scuola (Polizia postale - Centro Operativo per la Sicurezza Cibernetica, forze dell'ordine, servizi sociali, psicologi, educatori ...) per accrescere negli studenti e nelle studentesse la consapevolezza di particolari problemi relativi ad un uso improprio dell'online, ma anche per renderli consci dell'importanza di denunciare comportamenti sbagliati cui assistono, partecipano, di cui vengono a conoscenza.
- favorire la diffusione di informazioni e servizi disponibili per una utilità collettiva (ad esempio, promuovere la conoscenza dell'ePolicy nella comunità scolastica, promuovere la conoscenza di siti utili come Generazioni Connesse, le attività dell'Help line di Telefono Azzurro, del Co.Re.Com.).

Le **azioni di prevenzione** che il nostro Istituto intende intraprendere per prevenire la delicata problematica dei rischi online

sono:

- attivare percorsi di educazione civica digitale al fine di formare e consolidare le competenze educative di base necessarie a poter gestire le situazioni online e per un uso consapevole della rete;
- progettare attività, azioni ed interventi con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza degli studenti.

Qui di seguito alcuni suggerimenti utili in un'ottica di prevenzione dei rischi online:

- osservare in modo critico e attento i siti visitati;
- non dichiarare la propria identità;
- non condividere notizie riservate;
- non accettare l'installazione di script;
- non cliccare sui link o sui banner pubblicitari;
- quando si naviga, tenere aggiornato il browser e dopo avere visitato qualche sito sospetto eliminare i cookie (fare pulizia del browser).

Di seguito si indicano i principali rischi online e le azioni promosse dalla scuola.

CYBERBULLISMO

È molto importante sottolineare come il cyberbullismo non sia una problematica che riguarda unicamente vittima e cyberbullo, ma è un fenomeno sociale e di gruppo. Infatti, centrale è il ruolo delle agenzie educative e di socializzazione (formali e informali) più importanti per gli adolescenti: la famiglia, la scuola, i media, le tecnologie digitali e il gruppo dei pari.

Come riconoscere casi di cyberbullismo?

Di seguito, alcuni segnali generali che può manifestare la potenziale vittima di cyberbullismo:

- appare nervosa quando riceve un messaggio o una notifica;
- sembra a disagio nell'andare a scuola o finge di essere malata (ha spesso malesseri come mal di stomaco o mal di testa);
- cambia comportamento ed atteggiamento in modo repentino;
- mostra ritrosia nel dare informazioni su ciò che fa online;
- soprattutto dopo essere stata online, mostra rabbia o si sente depressa;
- inizia ad utilizzare sempre meno pc e telefono (arrivando ad evitarli);
- perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;
- il suo rendimento scolastico peggiora

Un'altra indicazione operativa concerne una valutazione circa l'eventuale stato di disagio vissuto dalla persona minorenne coinvolta e per cui potrebbe essere necessario rivolgersi a un servizio deputato ad offrire supporto psicologico e/o di mediazione.

Il nostro Istituto ritiene che solo interventi sinergici e condivisi sia sul piano verticale che orizzontale possano prevenire o affrontare gli atti del bullismo online, nella consapevolezza che le azioni efficaci debbano ricorrere agli strumenti educativi, rieducativi e di mediazione del conflitto, supportati anche da azioni di comunicazione e informazione di natura giuridica sulle responsabilità da conoscere intorno alla possibilità di commettere reati o danni civili.

Nell'Istituto opera un referente per il contrasto al bullismo e cyberbullismo che monitora la situazione e a cui i docenti fanno riferimento per realizzare, all'interno dell'azione curricolare e nel caso si verifichino episodi riconducibili a casi di cyberbullismo, percorsi di riflessione e dialogo con l'intero gruppo classe.

In coerenza con le Linee di Orientamento per la prevenzione e il contrasto del bullismo e cyberbullismo (Legge n. 70/2024, D.M. n. 18 del 13.1.2021, agg. 2021 – nota prot. 482 del 18.02.2021), all'interno dell'Istituto sono stati costituiti il Team Antibullismo e il Team per l'Emergenza che hanno le funzioni di coadiuvare il Dirigente Scolastico - che li coordina - nella definizione degli interventi di prevenzione e nella gestione dei casi di bullismo e cyberbullismo che si possono presentare. Dei Team nello specifico si è parlato al cap. 1.2, cui si rimanda.

HATE SPEECH

Online questo fenomeno si è propagato in maniera "liquida" e colpisce i più vulnerabili, in particolare i più giovani, spesso fragili e con personalità in formazione; alle volte risulta incitato da personaggi noti e influenti, dai social media, e per questo può fare facilmente presa.

Come riconoscerlo?

Il discorso dell'odio si manifesta con un ampio spettro di azioni: sebbene tutte le espressioni che istigano all'odio meritino di essere stigmatizzate, ne esistono alcune che possono essere più gravi di altre.

Come prevenirlo?

Il nostro Istituto, al fine di prevenire e affrontare tale fenomeno, fonda la sua azione su un curricolo verticale che si declina in percorsi/progetti didattico-educativi intorno ai temi dei diritti e doveri, del rispetto, dell'inclusione e del dialogo attivo e partecipe, della condivisione di buone regole di comportamento.

Contrastare questo fenomeno così complesso è difficile, ma l'Istituto valuta di intraprendere comunque alcune azioni specifiche:

- analizzare i siti che manifestano questo tipo di odio e sensibilizzare gli alunni mediante la realizzazione di attività (per esempio slogan pubblicitari);
- sensibilizzare gli alunni mediante campagne di educazione e formazione;
- valorizzare la dimensione relazionale dei più giovani, attraverso un loro coinvolgimento attivo anche in problematiche che riguardano la scuola, sensibilizzandoli alla capacità di analisi e discernimento;
- fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech;
- promuovere negli alunni la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- sostenere le vittime di abusi e discriminazione di questo tipo;
- educare ad un uso corretto delle piattaforme sociali e delle chat di messaggistica;
- esortare i soggetti di tali vessazioni a parlare con un docente, un adulto di fiducia o con il referente della scuola;

DIPENDENZA DA INTERNET E GIOCO ONLINE

Il nostro Istituto ritiene che sia utile riflettere con studenti e studentesse rispetto all'uso della tecnologia in termini di qualità e tempo, affinché siano consapevoli delle proprie abitudini online e dei rischi che comporta l'iperconnessione.

Altro aspetto fondamentale è cercare di cogliere, attraverso la relazione con gli studenti, segnali che possano far sospettare un'iperconnessione o l'attività del gioco d'azzardo online. Particolarmente importante risulta dunque anche il rapporto scuola-famiglia, in un dialogo educativo effettivamente sinergico.

SEXTING

I rischi del sexting, legati al revenge porn, possono contemplare violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie; le ripercussioni negative sulla vittima possono essere in termini di autostima, di credibilità, di stress emotivo, di reputazione sociale online e no.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata

problematica del sexting:

- integrare i corsi con contenuti informativi sui temi legati all'affettività, alla sessualità e alle differenze di genere, secondo le età degli studenti e delle studentesse, anche con il supporto di esperti esterni;
- aiutare gli studenti e le studentesse a sapere cosa fare e a chi rivolgersi in caso di sexting subito o di cui si è venuti a conoscenza;
- attuare campagne informative verso gli alunni e le alunne sui rischi anche penali che questa pratica può comportare;
- proporre ai docenti, e quindi agli studenti, percorsi di riflessione e confronto su questa tematica;
- consigliare ai genitori di parlare con i propri figli sull'uso della tecnologia e sui pericoli che possono crearsi in Internet; fornire loro informazione circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzare sulla necessità di monitorare la presenza sui social dei figli.

ADESCAMENTO ONLINE

L'adescamento online è un reato penalmente perseguibile. A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare questo problema:

- accompagnare studenti e studentesse in un percorso di educazione (anche digitale) all'affettività e alla sessualità, anche gestito da esperti esterni. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri;
- sensibilizzare studenti e studentesse, attraverso momenti formativi dedicati, sull'importanza della privacy, su tutti gli aspetti e le azioni che configurano il reato di adescamento e sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, non corrette con i minori;
- mettere a disposizione degli alunni un canale di comunicazione per eventuali preoccupazioni, segnalazioni o dubbi in merito. È molto importante, inoltre, che studenti e studentesse sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato.

Si fa inoltre presente che, all'interno dell'Istituto, oltre al Dirigente Scolastico e ai docenti, operano un referente per il contrasto al bullismo e cyberbullismo e uno psicologo scolastico (Sportello di Ascolto), con il compito di accogliere/supportare gli studenti e le studentesse.

PEDOPORNOGRAFIA

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

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

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

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

Se si è a conoscenza di tale tipologia di reato è possibile far riferimento ai seguenti servizi:

- Polizia di Stato – COSC;

- Polizia di Stato – Questura o Commissariato di P.S. del territorio di competenza;
- Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza.

Se casi di pedopornografia dovessero essere rilevati a scuola, ne sarà immediatamente informato il Dirigente Scolastico e verrà seguito l'iter di azione previsto.

A seguire vengono descritte le azioni, rivolte a genitori, alunni e docenti, che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica della pedopornografia:

- percorsi di riflessione e confronto proposti ai docenti e agli studenti su questa tematica;
- attività di sensibilizzazione degli alunni, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico;
- inserimento nel curricolo, ove possibile, di temi legati all'affidabilità delle fonti online e alla sessualità;
- informazione ai genitori circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare la presenza dei figli sui social e sulle chat.

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.

Come specifica il DigComp "Quadro di riferimento per le competenze digitali dei cittadini", le macro aree di competenza sono cinque:

1. Alfabetizzazione e dati
2. Comunicazione e collaborazione
3. Creazione di contenuti digitali
4. Sicurezza
5. Risoluzione di problemi

L'Istituto ha elaborato nell'a.s. 2019/2020 - e rivisto nell'a.s. 2025/2026 - il curricolo digitale verticale, parte integrante del PTOF.

La costruzione del curricolo digitale di ciascuno studente non è prerogativa di una singola disciplina: tutti gli insegnanti possono partecipare e concorrere alla sua realizzazione. Di seguito sono indicate le azioni che i docenti di ogni disciplina possono mettere in atto per sviluppare le competenze digitali degli studenti. Esse non vanno intese come un elenco di attività obbligatorie per ognuno: sta al singolo docente e al Consiglio di Classe selezionare quelle che ritengono più opportune in rapporto alle caratteristiche e alle peculiarità dei singoli alunni e del gruppo classe.

CLASSI PRIME (area di competenza: informazione e alfabetizzazione nella ricerca di dati)

COMPETENZA	OBIETTIVI DI APPRENDIMENTO	ESEMPI DIDATTICO - OPERATIVI
Navigare, ricercare e filtrare dati, informazioni e contenuti digitali	Trovare dati, informazioni, contenuti, attraverso una ricerca in ambienti digitali.	Effettuare una ricerca su un tema o all'interno di una specifica disciplina navigando su siti di riconosciuta validità. Utilizzare motori di ricerca, siti, blog ... attraverso parole chiave efficaci. Effettuare una ricerca per immagini. Utilizzare QR Code per accedere a informazioni. Leggere e ricercare informazioni online utilizzando dizionari digitali Utilizzare i filtri presenti nei motori di ricerca per effettuare ricerche più mirate.
Valutare dati, informazioni e contenuti digitali	Analizzare la credibilità e l'affidabilità delle fonti di dati, informazioni e contenuti digitali per riconoscere e sapersi difendere da contenuti dannosi e pericolosi.	Selezionare fonti online e confrontare le informazioni con altre fonti per valutarne l'affidabilità Analizzare notizie e informazioni per individuare fake news; Selezionare e confrontare fonti, documenti e dati per valutare la pertinenza dei dati Ricercare recensioni in rete per valutare la qualità di prodotti e servizi Distinguere un contenuto promozionale da altri contenuti online anche se non indicati come promozionali Saper riconoscere i siti più appropriati per una determinata ricerca. Conoscere i primi elementi dell'Intelligenza Artificiale e saperne valutare limiti e potenzialità. Riflettere su come linguaggi e tecniche utilizzati dai mass media – compresa l'Intelligenza Artificiale - possano influenzare e direzionare decisioni individuali. Analizzare come piattaforme di streaming o social network suggeriscono contenuti. Discutere su come i dati (input) influenzino i risultati (output)
Gestire dati, informazioni e contenuti digitali	Organizzare, archiviare e recuperare dati, informazioni e contenuti negli ambienti digitali.	Archiviare documenti digitali per rendere più facile la consultazione e/o il recupero: Organizzare documenti in cartelle e sottocartelle (offline) Caricare e organizzare documenti nel Cloud (Google Drive)
Bullismo e cyberbullismo	Conoscere le dinamiche, i ruoli e le responsabilità relativi a bullismo e cyberbullismo. Sapere a chi chiedere aiuto e come denunciare.	Analizzare e favorire la discussione di casi di bullismo e cyberbullismo sfruttando in via preferenziale il gioco di ruolo, il compito di realtà con un focus sulle dinamiche, sui ruoli (bullo, vittima, spettatori) e sulle azioni. Presentare la Legge su bullismo e cyberbullismo.

CLASSI SECONDE (area di competenza: comunicazione e collaborazione)

COMPETENZA	OBIETTIVI DI APPRENDIMENTO	ESEMPI DIDATTICO - OPERATIVI
Interagire con gli altri attraverso le tecnologie digitali	Conoscere i mezzi di comunicazione digitale. Interagire attraverso le tecnologie digitali e scegliere i mezzi di comunicazione digitale più adatti ad un determinato contesto.	Scaricare materiali didattici dal Registro elettronico, da Google Classroom, o altre piattaforme, rispondere ai post dei docenti su piattaforme didattiche e caricare a propria volta materiale (Google, Mail, Classroom o altro). Scrivere una mail corretta, anche da un punto di vista formale. Scrivere un post corretto ed efficace da un punto di vista comunicativo. Rielaborare e revisionare un testo già prodotto dallo studente allo scopo di migliorarlo guidando l'IA mediante prompt opportuni Comunicare con l'insegnante e/o i compagni secondo necessità e tramite mail istituzionale. Saper comunicare con i compagni di classe e organizzare il lavoro di gruppo usando strumenti di comunicazione digitali.
Condividere attraverso le tecnologie digitali	Scegliere tecnologie digitali appropriate per condividere dati, informazioni e contenuti.	Condividere dati, informazioni e contenuti attraverso gli strumenti digitali appropriati al contesto di riferimento (usare i canali di comunicazione formale/informale, ad es. le chat di gruppo tra coetanei e le comunicazioni via mail con i docenti). Saper selezionare e limitare le persone con cui condividere contenuti. Conoscere cosa siano i dati sensibili e la necessità di non condividerli. Leggere e commentare contratti di utilizzo dei principali social network Utilizzare strumenti cloud per la condivisione dei contenuti.
Esercitare la cittadinanza attraverso le tecnologie digitali	Scegliere servizi digitali per partecipare alla vita sociale	Saper discutere sulle tecnologie digitali appropriate per potenziare le proprie capacità personali e partecipare alla vita sociale. Creare e partecipare a sondaggi online. Creare e sottoscrivere petizioni online.
Collaborare attraverso le tecnologie digitali	Scegliere strumenti e tecnologie digitali per esperienze collaborative	Collaborare online con gli altri in diverse situazioni, condividendo dati, informazioni, creando gruppi di lavoro per es. per fasi di brainstorming, ripasso collettivo, lezioni peer to peer ... Utilizzare strumenti e strategie per collaborare con i compagni nella creazione di contenuti digitali, (ambiente Google Workspace d'Istituto).
Conoscere la "netiquette", ovvero le norme di comportamento online	Applicare le corrette norme comportamentali nella comunicazione digitale. Saper gestire i propri sentimenti e reazioni quando si parla con altre persone online. Saper riconoscere i messaggi e le attività online ostili e offensivi.	Essere consapevoli delle regole condivise di comportamento in rete. Definire e applicare regole di comportamento appropriato e responsabile, anche mentre si lavora online in gruppo. Definire e applicare regole di comportamento appropriato e responsabile per i gruppi informali (es. Whatsapp). Saper bloccare la ricezione di messaggi o mail indesiderati.

COMPETENZA	OBIETTIVI DI APPRENDIMENTO	ESEMPI DIDATTICO - OPERATIVI
Saper gestire la propria identità digitale	Avere contezza delle caratteristiche della propria presenza online Comprendere che l'io fisico e l'io digitale non sono differenti Curare la propria identità digitale.	Saper consultare il Registro Elettronico d'Istituto. Gestire in modo appropriato l'account e la casella mail fornita dall'Istituto. Conoscere gli elementi che costituiscono la propria identità digitale Cercare la propria identità digitale attraverso strumenti di ricerca online e discutere come essa possa impattare sul futuro, inclusa la ricerca di opportunità lavorative Esplorare la connessione tra identità digitale e mondo del lavoro, tra rischi e opportunità.

CLASSI TERZE (area di competenza: creazione di contenuti digitali)

COMPETENZA	OBIETTIVI DI APPRENDIMENTO	ESEMPI DIDATTICO - OPERATIVI
Sviluppare contenuti digitali	Creare e sviluppare contenuti in diversi formati per esprimersi attraverso strumenti digitali.	Creare, modificare e salvare i contenuti didattici in diversi formati e strumenti diversi per esprimersi attraverso gli strumenti digitali, come ad esempio linee del tempo, fogli di calcolo, blog, siti tematici, video, post, pagine web, brochure digitali, mappe concettuali (es. Cmap, Mind Map ...). Creare prodotti digitali per la presentazione di contenuti specifici. Creare disegni tecnici di particolari e salvarli in diversi formati. Compilare una bibliografia/sitografia organica e ordinata. Utilizzare la stampante 3D
Integrare e rielaborare contenuti digitali	Modificare e integrare informazioni e contenuti creandone di nuovi.	Lavorare con diversi contenuti digitali modificandone dati e impostazioni, integrandone la progettazione, per crearne nuovi e originali (aggiungendo testo, immagini, effetti visivi ...) Selezionare immagini e video non protetti da copyright per usarli all'interno di contenuti digitali. Rielaborare codice di programmazione esistente.
Copyright e licenze	Conoscere la normativa su copyright e licenze	Conoscere software open source e closed source. Conoscere i principi di tutela dell'opera d'autore e diritti d'autore (testi, audio, video, software) e conoscere le conseguenze delle violazioni. Conoscere diritti e limiti di utilizzo: copyright, licenze e brevetti. Verificare e citare le fonti di quanto viene condiviso. Analizzare le questioni di copyright relative ai contenuti generati da IA e all'uso di dati per l'addestramento. Progettare un semplice chatbot per la didattica (es. su un tema storico o letterario) Discutere sull'uso etico dell'IA e sui diritti d'autore.
Pensiero computazionale	Saper elencare semplici istruzioni in un sistema informatico per risolvere semplici problemi o fare svolgere semplici compiti. Essere in grado di procedere passo passo nello svolgimento di un compito specifico in ambiente digitale.	Far eseguire attività in laboratorio o su pc portatili sul sito MIUR programmailfuturo.it dove selezionare "l'ora del codice". Far eseguire, successivamente, attività usando l'applicazione App inventor. Serve per creare applicazioni.
Sexting	Conoscere il fenomeno e sapersene difendere	Esaminare casi e stimolare il confronto.

CLASSI QUARTE (area di competenza: sicurezza)

COMPETENZA	OBIETTIVI DI APPRENDIMENTO	ESEMPI DIDATTICO - OPERATIVI
Proteggere i dispositivi	Individuare modi per proteggere dispositivi e contenuti digitali. Avere consapevolezza di rischi e minacce negli ambienti digitali.	Saper impostare una password efficace per proteggere i propri dispositivi. Conoscere cosa siano i dati personali. Conoscere gli strumenti per la gestione e il salvataggio dei dati personali (dati di login). Saper installare e usare software di protezione (antivirus, antimalware, firewall). Conoscere la firma digitale per garantirne l'autenticità. Conoscere rischi e minacce digitali avvenuti e riflettere su come tutelarsi.
Proteggere i dati personali e la privacy	Scegliere modalità per proteggere i propri dati personali e la privacy negli ambienti digitali.	Navigare in anonimato. Conoscere cosa siano i dati personali. Comprendere e saper interpretare le informative sulla privacy. Compilare un curriculum con attenzione a quali dati personali sia possibile inserire. Navigare e usare il sito dell'Autorità garante per la protezione dei dati personali. Usare software per salvare in modo sicuro le password. Saper esercitare un controllo sui propri dati e sulle proprie immagini e web reputation.
Tutelare la salute e il benessere	Saper distinguere modalità per evitare i principali rischi per la salute e le minacce al benessere psico–fisico nell'utilizzo delle tecnologie digitali. Condividere modalità per proteggere se stessi e gli altri da possibili pericoli negli ambienti digitali.	Conoscere i rischi che un uso eccessivo o improprio della tecnologia comporta per la propria salute psicofisica. Aderire a iniziative di sensibilizzazione attraverso progetti e partecipazione ad eventi sulle tecnodipendenze. Saper distinguere modalità per evitare i principali rischi per la salute e le minacce al benessere psico – fisico nell'utilizzo delle tecnologie digitali. Analizzare rischi di manipolazione e disinformazione (fake news) generati da IA

CLASSI QUINTE (area di competenza: soluzione di problemi)

COMPETENZA	OBIETTIVI DI APPRENDIMENTO	ESEMPI DIDATTICO - OPERATIVI
Risolvere problemi tecnici	Individuare e risolvere problemi tecnici relativi ai dispositivi e agli ambienti digitali	Saper usare manuali tecnici online e offline per trovare soluzioni a problemi tecnici. Saper adottare un approccio per fasi per identificare la fonte di un problema tecnico. Saper come trovare soluzioni su Internet quando ci si trova di fronte ad un problema tecnico
Identificare i bisogni e le risposte tecnologiche	Individuare le esigenze e selezionare gli strumenti digitali adeguati	Saper individuare esigenze, riconoscere semplici strumenti digitali e possibili risposte tecnologiche per soddisfarle. Saper scegliere modalità per adattare e personalizzare gli ambienti digitali alle esigenze personali.
Utilizzare in modo creativo le tecnologie digitali	Usare strumenti e tecnologie digitali per elaborare soluzioni adatte a migliorare l'apprendimento	Saper usare le tecnologie digitali per supportare l'attuazione delle proprie idee. Saper pianificare strategie per portare a termine un'attività usando molteplici tecnologie Riflettere sull'uso dell'IA in una società sostenibile e sulle future implicazioni per il mondo del lavoro

ORGANIZZAZIONE E GESTIONE

Il CdC, nella riunione di ottobre, prende i primi accordi/compila la scheda di progettazione specificando:

- il referente
- i nomi dei docenti che attueranno il curricolo
- i tempi
- le attività proposte
- l'eventuale richiesta di supporto del Team ePolicy per l'attuazione delle competenze

La scheda va caricata dal Coordinatore di classe nella cartella appositamente predisposta entro la data stabilita dalla Dirigenza.

Se il docente realizza un'attività nuova, non disponibile nel repertorio suindicato, è pregato di compilare la scheda attività (disponibile su Drive) e di inviarla al team ePolicy per la sua archiviazione.

Il CdC verifica autonomamente l'acquisizione delle competenze digitali tramite verifica condivisa tra più docenti o tramite verifiche singole.

Le attività possono afferire sia al curricolo digitale, sia a quello di Educazione civica.

Il referente del curricolo digitale, in accordo con i membri del Team ePolicy, somministrerà agli studenti nel mese di maggio, su apposito modulo, un questionario relativo al percorso svolto, i cui risultati verranno illustrati nell'ultimo Collegio dei Docenti.

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.

I materiali didattici utili a realizzare le attività sono liberamente creati dai docenti o disponibili ai seguenti link:

- Generazioni Connesse - Le tematiche (le tematiche fondamentali del digitale con schede teoriche e operative)
- Generazioni Connesse - Il Kit Didattico (schede teoriche e applicazioni didattiche)
- https://www.ancheioinsegno.it (Schede didattiche elaborate da Parole O_stili)
- DigComp 2.2 Il Quadro delle Competenze Digitali per i Cittadini (esempi di attività proposte dalla versione DigComp 2.2).

Sono inoltre disponibili attività caricate sul Drive d'Istituto e realizzate dai docenti.

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.

1) Trattamento dei dati personali e particolari.

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica etc.

In particolare i dati possono essere suddivisi nelle seguenti categorie:

- i dati che permettono l'identificazione diretta di una persona, come i dati anagrafici (ad es. nome e cognome);
- i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad es. il codice fiscale, l'indirizzo IP, il numero di targa);
- i dati rientranti in specifiche categorie: si tratta dei dati cosiddetti particolari, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale di una persona, i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;
- i dati relativi a condanne penali e reati: si tratta dei dati cosiddetti giudiziari, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad es. i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto o l'obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

Questi dati subiscono, da parte dell'Istituto, un trattamento tramite le seguenti tipologie di operazioni: la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Le istituzioni scolastiche pubbliche possono trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali, oppure quelli espressamente previsti dalla normativa di settore. Per tali trattamenti non viene chiesto il consenso al trattamento alle famiglie o agli studenti.

Alcune categorie di dati personali degli/lle studenti/esse e delle famiglie, come quelli particolari e giudiziari, devono essere trattate con estrema cautela, nel rispetto di specifiche norme di legge, verificando in primis non solo la pertinenza e completezza dei dati, ma anche la loro indispensabilità rispetto alle "finalità di rilevante interesse pubblico" che si intendono perseguire.

Periodicamente, almeno una volta durante l'anno scolastico viene effettuata una Valutazione dei rischi sulla privacy relativamente ad alcune tipologie di trattamento dei dati particolari.

L'attenzione si focalizza nello specifico sui dati particolari, che la scuola tratta per favorire l'integrazione, come ad esempio dati relativi alle origini razziali.

Vengono anche esaminate le situazioni che riguardano dati relativi alla salute per adottare misure di sostegno degli alunni o i dati vaccinali con le ATS.

Per queste particolari categorie di dati viene richiesto espresso consenso alle famiglie o agli studenti, se maggiorenni.

La scuola fornisce una lettera di incarico per il trattamento dei dati al personale ATA, ai collaboratori scolastici e ai docenti.

2) Sito web istituzionale di riferimento e infrastrutture tecnologiche della scuola

La connessione al sito è protetta tramite HTTPS, così come tutte le transazioni su Google Workspace for Education.

La rete è protetta da firewall; l'accesso alla rete Wifi dell'istituto prevede due fattori di protezione: l'utilizzo di una password e l'autorizzazione al singolo dispositivo tramite MAC address.

I dati sono gestiti tramite il servizio offerto da "Axios", responsabile anche della gestione delle copie di backup. Ogni assistente amministrativo ha accesso soltanto alle aree della piattaforma e ai dati strettamente correlati con la funzione svolta.

I docenti, per l'accesso al registro elettronico sono dotati di username e password personale e hanno accesso soltanto ai dati indispensabili e relativi alla propria attività nelle proprie classi.

3.2 - Strumenti di comunicazione online (PUA)

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

Il nostro Istituto consente l'accesso a Internet attraverso una rete abbastanza adeguata ed in grado di supportare il traffico dati generato da un numero elevato di utenti. L'accesso ad Internet, protetto da software antivirus, è consentito:

- al personale docente e non docente per uso didattico e/o di formazione;
- agli alunni per lo svolgimento delle attività didattiche guidate dal docente e sotto la sua responsabilità.

Per garantire maggiore sicurezza nell'accesso ai dati particolari, le reti *didattica* e *segreteria* sono mantenute separate e gestite in modo autonomo e con regole differenti.

Si rammenta che, a norma delle leggi vigenti, l'utente è responsabile direttamente, civilmente e penalmente dell'uso effettuato del servizio Internet.

Per quanto riguarda l'accesso ad Internet, all'interno dei laboratori dell'Istituto si rimanda agli specifici regolamenti di accesso e di utilizzo vigenti approvati, consultabili sul sito della scuola.

Gli assistenti tecnici periodicamente provvedono alla manutenzione e all'aggiornamento del sistema e degli antivirus installati, richiedendo, ove necessario, l'intervento di tecnici esterni.

La posta elettronica istituzionale, fornita ad ogni docente, studente e al personale ATA, è protetta da antispam ed è fornita da Google Workspace for Education.

L'accesso al registro elettronico viene abilitato per docenti, genitori e studenti tramite credenziali di accesso da custodire con la dovuta diligenza. Il registro elettronico deve essere utilizzato esclusivamente per le finalità istituzionali predeterminate dall'Istituto (es. caricamento e lettura voti, assenze, avvisi, ecc.). Si evidenzia l'importanza di mantenere riservate le credenziali di accesso al RE da parte di genitori/tutori al fine di evitare l'utilizzo improprio dello stesso da parte degli studenti.

Al fine di garantire il diritto di accesso a Internet in condizioni di sicurezza, l'istituto ha considerato la prevenzione dei rischi in rete, in termini di uso consapevole delle tecnologie digitali e mediante i protocolli di sicurezza che rendono accessibile l'ambiente digitale, dall'antivirus ai firewall, all'aggiornamento periodico dei sistemi operativi e browser, dei software gestiti dai server, per garantire che il sistema sia il più possibile aggiornato e protetto dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo.

L'Istituto ha dunque adottato le necessarie precauzioni per interdire agli studenti e alle studentesse, negli spazi della scuola, l'accesso online a materiali a loro non adatti, attraverso l'adozione di sistemi di filtraggio hardware (filtraggio dei contenuti).

Si invita quindi l'intera comunità scolastica a rispettare le seguenti linee guida di buona condotta/buone pratiche:

- tutela della propria privacy, di quella degli altri utenti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui si ha accesso;
- rispetto della legislazione vigente;
- rispetto di una netiquette, cioè di regole condivise che disciplinano il rapportarsi fra utenti della rete, siti, forum, mail e qualsiasi altro tipo di comunicazione a distanza;
- controllo della validità e dell'origine delle informazioni a cui si accede o che si ricevono;
- rispetto dei diritti di autore e dei diritti di proprietà intellettuale;
- divieto di installare e/o scaricare sui device software non autorizzati o senza licenza;
- accesso consentito al personale scolastico ad esclusivo uso didattico o di formazione;
- accesso consentito agli alunni sotto la responsabilità di un docente.

Nel caso in cui un docente preveda l'utilizzo di Internet all'interno dell'attività didattica è opportuno che:

- dia chiare indicazioni agli studenti sul corretto utilizzo della rete;
- si assuma la responsabilità di segnalare prontamente all'Ufficio Tecnico e/o all'animatore digitale eventuali malfunzionamenti/danneggiamenti o l'utilizzo improprio della rete;
- non salvi sui computer dell'Istituto file contenenti dati personali e/o particolari;
- filtri i contenuti in base all'età e al ruolo dell'utente;
- richieda l'accesso per i dispositivi personali alla rete Internet d'Istituto tramite apposito modulo rintracciabile sul sito della scuola;

- usi password personali di accesso forti e non vulnerabili (almeno 8 caratteri con numeri, caratteri maiuscoli e minuscoli e caratteri speciali);
- non memorizzi password sui dispositivi scolastici;
- non condivida le password con nessuno.

L'Istituto fornisce in comodato d'uso dei pc a studenti in situazione di svantaggio socio-economico.

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.

Con la Circolare Ministeriale n. 3392 del 16.06.2025 il Ministero dell'Istruzione e del Merito ha stabilito che, a partire dal 1° settembre 2025, in tutte le scuole secondarie di secondo grado è vietato l'uso dei telefoni cellulari durante l'orario scolastico. Sulla base di quanto premesso, è stato redatto un regolamento apposito, relativo al divieto di uso degli smartphone, che è parte integrante del PTOF e a cui si rimanda.

Resta tuttavia possibile per gli studenti usare dispositivi mobili a scuola (BYOD). Anche in questo caso l'Istituto ha predisposto un regolamento apposito, parte integrante del PTOF, di cui qui si riporta un estratto:

La scuola riconosce agli studenti la possibilità di una formazione digitale che parta dal saper utilizzare in modo consapevole e adeguato i propri dispositivi: "La scuola digitale, in collaborazione con le famiglie e gli enti locali, deve aprirsi al cosiddetto BYOD (Bring Your Own Device), ossia a politiche per cui l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficientemente integrato".

Si tratta di offrire agli studenti opportunità innovative per ampliare la loro formazione, migliorando contestualmente l'ambiente educativo e di apprendimento. Il nostro Istituto, pertanto, intende favorire l'uso responsabile dei dispositivi digitali mobili personali, integrandoli nell'attività didattica quotidiana dei docenti che ne vorranno fare uso: il che comporta la necessità di definire con chiarezza le norme che regolano l'uso degli stessi a scuola per fini didattici, anche allo scopo di tutelare gli allievi dai rischi e dai pericoli dall'uso improprio dei dispositivi, di formarli alla corretta gestione delle nuove tecnologie ed ai principi della sicurezza informatica.

ART. 1 - DISPOSITIVI AMMESSI

In tutte le classi sono ammessi i seguenti dispositivi mobili: qualsiasi computer portatile, tablet, e-reader purché non connessi alla rete.

ART. 2 - DISPOSITIVI VIETATI

In conformità alla Nota Ministeriale n. 3392 del 16.06.2025, è vietato l'uso del telefono cellulare durante lo svolgimento dell'attività didattica (anche a fini didattici) e più in generale in orario scolastico.

L'uso dello smartphone è consentito esclusivamente nei seguenti casi:

- per dichiarate e motivate ragioni personali (es. necessità di salute): i genitori possono inoltrare formale richiesta al DS che il proprio figlio/a possa tenere con sé il cellulare;
- quando previsto dal Piano Didattico Personalizzato (PDP);
- quando previsto dal Piano Educativo Personalizzato (PEI);

Gli alunni, in possesso del cellulare in quanto autorizzati, possono utilizzarlo limitatamente alle attività di cui alla deroga concessa. L'eventuale autorizzazione a tenere il cellulare a scuola non implica la conseguente responsabilità, da parte dell'Istituzione Scolastica, per eventuali smarrimenti, furti o danneggiamenti.

Per ogni altra indicazione in merito, comprese le misure organizzative per la gestione del proprio smartphone a scuola, si rimanda al Regolamento sull'uso degli smartphone negli istituti scolastici di secondo grado e al Codice disciplinare degli alunni, allegati al P.T.O.F.

ART. 3 - USO DEI DISPOSITIVI

I dispositivi ammessi, di cui agli artt. 1 e 2, devono essere usati a scuola soltanto per scopi didattici. Gli studenti possono registrare video, file audio o scattare foto in classe e/o in altri ambienti scolastici (ad es. laboratori, palestra) solo con il consenso esplicito e la supervisione dell'insegnante, e sempre a fini didattici. Qualsiasi uso improprio e non autorizzato prevede il ritiro del dispositivo e la segnalazione al Dirigente Scolastico.

ART. 4 - UTILIZZO DIDATTICO DI AUDIO E VIDEO CONDIVISIONE DI FILE E GESTIONE DEI SOFTWARE

Le fotografie e i file audio-video registrati a scuola, possono essere pubblicati, solo previa autorizzazione del docente ed esclusivamente in canali di comunicazione e piattaforme individuate ed ufficializzate dall'Istituto e unicamente a scopi didattici.

È tassativamente vietata la pubblicazione e diffusione di riprese audio-video e di fotografie effettuate dagli studenti all'interno degli ambienti scolastici, su qualunque tipo di piattaforma non autorizzata.

Si richiama l'attenzione degli studenti, dei docenti e delle famiglie sulle possibili conseguenze: tali pratiche possono dar luogo a gravi violazioni del diritto alla riservatezza e tutela dei dati personali di altre persone, incorrendo in sanzioni disciplinari, pecuniarie e di natura penale.

Ogni dispositivo dovrà essere dotato di software antivirus per garantire un adeguato livello di sicurezza.

ART. 5- RESPONSABILITÀ DEI DISPOSITIVI

Gli studenti sono responsabili personalmente dei propri dispositivi. L'alunno deve prendere coscienza del fatto che il dispositivo mobile è uno strumento funzionale al suo apprendimento: pertanto è sua precisa responsabilità presentarsi a scuola, quando richiesto, con il proprio dispositivo, garantendone la funzionalità (adeguata capienza di memoria) come qualsiasi altro supporto alla didattica. Agli studenti è richiesto di caricare completamente il dispositivo a casa e devono essere consapevoli che:

a. non sarà possibile ricaricare i dispositivi durante l'orario di lezione;

b. non sarà possibile ricaricare i dispositivi in aula.

La scuola non è responsabile della custodia dei dispositivi e di eventuali danni ad essi cagionati dal proprietario o da altri studenti. Gli studenti hanno la responsabilità di riportare a casa il dispositivo al termine delle lezioni. La scuola non sarà ritenuta responsabile e non si assume la responsabilità della custodia del dispositivo lasciato a scuola; l'Istituto non risponde di eventuali furti, rotture o smarrimenti.

ART. 6- CONNESSIONE ALLA RETE WI-FI DELL'ISTITUTO

Non è consentito connettersi alla rete Wi-fi d'Istituto mediante dispositivi personali, pena responsabilità disciplinari.

La scuola si riserva il diritto di monitorare le attività online degli utenti, rivelandone il contenuto alle forze dell'ordine qualora lo ritenga necessario.

ART. 7- COMPORTAMENTI SANZIONABILI PER IL MANCATO RISPETTO DEL REGOLAMENTO

L'uso della tecnologia comporta responsabilità personali. Gli studenti sono tenuti a rispettare le regole dell'Istituto e quelle del presente Regolamento, pena l'attivazione di azioni disciplinari.

ART. 8- SANZIONI PER IL MANCATO RISPETTO DEL REGOLAMENTO

Le sanzioni sono commisurate alla gravità dell'accaduto e verranno irrogate come previsto dal Regolamento disciplinare degli Studenti dell'Istituto o dalle forze dell'ordine nel caso di reati gravi.

ART. 9- COMPITI DEL DOCENTE

L'insegnante ha la responsabilità e il dovere di sorvegliare costantemente l'attività degli alunni. Deve segnalare con tempestività al Dirigente Scolastico eventuali anomalie e/o comportamenti degli alunni in contrasto con il presente regolamento.

ART. 10- COMPITI DELL'ISTITUTO E COLLABORAZIONE DELLE FAMIGLIE

La Scuola promuove azioni di educazione alla cittadinanza digitale. Sarà cura della scuola provvedere a mettere a disposizione un adeguato numero di dispositivi per gli studenti la cui condizione socio - economica, debitamente certificata, non ne consenta l'acquisto, al fine di permettere la partecipazione di tutti gli alunni della classe alle attività programmate dai docenti. Le famiglie degli allievi, preso atto degli articoli sopra citati, sono tenute a collaborare con l'Istituto nel favorire il rispetto del presente regolamento.

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.

La comunità scolastica tutta (docenti, genitori, studenti e studentesse, personale ATA) deve essere sensibile e deve agire con tempestività e responsabilmente nel caso sospetti o accerti che uno studente o una studentessa sia stato vittima o presunta vittima di casi di bullismo, cyberbullismo, adescamento on line, sexting e di altri cybercrimes.

Le procedure saranno condivise con l'intera comunità scolastica mediante:

- gli organi collegiali deputati (il Collegio dei Docenti)
- il sito web della scuola
- assemblee dedicate rivolte a studenti e famiglie

Qui di seguito si ricordano alcuni rischi relativi al mondo virtuale che potrebbero – in molte circostanze – non essere percepiti come tali soprattutto dagli studenti e dalle studentesse, ma che invece devono essere segnalati secondo le procedure allegate a questa ePolicy. E' dunque importante che la comunità educante (genitori, docenti, personale ATA), ma anche gli studenti e le studentesse, possano conoscerli, con l'obiettivo di prevenirli e, all'occorrenza, segnalarli.

- esposizione a contenuti ingannevoli e ad informazioni scorrette (fake news);
- esposizione a contenuti violenti, o uso di videogiochi diseducativi (gaming online, gioco d'azzardo online);
- esposizione a siti violenti, razzisti, inneggianti all'odio, che invitano al suicidio o a comportamenti alimentari scorretti (hate speech, siti pro-anoressia e pro-bulimia);
- contatti con adulti che vogliono conoscere e avvicinare ragazzi e ragazze (adescamento on line);
- molestie, vessazioni o maltrattamenti da coetanei mediante la rete, i social, le chat (cyberbullismo);
- scambio e/o diffusione non autorizzata di materiale a sfondo sessuale (sexting);
- uso eccessivo di Internet e dei device che mina la socialità (dipendenza);
- uso improprio di materiali personali – in particolare foto e video – (web reputation);
- uso scorretto dei device dell'Istituto (p.e. mediante il caricamento/l'apertura di programmi contenenti malware; installazione di software non autorizzati, senza licenza, non conformi alle leggi sul copyright);

E' fondamentale monitorare con attenzione le relazioni all'interno della classe, onde poter individuare potenziali situazioni di disagio ed intervenire tempestivamente, anche mediante il ricorso alle figure specializzate, per sostenere il singolo nelle situazioni di difficoltà personale e favorire nel gruppo un clima positivo, di reciproca accettazione e rispetto.

Tale percorso potrà essere ulteriormente rinforzato dalla partecipazione a progetti e/o iniziative coerenti con i temi sopramenzionati.

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.

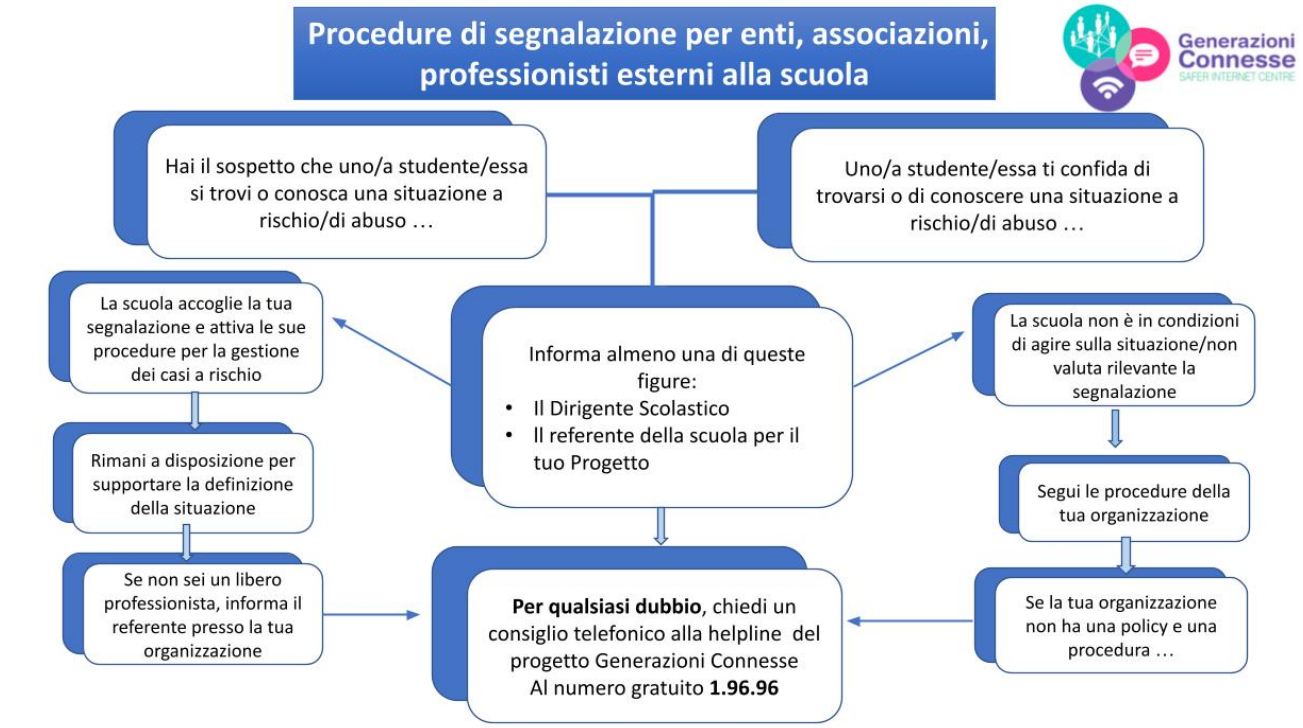
Strumenti a disposizione di studenti/esse

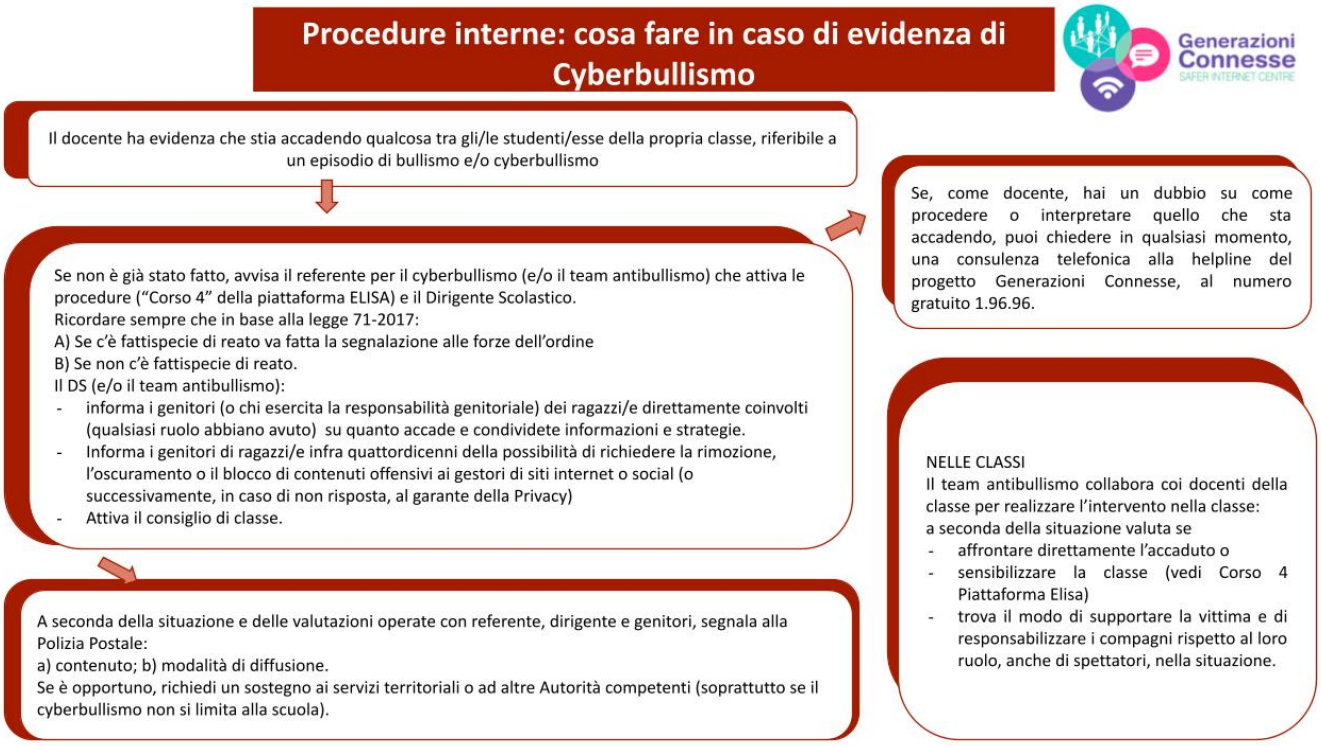
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

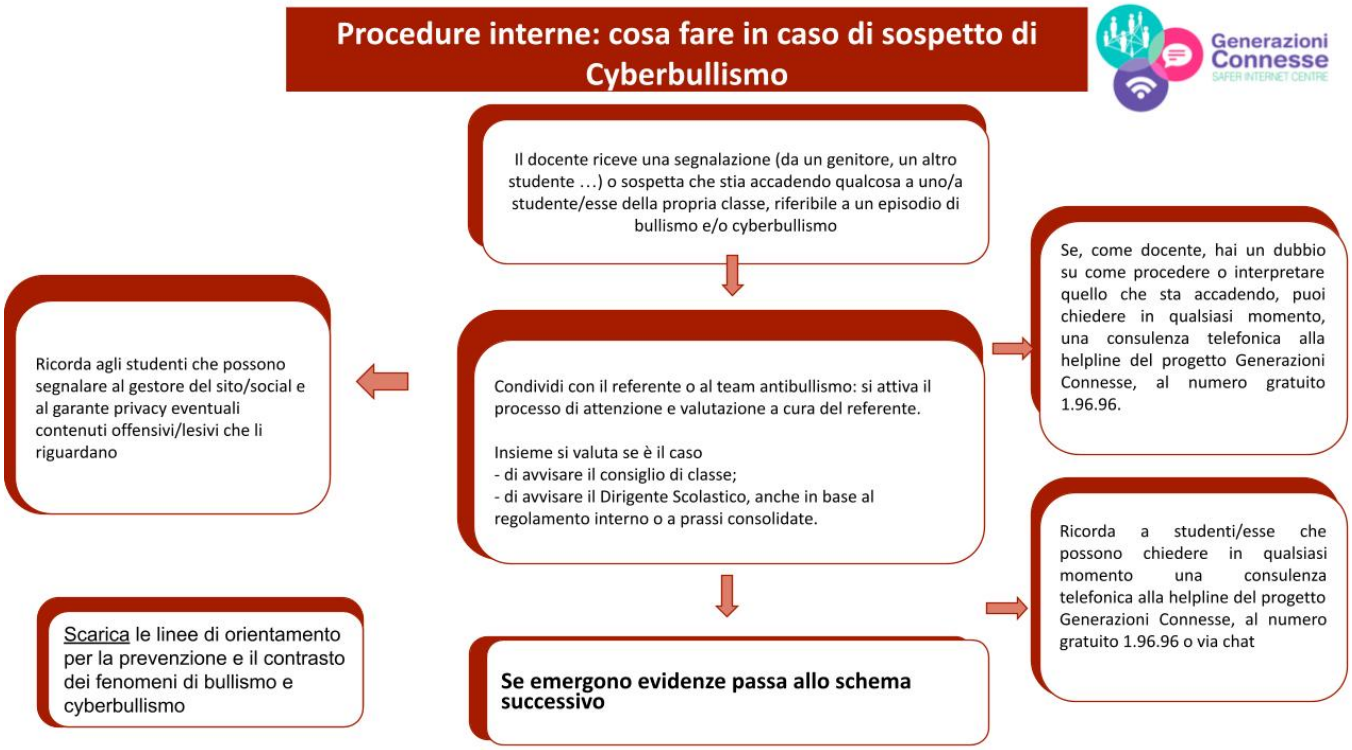
In particolare, sarebbe utile che la scuola attivi un sistema di segnalazione utile anche al monitoraggio dei fenomeni dal quale partire per integrare azioni didattiche preventive e giornate di sensibilizzazione, insieme agli Enti/Servizi presenti sul territorio di riferimento. Importante, altresì, immaginare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

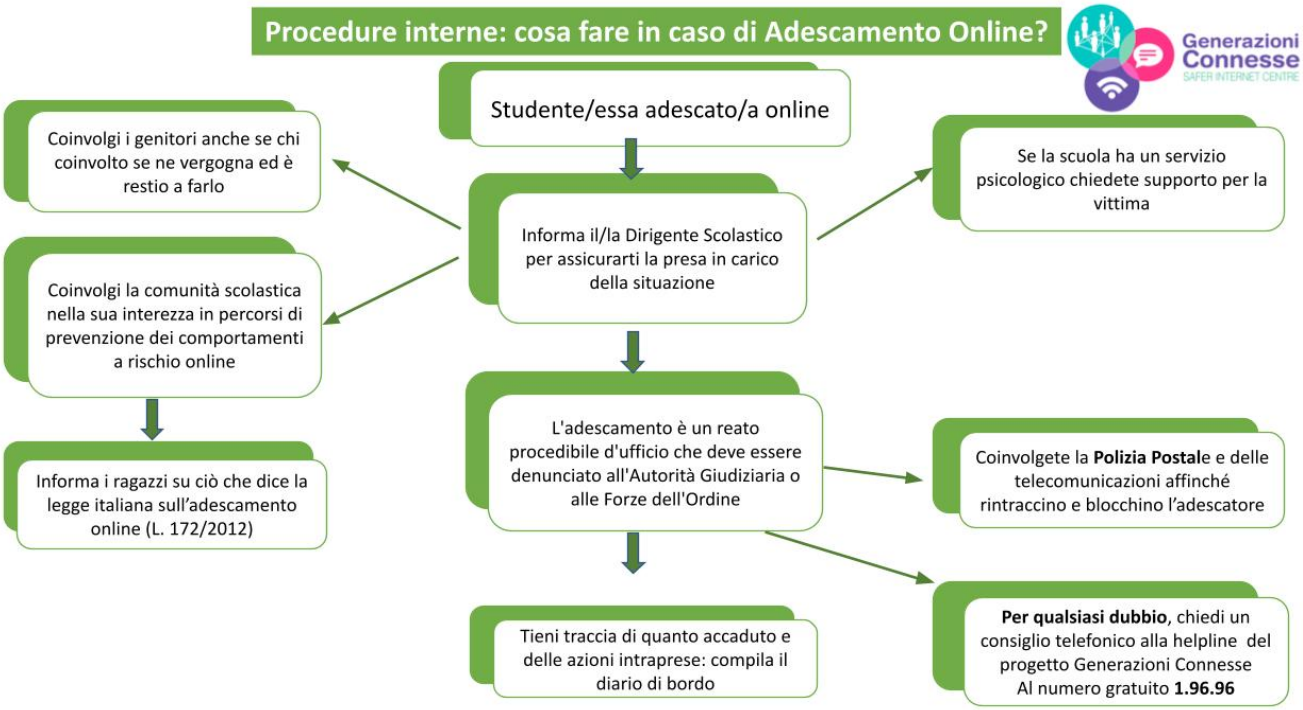
Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle Linee di Orientamento per la prevenzione e il contrasto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

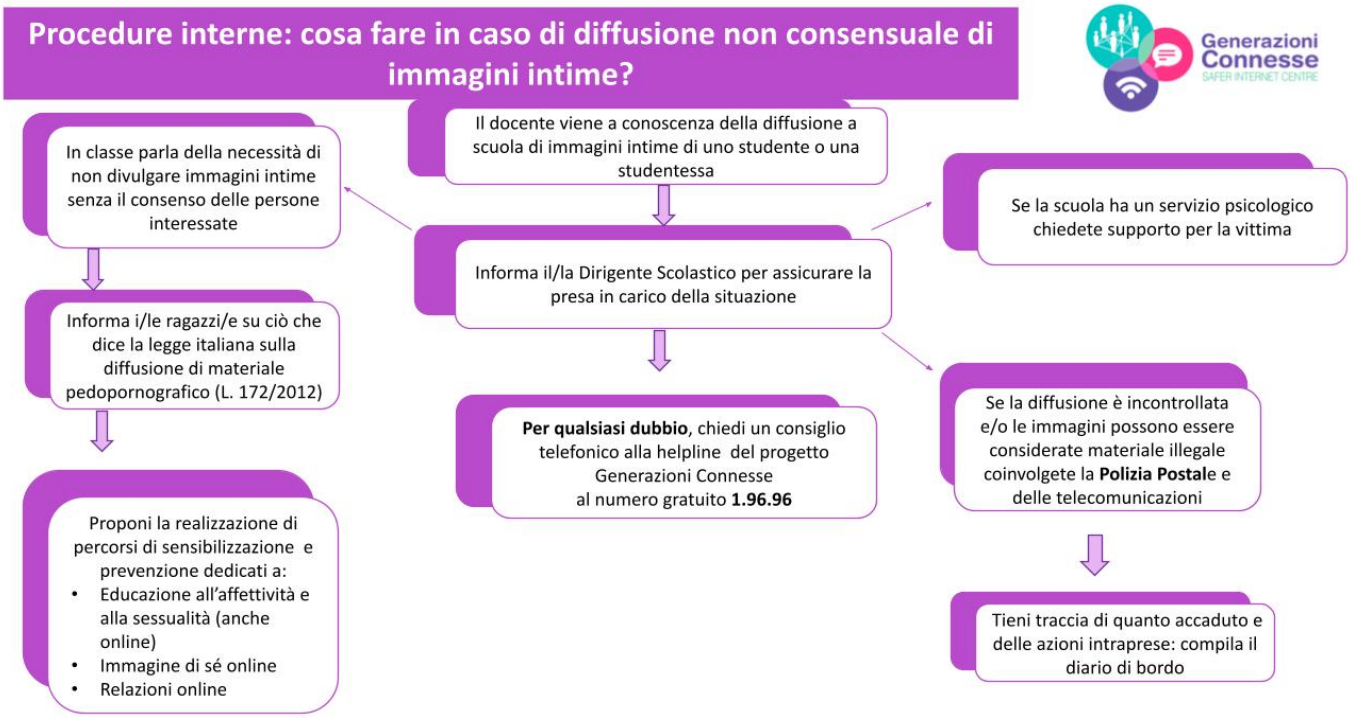
Procedure


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
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
Rimani a disposizione per supportare la definizione della situazione
Segui le procedure della tua organizzazione
Se non sei un libero professionista, informa il referente presso la tua organizzazione
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse Al numero gratuito 1.96.96
Se la tua organizzazione non ha una policy e una procedura …


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, 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.
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.
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.
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).


Procedure interne: cosa fare in caso di sospetto di Cyberbullismo
Generazioni Connesse
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.
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano
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 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
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
Informa i ragazzi su ciò che dice la legge italiana sull'adescamento online (L. 172/2012)
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
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



Procedure adottate dal nostro Istituto:

Caso A (sospetto caso di bullismo/cyberbullismo): se un docente riceve una segnalazione (per esempio da una presunta vittima, da un altro docente, da un genitore, da uno studente, da testimoni, da un collaboratore scolastico) o sospetta che nella propria classe ci sia un caso di bullismo o cyberbullismo o di altra problematica relativa ai rischi on line, si segue la procedura qui indicata:

- il docente avvisa il **Coordinatore di classe** e il **referente d'Istituto** per il contrasto al bullismo e cyberbullismo.
- Il referente informa per iscritto il **Dirigente Scolastico**.
- Il referente effettua una *valutazione approfondita* per capire se il caso si inquadra in una situazione di bullismo/cyberbullismo e vittimizzazione. La valutazione approfondita avviene attraverso colloqui con gli attori coinvolti a qualunque titolo, gestiti dal referente e/o da un membro del Team per l'emergenza.
- Può essere utile, a seconda delle situazioni, informare anche il **Consiglio di classe** o altri **docenti della classe** in quanto l'attenzione dei singoli docenti può essere meglio finalizzata ad un'osservazione delle dinamiche all'interno della classe. Lo scopo, in questa fase è osservare il clima della classe, le dinamiche relazionali e tener traccia di osservazioni e valutazioni.
- Se la situazione non si configura come caso di bullismo o cyberbullismo, il referente valuta con il Coordinatore di classe e il docente che ha segnalato il sospetto le possibili strategie d'intervento, che di norma comportano uno o più *interventi educativi* sulla classe, nell'ottica di una *prevenzione universale*. Questa modalità di azione può trovare spazio anche all'interno di momenti laboratoriali, (gestiti dal docente, da un membro del Consiglio di classe, dal referente per il contrasto al bullismo e cyberbullismo, dal Team per l'emergenza) svolgendo con la classe attività che diano a studentesse e studenti occasioni di riflessione anche personale, condivisa e informazioni su come agire per denunciare ciò cui potrebbero aver assistito, di cui potrebbero aver sentito parlare. Può essere utile parlare alla classe, senza riferimenti alla vicenda, ma invitando gli studenti e le studentesse a chiedere aiuto se pensano di vivere situazioni o di subire atti identificabili come bullismo e cyberbullismo o riconducibili ad altri rischi on line.
- Il referente monitora la situazione nel breve e lungo periodo.

Stante la complessa e sempre diversa dinamica di situazioni analoghe a quella descritta, si ricorda che i docenti, gli studenti e le famiglie possono essere sempre supportati dalla Helpline della piattaforma Generazioni Connesse al numero gratuito 19696.

Se l'iniziale sospetto si configura come caso di bullismo e/o cyberbullismo, si adotta la procedura indicata nel "Caso B".

Caso B (evidenza caso/i di bullismo/cyberbullismo): se un docente è certo che nella propria classe ci sia un caso di bullismo, cyberbullismo o altra problematica riconducibile ai rischi on line, si segue la procedura qui indicata:

- chi segnala il caso avvisa immediatamente il **referente** per il contrasto al bullismo e al cyberbullismo.
- Il referente informa per iscritto il **Dirigente Scolastico**.
- Se si ravvisano situazioni di reato, vengono attivate le forze dell'ordine.
- Se non si ravvisano situazioni di reato, il referente o un docente del Team per l'emergenza - eventualmente coadiuvato dal DS, dal Coordinatore o da altro docente coinvolto - effettua la *valutazione approfondita* mediante colloqui con studenti e studentesse direttamente coinvolti (siano essi vittime, attori, spettatori).
- Il referente contatta i **genitori** (anche degli studenti maggiorenni) in merito ai colloqui effettuati con i propri figli.
- Al termine del procedimento utile ad acclarare i fatti, viene convocato **in sessione straordinaria il Consiglio di Classe** in cui il referente riferisce quanto emerso.
- Il Consiglio di classe valuta e decide le **sanzioni disciplinari** (per le situazioni specifiche si faccia riferimento al Codice disciplinare degli studenti allegato al PTOF) e opera attivamente in sinergia con il referente perché la classe e gli attori coinvolti possano beneficiare di una o più occasioni di confronto e riflessione sulle tematiche legate all'evento.
- Il referente monitora la situazione nel breve e lungo periodo.

A seconda delle situazioni possono essere coinvolti:

- lo psicologo scolastico per una consulenza di supporto all'azione della scuola ed eventualmente per supportare tutti o alcuni degli attori dell'evento;
- I servizi e le associazioni territoriali di riferimento nella necessità di un sostegno mirato ed eventualmente prolungato

E' importante che di fronte ad atteggiamenti supposti o reali di bullismo e/o cyberbullismo, gli studenti e le studentesse siano educati a non essere omertosi (per esempio per paura di ritorsioni o vendette, per disinteresse, per non riconoscimento della gravità del fatto). Si ribadisce dunque la significatività di percorsi educativi in merito che è opportuno possano essere attivati anche alla luce di casi di cui si ha sospetto o che sono evidenti.

Gli studenti e le studentesse sono parte attiva della relazione educativa; per aiutarli a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, l'Istituto prevede questi strumenti:

- possibilità di rivolgersi, tramite mail istituzionale o di persona, al referente per il contrasto del bullismo e del cyberbullismo, scrivendo al seguente account: referente.bullismo@istitutovanonimenaggio.edu.it
- form specifico per segnalazione bullismo/cyberbullismo presente sul sito
- box per la raccolta di segnalazioni anonime che verrà dislocato in uno spazio accessibile e ben visibile della scuola
- sportello di ascolto con lo psicologo scolastico
- possibilità di rivolgersi alla Help line del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità

della scuola.

Si segnalano i seguenti servizi territoriali di possibile utilità:

Co.Re.Com: www.corecomlombardia.it Sportello Help-Web Reputation Giovani; indirizzo: c/o Consiglio Regionale, Via F.Filzi, 22 20124 Milano; Contatti: 02.67482725.

Garante per l'Infanzia e l'Adolescenza: Indirizzo: c/o Consiglio Regionale, Via F.Filzi, 22 20124 Milano; Contatti: 02.67486290; garante@consiglio.regione.lombardia.it

MIM: https://www.istruzione.it/bullismo-e-cyberbullismo/index.html

USR: https://www.mim.gov.it/web/usr-lombardia

USP: https://www.mim.gov.it/web/como Indirizzo: via Borgo Vico, 171 22100 Como; Contatti: 031.237211; usp.co@istruzione.it

Polizia Postale e delle Comunicazioni: https://www.commissariatodips.it/

Firmato da:
PERTICARO GIUSEPPE
Codice fiscale: PRTGPP68E13Z133D
28/05/2026 12:34:42