



Documento di ePolicy

D.D. "DON BOSCO" BASTIA UMBRA

VIA ROMA 54 - 06083 - BASTIA UMBRA
Perugia (PG) - Umbria
Data di approvazione: 13/11/2025 - 17:17

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.

La presente ePolicy è il documento ufficiale della Direzione Didattica "Don Bosco" che definisce le regole, le azioni e le responsabilità condivise per garantire un uso sicuro, consapevole e responsabile delle tecnologie digitali all'interno della comunità scolastica.

È rivolta a docenti, personale ATA, alunni, famiglie e a tutti coloro che collaborano con la scuola, promuovendo un clima educativo fondato sul rispetto, la collaborazione e la cittadinanza digitale.

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 pedagogo, 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.

Affinché l'ePolicy della Direzione Didattica "Don Bosco" sia uno strumento realmente efficace e condiviso, è fondamentale che ogni componente della comunità scolastica - personale docente e ATA, alunni, famiglie e partner esterni - contribuisca alla sua attuazione, secondo il proprio ruolo e responsabilità.

La scuola riconosce l'importanza della collaborazione tra tutte le figure educative per promuovere una cultura digitale positiva, sicura e inclusiva, in coerenza con il **PTOF** e con la **Mission educativa dell'Istituto**.

Il Dirigente Scolastico

Il Dirigente Scolastico:

- promuove la cultura della sicurezza digitale all'interno della scuola, in linea con le indicazioni del MIM e con la normativa vigente;
- assicura che l'uso delle tecnologie sia coerente con le finalità educative e didattiche dell'Istituto;
- garantisce la sicurezza della rete, dei dispositivi e la protezione dei dati personali;
- coordina la redazione, l'attuazione e l'aggiornamento dell'ePolicy;
- promuove la formazione continua del personale sulla sicurezza digitale e sull'uso consapevole delle tecnologie;
- è a conoscenza e attiva le procedure necessarie in caso di incidenti informatici o comportamenti a rischio online.

L'Animatore Digitale e il Team per l'Innovazione

L'Animatore Digitale e il Team per l'Innovazione Digitale:

- collaborano con il Dirigente e con il Referente ePolicy nell'attuazione del piano d'azione digitale;
- organizzano attività di formazione e aggiornamento rivolte ai docenti;
- promuovono la diffusione delle buone pratiche didattiche digitali;
- vigilano sull'uso corretto delle TIC da parte degli alunni durante le attività laboratoriali e didattiche.

Il Referente per il Bullismo e Cyberbullismo

Il Referente:

- coordina le iniziative di prevenzione e contrasto dei fenomeni di bullismo e cyberbullismo;
- collabora con il Dirigente e con il Team ePolicy nella gestione di eventuali segnalazioni;
- promuove attività di sensibilizzazione rivolte a docenti, alunni e famiglie;
- mantiene i contatti con gli enti territoriali e con la Polizia Postale per azioni di informazione e formazione.

Il Team Antibullismo e per l'Emergenza

Il Team Antibullismo:

- collabora con il Dirigente nella definizione di strategie preventive;
- interviene in situazioni di disagio o conflitto, favorendo la mediazione educativa;
- promuove progetti e iniziative per la conoscenza e la prevenzione del bullismo e del cyberbullismo;
- comunica a tutta la comunità scolastica la possibilità di rivolgersi al Team per consulenze o segnalazioni.

I Docenti

I docenti:

- guidano gli alunni all'uso sicuro e consapevole delle tecnologie digitali;
 - integrano nelle proprie attività didattiche esperienze di educazione alla cittadinanza digitale;
 - vigilano durante l'uso dei dispositivi digitali, favorendo comportamenti corretti e rispettosi;
 - informano tempestivamente il Dirigente o il Referente ePolicy di eventuali situazioni di rischio o uso improprio della rete;
 - collaborano con le famiglie per educare i bambini all'uso responsabile degli strumenti digitali.
-

Il Responsabile della Protezione dei Dati (RPD/DPO)

Il RPD:

- garantisce il rispetto delle normative sulla protezione dei dati personali;
 - fornisce consulenza alla scuola su privacy e sicurezza informatica;
 - partecipa alle azioni di informazione e formazione sulla tutela dei dati sensibili.
-

Il Personale ATA

Il personale amministrativo, tecnico e ausiliario:

- supporta l'attuazione delle misure di sicurezza informatica e la corretta gestione dei dati;
 - segnala comportamenti inadeguati o situazioni di rischio;
 - collabora nella diffusione di buone pratiche digitali, contribuendo al clima di responsabilità condivisa.
-

Gli Alunni

Gli alunni della scuola primaria, secondo il proprio grado di maturità:

- imparano a utilizzare in modo corretto e sicuro i dispositivi e le risorse digitali;
- rispettano le regole di comportamento online e i compagni;
- partecipano con impegno ai progetti di educazione digitale e di cittadinanza responsabile.

Per la scuola dell'infanzia, l'avvicinamento al digitale avviene in forma **giocosa e mediata dall'adulto**, attraverso esperienze di robotica educativa, narrazione e gioco simbolico.

I Genitori

Le famiglie sono parte attiva della comunità educante e:

- collaborano con la scuola per accompagnare i figli a un uso consapevole delle tecnologie;
- partecipano agli incontri informativi e condividono le linee educative dell'Istituto;
- sostengono l'attuazione del Patto di corresponsabilità e del documento ePolicy;
- segnalano tempestivamente situazioni di rischio o disagi legati all'uso della rete.

Enti esterni e associazioni

Gli enti e le associazioni che collaborano con la Direzione Didattica "Don Bosco":

- si impegnano a rispettare le linee guida dell'ePolicy;
- propongono progetti e attività coerenti con i principi di sicurezza, inclusione e cittadinanza digitale;
- promuovono comportamenti sicuri e responsabili durante le attività con gli alunni;
- collaborano con la scuola per garantire la tutela dei minori e la qualità educativa degli interventi.

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.

Integrazione dell'ePolicy nei documenti dell'Istituto

La Direzione Didattica "*Don Bosco*" riconosce l'ePolicy come parte integrante della propria identità educativa e organizzativa.

Il documento, in coerenza con le **Linee Guida del MIM** e con le più recenti indicazioni ministeriali sull'uso consapevole e responsabile delle tecnologie digitali e dell'intelligenza artificiale a scuola, sarà recepito e richiamato nei principali atti che regolano la vita scolastica e i rapporti con le famiglie.

Regolamento di Istituto

Il Regolamento d'Istituto sarà aggiornato con specifici riferimenti all'ePolicy, in particolare riguardo:

- le regole di utilizzo dei dispositivi digitali da parte di docenti e alunni;
- la sicurezza informatica e la protezione dei dati personali;
- il comportamento corretto e rispettoso negli ambienti digitali;
- la prevenzione di episodi di bullismo e cyberbullismo.

Tali indicazioni saranno formulate in modo chiaro e comprensibile, con un linguaggio adatto all'età degli alunni e condiviso con le famiglie.

Patto Educativo di Corresponsabilità

Nel Patto di Corresponsabilità tra scuola e famiglia saranno inseriti i riferimenti all'ePolicy per rafforzare la collaborazione educativa tra le parti.

La scuola si impegna a:

- organizzare momenti di formazione e informazione per genitori e docenti sull'uso consapevole delle tecnologie e sull'educazione digitale;
- promuovere percorsi di cittadinanza digitale sin dalla scuola dell'infanzia, con attività ludiche e laboratoriali mirate alla costruzione di comportamenti corretti, responsabili e sicuri online.

Le famiglie, a loro volta, si impegnano a:

- condividere e sostenere le regole stabilite dall'Istituto sull'uso dei dispositivi digitali;
- accompagnare i propri figli nell'apprendimento di comportamenti rispettosi e sicuri nell'ambiente digitale;
- collaborare con la scuola nella prevenzione e nella gestione di eventuali situazioni problematiche.

Piano Triennale dell'Offerta Formativa (PTOF)

Nel PTOF l'ePolicy trova spazio come parte integrante della progettualità educativa dell'Istituto.

Sono previste:

- azioni di **media education** e **educazione alla cittadinanza digitale**;
- percorsi laboratoriali di **robotica educativa**, **coding** e **intelligenza artificiale responsabile**, calibrati sull'età degli alunni;
- attività di sensibilizzazione rivolte a docenti e famiglie;
- collaborazioni con enti, associazioni e servizi del territorio per la promozione della sicurezza digitale e della partecipazione consapevole alla vita online.

RAV e miglioramento

Nel **Rapporto di Autovalutazione (RAV)**, l'ePolicy sarà richiamata tra le azioni strategiche per il miglioramento, in particolare nell'ambito della **competenza digitale** e della **cittadinanza attiva e responsabile**.

La sua implementazione sarà oggetto di monitoraggio continuo e di revisione periodica, con particolare attenzione alla partecipazione della comunità educante e all'impatto delle azioni formative sul benessere e sulla sicurezza di alunni e personale.

Conclusione

L'integrazione dell'ePolicy nei documenti fondamentali dell'Istituto consente di rendere **coerente e condivisa la visione educativa digitale**, ponendo al centro il bambino e la bambina come cittadini digitali del futuro, capaci di utilizzare la tecnologia con consapevolezza, creatività e responsabilità.

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

1. il curriculum 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.

La Direzione Didattica “Don Bosco” considera la diffusione e la condivisione dell’ePolicy parte fondamentale del proprio impegno educativo e formativo. Il documento non è solo uno strumento tecnico o normativo, ma un mezzo per **promuovere una cultura digitale consapevole, partecipata e responsabile** all’interno della comunità educante.

1. Informazione della comunità educante

L’Istituto promuove una costante azione di informazione e sensibilizzazione sull’uso consapevole e sicuro di Internet e delle tecnologie digitali, rivolta a docenti, alunni e famiglie.

L’ePolicy è condivisa attraverso momenti dedicati di presentazione e formazione che si inseriscono nel più ampio percorso di educazione civica e digitale previsto dal curriculum di istituto, in coerenza con il quadro di riferimento europeo **DigComp 2.2**.

Le principali modalità di condivisione e informazione prevedono:

- la pubblicazione dell’ePolicy e delle versioni sintetiche sul **sito web istituzionale**;
- la presentazione della versione per le **famiglie** durante incontri informativi e colloqui scuola-famiglia;
- l’inserimento della versione per **gli alunni** all’interno delle attività di educazione alla cittadinanza digitale, con linguaggio e strumenti adeguati all’età;
- l’organizzazione di **laboratori, giornate tematiche e incontri formativi** in collaborazione con esperti esterni, volti a rafforzare le competenze digitali e la consapevolezza dei rischi e delle opportunità della rete.

In particolare, per la scuola dell’infanzia e primaria, la comunicazione avviene in modo **ludico e laboratoriale**, attraverso storie, giochi di ruolo e attività creative che favoriscono la comprensione dei concetti di sicurezza, rispetto e collaborazione anche nel mondo digitale.

2. Comunicazione e condivisione con gli attori pubblici e privati

La Direzione Didattica “Don Bosco” promuove la collaborazione con il territorio per la realizzazione di iniziative condivise sui temi della **cittadinanza digitale**, della **media education** e della **prevenzione dei rischi online**.

L’ePolicy costituisce un punto di riferimento per enti, associazioni, aziende e realtà del terzo settore che operano in sinergia con la scuola, garantendo che ogni intervento sia coerente con i valori educativi dell’Istituto e con le normative vigenti in materia di tutela dei minori e protezione dei dati personali.

L’Istituto:

- comunica l’adozione e l’aggiornamento dell’ePolicy all’**USR di riferimento** e al **Comune (Servizi Istruzione e Servizi Sociali)**;
- condivide gli **allegati sintetici informativi** con le istituzioni e le realtà partner del territorio;

- partecipa a **reti e tavoli di lavoro locali** per la promozione dell'educazione digitale e dell'uso etico della tecnologia;
- valorizza le esperienze di **co-progettazione** con soggetti pubblici e privati su progetti di innovazione didattica, sicurezza digitale e inclusione tecnologica.

3. Educazione all'Intelligenza Artificiale

In coerenza con la **Nota MIM n. 2792 del 17 ottobre 2024**, l'Istituto promuove un approccio **critico, etico e responsabile** all'uso dell'Intelligenza Artificiale nella didattica.

Sono previste azioni di sensibilizzazione rivolte a docenti e genitori, finalizzate a comprendere le potenzialità educative e i limiti degli strumenti di IA, nel rispetto della tutela dei dati personali e del principio della centralità della persona.

Anche con i bambini, in forme ludiche e narrative, si avviano riflessioni sull'uso delle "macchine intelligenti" come strumenti di supporto alla creatività e non di sostituzione del pensiero umano.

Conclusione

Attraverso la diffusione, la comunicazione e la condivisione dell'ePolicy, la Direzione Didattica "*Don Bosco*" intende rafforzare la collaborazione tra scuola, famiglie e territorio, per costruire insieme una comunità educante digitale fondata su **sicurezza, responsabilità, partecipazione e fiducia**.

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 del 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

La Direzione Didattica "Don Bosco" promuove una visione educativa della cittadinanza digitale come parte integrante della

crescita personale, civica e culturale di bambini, docenti e famiglie.

I Piani di Azione dell'ePolicy rappresentano il percorso triennale che la scuola intende seguire per **diffondere la cultura della sicurezza digitale, dell'uso consapevole delle tecnologie e del rispetto in rete**, in coerenza con gli obiettivi del curriculum di educazione civica e con la **Legge 92/2019**.

Il piano tiene conto delle specificità dell'infanzia e della primaria, privilegiando metodologie esperienziali, cooperative e narrative, per favorire nei più piccoli un approccio sereno e positivo alle tecnologie.

1° Anno di attività con l'ePolicy

Modulo I - Diffusione e sensibilizzazione

- Presentazione ufficiale dell'ePolicy ai **docenti** dell'Istituto in occasione del Collegio e attraverso incontri dedicati di formazione interna.
- Presentazione dell'ePolicy a **famiglie e studenti** durante gli **Open Day** e nella **Giornata per la Sicurezza in Rete (SID)**, con materiali e linguaggi adeguati all'età dei bambini.
- Diffusione delle **versioni semplificate dell'ePolicy** (studenti/famiglie/docenti) tramite sito web, bacheche scolastiche e piattaforma digitale d'Istituto.

Modulo II - Analisi dei bisogni e sperimentazione didattica

- Rilevazione del **fabbisogno formativo dei docenti** sull'uso educativo del digitale e sulle competenze DigComp 2.2.
- Rilevazione di **interessi e bisogni delle famiglie** sull'educazione digitale in età evolutiva.
- Avvio di una **sperimentazione pilota del Kit Didattico "Generazioni Connesse"** in alcune sezioni e classi della scuola dell'infanzia e primaria.

Modulo III - Integrazione nei documenti dell'Istituto

- Aggiornamento del **Regolamento d'Istituto** e della **Politica d'Uso Accettabile (PUA)**, adattando il linguaggio ai contesti della scuola dell'infanzia e primaria.
- Inserimento di riferimenti espliciti all'ePolicy nel **Patto di Corresponsabilità educativa** e nel **PTOF**.

Modulo IV - Segnalazione e monitoraggio

- Definizione di **procedure di segnalazione accessibili ai minori**, attraverso linguaggi chiari, visuali e child-friendly.
- Creazione di un sistema di **raccolta e monitoraggio delle segnalazioni** legate a episodi di uso improprio della rete o dei dispositivi, con la supervisione del team ePolicy.

2° Anno di attività con l'ePolicy

Modulo I - Formazione e consolidamento

- Attivazione di **percorsi di formazione per docenti**, basati sui risultati del monitoraggio dell'anno precedente, anche attraverso il portale *Generazioni Connesse* o esperti esterni.
- Coinvolgimento di **almeno il 60% del personale docente** in percorsi di aggiornamento sull'educazione civica digitale, sicurezza online e intelligenza artificiale a scuola.

Modulo II - Attuazione educativa e partecipazione

- Utilizzo sistematico del **Kit Didattico** come risorsa metodologica per i percorsi di cittadinanza digitale.
- Attività rivolte a **bambini e bambine**, calibrate sull'età, per favorire il pensiero critico, la collaborazione online e la consapevolezza digitale (giochi cooperativi, storytelling digitale, attività con BeeBot e Scratch Jr).
- Percorsi informativi per le **famiglie**, con focus su sicurezza, uso consapevole del tempo online e strumenti digitali educativi.
- Rilevazione annuale di **interessi, abitudini e comportamenti digitali** nella comunità scolastica per valutare l'impatto delle azioni.

3° Anno di attività con l'ePolicy

- **Revisione e aggiornamento** dell'ePolicy sulla base dei dati di monitoraggio e delle nuove indicazioni ministeriali.
- Inserimento di azioni specifiche sull'uso dell'**Intelligenza Artificiale nella didattica**, in coerenza con le **Linee guida** per l'introduzione dell'Intelligenza Artificiale nelle istituzioni scolastiche, allegate al **DM 166/2025**, pubblicate dal MIM, che forniscono un quadro di riferimento strutturato per l'adozione consapevole e responsabile della IA a scuola, favorendo un approccio etico e critico anche nei più piccoli.
https://www.mim.gov.it/documents/20182/0/MIM_Linee+guida+IA+nella+Scuola_09_08_2025-signed.pdf/b70fdc45-4b75-1f7e-73bf-eab12989b928?t=1756468797694
-
- Consolidamento delle **reti territoriali** con enti pubblici, forze dell'ordine e associazioni del terzo settore per una cittadinanza digitale condivisa.
- Pubblicazione di un **report triennale di valutazione** delle azioni svolte e pianificazione del successivo ciclo di aggiornamento.

Conclusione

I Piani di Azione della *Direzione Didattica "Don Bosco"* mirano a creare una **comunità educante digitale** consapevole, collaborativa e protettiva, dove bambini, docenti e famiglie imparano a usare la tecnologia come strumento di crescita, creatività e partecipazione responsabile.

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](#)

La Direzione Didattica *"Don Bosco"* utilizza le risorse del progetto **Generazioni Connesse** come strumenti didattici, formativi e di supporto per promuovere la cittadinanza digitale e un uso consapevole e sicuro delle tecnologie, sia in classe sia a casa.

Le principali risorse disponibili sono:

- **Kit Didattico:** materiale modulare e adattabile alle diverse età, con schede operative, giochi, laboratori e attività digitali pensati per bambini e bambine della scuola dell'infanzia e primaria. Consente di affrontare temi come sicurezza online, privacy, cyberbullismo e utilizzo creativo della tecnologia.
- **Area Formazione online:** percorsi dedicati a **docenti, famiglie e studenti**, con contenuti su educazione digitale, sicurezza in rete, cittadinanza digitale e strumenti didattici da utilizzare a scuola o a casa.
- **Canale YouTube:** video-stimolo, tutorial e webinar per insegnanti, studenti e famiglie, con spiegazioni semplici e attività pratiche.
- **Canali Social (TikTok, Instagram, Facebook):** contenuti brevi e accessibili, pensati per stimolare curiosità, creatività e consapevolezza digitale, con messaggi chiari per i più piccoli e indicazioni per le famiglie.

La scuola integra queste risorse nei percorsi curricolari, nei laboratori e nelle attività di sensibilizzazione rivolte a bambini, docenti e genitori, favorendo **un approccio attivo, esperienziale e partecipativo**.

Le risorse di Generazioni Connesse diventano così strumenti concreti per:

- Educare all'uso sicuro di internet e dei dispositivi digitali.
- Stimolare la creatività digitale e il pensiero critico.
- Promuovere comportamenti responsabili e collaborativi in rete.

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.

La Direzione Didattica "Don Bosco" promuove la **consapevolezza digitale** come parte integrante del percorso educativo, coinvolgendo **docenti, alunni e famiglie** in attività di informazione, prevenzione e formazione.

L'obiettivo principale è educare i bambini e le bambine a **un uso sicuro, rispettoso e positivo delle tecnologie digitali e di internet**, fin dai primi anni della scuola dell'infanzia e primaria.

Le azioni principali sono:

- **Attività formative in classe:** laboratori digitali, giochi educativi e attività pratiche che stimolano la conoscenza dei rischi e delle opportunità della rete. Le attività sono progettate per essere **divertenti, semplici e interattive**, adatte all'età dei bambini.
- **Coinvolgimento dei genitori:** incontri, colloqui e materiali informativi per condividere strategie di prevenzione, regole di sicurezza online e strumenti per accompagnare i figli nell'uso della tecnologia a casa.
- **Formazione docenti:** La scuola per favorire una più adeguata formazione si avvale di piattaforme ministeriali quali: **Piattaforma Elisa - Generazioni Connesse - OnLife Pass - Programma il Futuro** che promuovono corsi e workshop su sicurezza digitale, cittadinanza digitale, cyberbullismo e strumenti didattici digitali.
- **Percorsi di cittadinanza digitale:** percorsi curricolari integrati nel PTOF e nelle attività di educazione alla cittadinanza, che sviluppino la conoscenza dei diritti in rete, il rispetto degli altri utenti, la gestione dei dati personali e delle informazioni, e la capacità di distinguere contenuti sicuri da quelli rischiosi.
- **Kit didattico e risorse digitali:** utilizzo del materiale a disposizione nelle varie piattaforme ministeriali e non per stimolare il pensiero critico, la consapevolezza digitale e la partecipazione attiva, con schede operative, giochi e attività collaborative.

La scuola ritiene fondamentale che ogni componente della comunità educante sviluppi **competenze digitali consapevoli**, promuovendo comportamenti responsabili e prevenendo situazioni di rischio online. Le azioni sono sempre adattate all'età e alla maturità dei bambini e delle bambine, nel rispetto della loro curiosità e sicurezza.

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 curriculum di educazione alla Cittadinanza Digitale previsto dalla L. 92/2019. Il curriculum prende forma attorno all'ePolicy e le attività didattiche sono legate al documento ed alle scelte dell'Istituto al suo interno.

Nel curriculum 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.

La Direzione Didattica "Don Bosco" integra le competenze digitali nel **curricolo scolastico**, adattando le linee guida europee del **DigComp 2.2** all'età dei bambini e delle bambine.

Il curriculum digitale ha l'obiettivo di:

- **Educare alla cittadinanza digitale:** far conoscere ai bambini e alle bambine i diritti e i doveri in rete, sviluppando comportamenti sicuri e rispettosi;
- **Favorire la consapevolezza digitale:** stimolare la capacità di riconoscere contenuti appropriati, proteggere i propri dati personali e utilizzare la tecnologia in maniera positiva;
- **Coinvolgere le famiglie:** informare e supportare i genitori attraverso materiali dedicati, incontri e momenti di formazione per promuovere comportamenti responsabili a casa;
- **Sostenere i docenti:** offrire strumenti, risorse e kit didattici per facilitare l'educazione digitale nelle attività quotidiane, con laboratori, giochi educativi e attività pratiche.

In ogni classe viene previsto almeno **un momento didattico specifico** dedicato alla cittadinanza digitale e all'uso consapevole degli strumenti tecnologici, calibrato secondo l'età dei bambini e delle bambine.

Le **attività di prevenzione e sensibilizzazione**, presenti nell'ePolicy, sono parte integrante delle programmazioni scolastiche e costituiscono un filo conduttore che accompagna i bambini nella crescita, aiutandoli a vivere il mondo digitale in modo sicuro e positivo.

L'uso dei **kit didattici** e delle risorse digitali disponibili attraverso Generazioni Connesse permette di collegare le attività di classe con i progetti di educazione alla cittadinanza digitale, promuovendo la partecipazione attiva di tutti gli alunni e alunne.

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.

Alla Direzione Didattica "Don Bosco", il **Kit Didattico** rappresenta uno strumento fondamentale per portare in classe la cultura della sicurezza digitale in modo **pratico, coinvolgente e accessibile**.

Il Kit è pensato per essere utilizzato dai **docenti** come supporto alle lezioni di cittadinanza digitale e consente di lavorare su temi come:

- la **sicurezza in rete** e la tutela dei propri dati personali;
- l'**etica digitale**, il rispetto reciproco e le regole di buona convivenza online;
- l'**uso consapevole dei dispositivi tecnologici**, adattato all'età degli alunni e delle alunne;
- l'**approccio critico ai contenuti digitali**, imparando a distinguere informazioni affidabili da quelle potenzialmente pericolose;
- la **protezione dei minori online**, con materiali sviluppati in collaborazione con enti come **UNICEF, Save the Children, Telefono Azzurro** e altre organizzazioni attive nella tutela dei bambini.

Il Kit contiene materiali diversificati: attività ludiche, schede operative, presentazioni, video e guide per i docenti. Può essere utilizzato nella **sua interezza o selezionando le risorse più adatte** alla classe e all'età dei bambini, favorendo così un apprendimento graduale e personalizzato.

Per i **docenti della scuola dell'infanzia**, il Kit offre proposte di attività basate sul gioco e sulla narrazione, mentre nella **primaria** consente laboratori pratici, esperimenti guidati e momenti di riflessione condivisa.

Grazie al Kit Didattico, ogni lezione diventa un'opportunità per sviluppare la **consapevolezza digitale**, promuovere comportamenti sicuri e responsabili nella vita online e coinvolgere **famiglie e comunità scolastica** nella costruzione di un ambiente digitale protetto e positivo.

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.

Alla Direzione Didattica *Don Bosco*, la protezione dei dati personali di studenti, famiglie e personale scolastico è una priorità fondamentale. Ogni membro della comunità scolastica ha il diritto di sapere che le informazioni che lo riguardano sono trattate in modo sicuro e nel rispetto della normativa vigente.

Cosa significa proteggere i dati personali

Per dati personali si intendono tutte le informazioni che permettono di identificare una persona, come:

- nome e cognome;
- dati di contatto (telefono, email);
- immagini e video realizzati durante attività scolastiche;
- informazioni scolastiche e didattiche (valutazioni, partecipazione a laboratori, attività extracurricolari).

La scuola si impegna a trattare questi dati solo per **finalità legate all'educazione, alla sicurezza e alla gestione scolastica**, secondo quanto previsto dal **Regolamento Europeo 2016/679 (GDPR)** e dal **Codice Privacy (Dlgs 196/2003)**.

Responsabile della protezione dei dati (RPD o DPO)

Per garantire la corretta gestione dei dati, la scuola ha nominato un **Responsabile della Protezione dei Dati (RPD o DPO)**, che ha il compito di:

- fornire consulenza e supporto su tutte le questioni legate alla privacy;
- supervisionare l'applicazione delle regole interne sulla gestione dei dati;
- controllare che tutti i processi rispettino il GDPR;
- ricevere segnalazioni da parte di genitori, docenti o studenti riguardanti il trattamento dei dati.

Organizzazione e strumenti

La scuola ha predisposto procedure e strumenti chiari per la protezione dei dati:

- **Organigramma privacy**, che identifica chi gestisce i dati e per quali finalità;
- **Informativa sulla privacy**, consegnata a famiglie e personale al momento della raccolta dei dati;
- **Registro dei trattamenti**, che documenta in modo trasparente come e perché i dati vengono utilizzati;
- **Controlli e monitoraggio periodici**, per garantire la sicurezza dei dati sui dispositivi scolastici e nelle piattaforme digitali.

Impegno della comunità scolastica

Tutti i membri della scuola – docenti, famiglie, studenti – sono invitati a collaborare rispettando le regole sulla privacy:

- condividendo dati personali solo se necessario e con consapevolezza;
- utilizzando in modo corretto piattaforme digitali e strumenti ICT forniti dalla scuola;
- segnalando eventuali anomalie o dubbi al RPD o al Dirigente Scolastico.

La protezione dei dati personali non è solo un obbligo normativo: è un elemento essenziale per garantire **fiducia, sicurezza e un ambiente digitale positivo** per bambini e bambine della scuola dell'infanzia e primaria.

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.

Alla Direzione Didattica *Don Bosco*, l'uso della rete e degli strumenti digitali è un'opportunità educativa importante, ma richiede regole chiare per garantire sicurezza e responsabilità. Per questo motivo la scuola ha adottato la **Politica d'Uso Accettabile e Responsabile della Rete (PUA)**, un documento che stabilisce modalità corrette e sicure di utilizzo di internet, piattaforme digitali e dispositivi scolastici.

Cosa prevede la PUA

La PUA si rivolge a tutti i membri della comunità scolastica:

- studenti e studentesse della scuola dell'infanzia e primaria;
- docenti e personale scolastico;
- professionisti esterni che collaborano con la scuola.

Il documento definisce **regole di comportamento e responsabilità** per garantire un uso sicuro, educativo e rispettoso della rete e dei dispositivi digitali. Tra i principali punti:

- usare internet e le piattaforme digitali solo per finalità didattiche o educative;
- non cercare o diffondere contenuti inappropriati, violenti o non adatti all'età;
- rispettare la privacy e i dati personali di tutti, evitando di condividere informazioni sensibili senza autorizzazione;
- non violare diritti d'autore o proprietà intellettuale di materiali online;
- utilizzare i dispositivi scolastici (tablet, LIM, PC) solo secondo le indicazioni dei docenti;
- evitare giochi o azioni che possano compromettere la sicurezza della rete scolastica;

- segnalare subito eventuali contenuti sospetti o comportamenti scorretti osservati online.

Perché è importante la PUA

La PUA serve a costruire **un ambiente digitale sicuro e positivo**, dove bambini e bambine possono esplorare la tecnologia e imparare in modo consapevole. Aiuta anche docenti e famiglie a conoscere i rischi della rete e a collaborare nella prevenzione di episodi di cyberbullismo, sexting o comportamenti a rischio online.

Ruolo di tutti gli attori

- **Studenti e studentesse:** seguono le regole della PUA, imparano a proteggersi online e a rispettare i compagni;
- **Docenti:** guidano l'uso corretto degli strumenti digitali, monitorano comportamenti a rischio e intervengono in caso di necessità;
- **Famiglie:** supportano i figli nell'uso consapevole della rete, dialogano con i docenti e segnalano eventuali criticità;
- **Personale scolastico e professionisti esterni:** rispettano le stesse regole e collaborano alla sicurezza digitale dell'Istituto.

La PUA è integrata con il **Documento Programmatico sulla Sicurezza (DPS)** e con il regolamento d'Istituto, e rappresenta uno strumento operativo concreto per promuovere **un uso positivo e responsabile delle tecnologie digitali**, in linea con l'ePolicy della scuola.

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.

Alla Direzione Didattica *Don Bosco*, per motivi di sicurezza, tutela dei minori e uniformità didattica, **non è consentito l'uso di dispositivi personali (BYOD)** da parte di bambini e bambine della scuola dell'infanzia e primaria.

Obiettivi della regolamentazione

Questa scelta ha lo scopo di:

- garantire la sicurezza dei bambini e delle bambine durante le attività digitali;

- permettere un controllo completo sui contenuti e sugli strumenti utilizzati;
- promuovere un approccio condiviso e guidato dall'insegnante all'uso delle tecnologie;
- evitare rischi legati a privacy, malware, contenuti inappropriati e disuguaglianze tra alunni.

Uso dei dispositivi in classe

- Tutte le attività digitali vengono svolte **solo con i dispositivi forniti dalla scuola**, sotto la supervisione dei docenti;
- L'uso dei dispositivi è sempre **guidato e monitorato** dai docenti, che scelgono le applicazioni e i contenuti più adeguati all'età dei bambini;
- Gli studenti non devono portare dispositivi personali (tablet, smartphone, notebook) a scuola, se non espressamente autorizzati per specifici progetti didattici concordati con la Dirigenza.

Ruolo dei docenti e delle famiglie

- I docenti guidano e supportano l'uso responsabile dei dispositivi digitali forniti dalla scuola;
- I genitori sono invitati a sostenere l'educazione digitale dei figli a casa, promuovendo comportamenti sicuri e consapevoli;
- Eventuali attività digitali a casa devono essere concordate con i docenti e svolte sotto la supervisione dei genitori.

Conclusioni

Questa regolamentazione garantisce che l'uso della tecnologia a scuola sia **sicuro, equo e educativo**, in linea con il PTOF, l'ePolicy e il regolamento d'Istituto, proteggendo i bambini e le bambine dai rischi online e promuovendo un approccio guidato e consapevole all'uso delle tecnologie digitali.

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/le studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).

Adescamento online: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona 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.

Alla Direzione Didattica *Don Bosco*, la sicurezza dei bambini e delle bambine in rete è una priorità. Questo capitolo indica **cosa segnalare** e come farlo, affinché la scuola possa intervenire in modo tempestivo e adeguato.

1. Cosa segnalare

Le segnalazioni riguardano comportamenti online o situazioni che mettono a rischio il benessere dei bambini, ad esempio:

- **Cyberbullismo:** insulti, esclusioni o prese in giro online tra alunni/e. È importante valutare se il comportamento è ripetuto, intenzionale e se causa disagio alla vittima.
- **Adescamento online:** messaggi o contatti da parte di persone sconosciute che tentano di instaurare rapporti con i bambini. Non cancellare prove e non rispondere al posto del bambino.
- **Diffusione non autorizzata di immagini o video (sexting):** se foto o video dei bambini vengono condivisi senza consenso, l'obiettivo è proteggere il minore e bloccare la diffusione del materiale.

2. Come segnalare

- Le segnalazioni devono essere rivolte **al Dirigente Scolastico**, al **Referente per il bullismo e cyberbullismo** o al **team interno preposto**.
- La comunicazione deve essere **chiara, dettagliata e scritta**, indicando ciò che è successo senza modificare o cancellare eventuali prove.
- La scuola valuterà la gravità del caso e attiverà i percorsi adeguati, anche coinvolgendo **esperti esterni** se necessario.

3. Coinvolgimento della comunità

- I docenti osservano comportamenti a rischio e informano tempestivamente la scuola.
- I genitori possono segnalare preoccupazioni legate all'uso della rete dei loro figli.
- Tutte le segnalazioni sono gestite con **riservatezza** e nell'interesse del benessere dei bambini.

4. Risorse e supporto

In caso di emergenza o per assistenza:

- **Helpline 19696 e Chat di Telefono Azzurro**
- **Clicca e Segnala di Telefono Azzurro**
- **STOP-IT di Save the Children Italia**

Questi servizi aiutano a tutelare i minori, rimuovere contenuti inappropriati e fornire supporto psicologico.

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 minorenni.

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

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

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

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

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

Gli insegnanti e i genitori, come studenti e studentesse, si possono rivolgere alla Helpline del progetto Generazioni Connesse, al numero gratuito 19696, attraverso la chat disponibile sul [sito](#) o tramite chat WhatsApp per ricevere supporto e consulenza. Per tutti i dettagli, il riferimento è agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

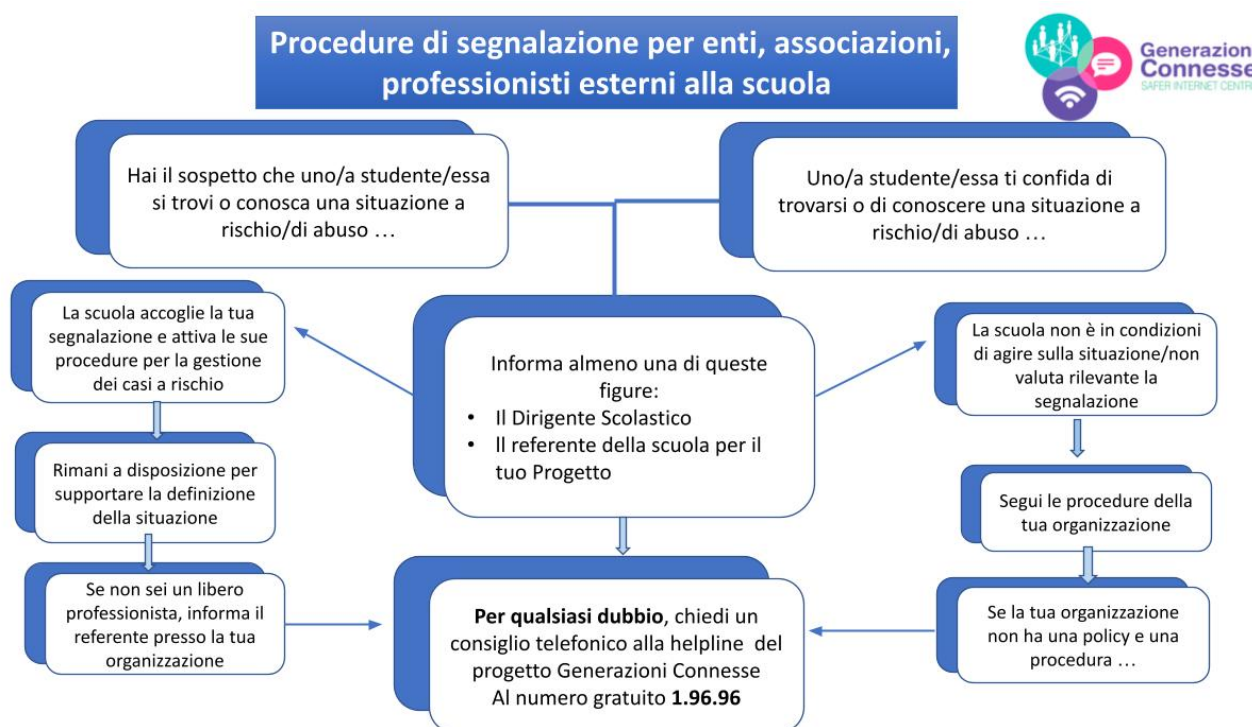
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

visibile della scuola; sportello di ascolto con professionisti; docente referente per le segnalazioni.

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

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

Procedure



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo



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

Se non è già stato fatto, avvisa il referente per il cyberbullismo (e/o il team antibullismo) che attiva le procedure ("Corso 4" della piattaforma ELISA) e il Dirigente Scolastico.

Ricordare sempre che in base alla legge 71-2017:

A) Se c'è fattispecie di reato va fatta la segnalazione alle forze dell'ordine

B) Se non c'è fattispecie di reato.

Il DS (e/o il team antibullismo):

- informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto) su quanto accade e condivide 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.

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

NELLE CLASSI

Il team antibullismo collabora coi docenti della classe per realizzare l'intervento nella classe:

a seconda della situazione valuta se

- affrontare direttamente l'accaduto o
- sensibilizzare la classe (vedi Corso 4 Piattaforma Elisa)
- trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.

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



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

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.

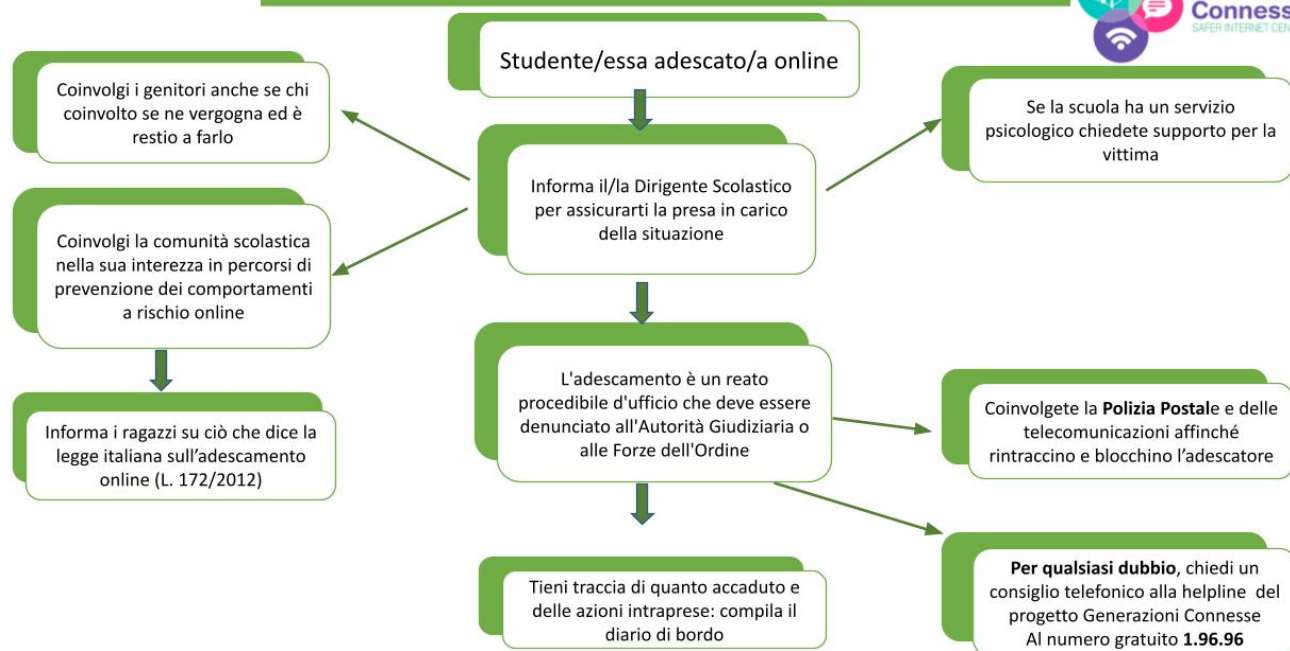
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

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

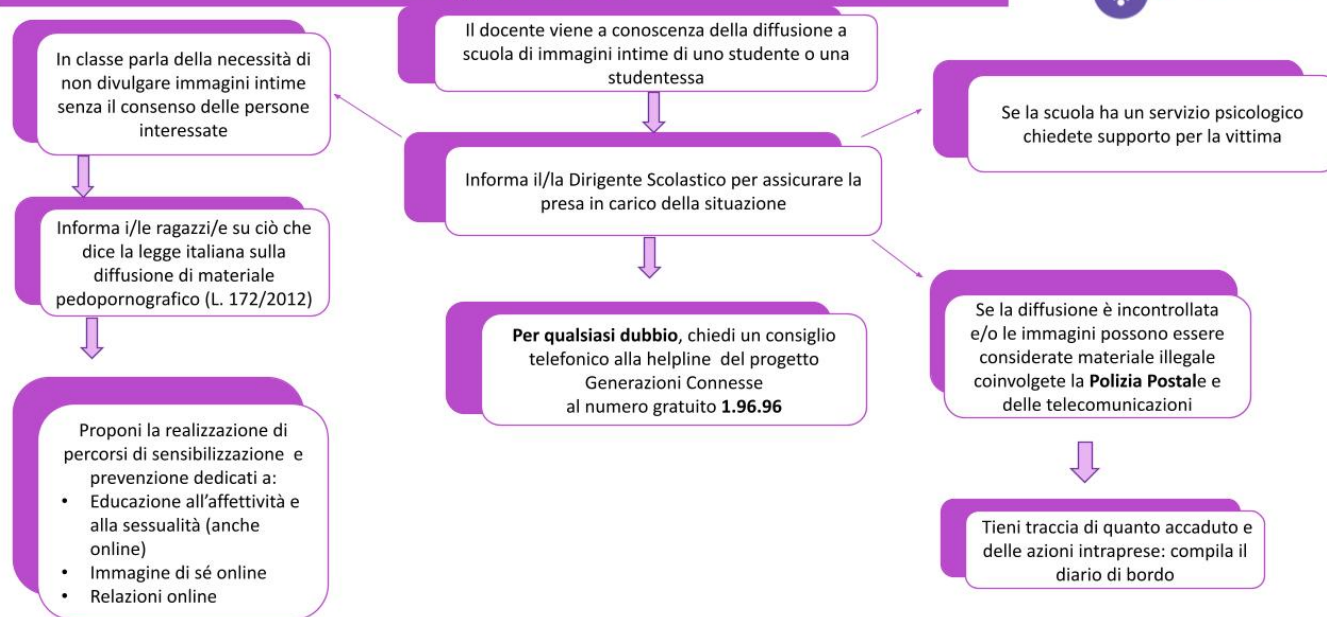
Se emergono evidenze passa allo schema successivo

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

Procedure interne: cosa fare in caso di Adescamento Online?



Procedure interne: cosa fare in caso di diffusione non consensuale di immagini intime?



Alla Direzione Didattica *Don Bosco* tutti i docenti, in quanto **pubblici ufficiali**, hanno la responsabilità di tutelare i bambini e le bambine anche nell'uso della rete e delle tecnologie digitali.

1. Chi interviene

In caso di situazioni problematiche online o comportamenti a rischio, interviene un **team di docenti dedicato** composto da:

- Il **Dirigente Scolastico**
- Il **docente referente ePolicy**
- L'**Animatore Digitale**
- Il **Referente bullismo e cyberbullismo**
- Altri docenti coinvolti in attività di educazione civica e digitale

Se necessario, la scuola può coinvolgere **esperti esterni** per supporto psicologico o educativo.

2. Tipologie di segnalazione

CASO A - SOSPETTO

Quando il docente ha il sospetto che stia accadendo un episodio di bullismo o cyberbullismo tra bambini, la segnalazione deve essere:

- Rivolta al **Referente e al team antibullismo**, con allertamento del Dirigente.
- Scritta, dettagliata e oggettiva.
- Utilizzata per valutare se attivare percorsi di sensibilizzazione o interventi educativi.

CASO B - EVIDENZA

Quando il docente ha evidenza certa di un episodio:

- La segnalazione va al **Referente e al team antibullismo**, con allertamento del Dirigente.
- Il team valuta i fatti, coinvolge esperti se necessario e, se rilevante penalmente, attiva le **procedure con l'autorità giudiziaria** (Procura Minorile o ordinaria a seconda dei casi).

Nota: In nessun caso l'insegnante deve sostituirsi alle autorità competenti; il suo ruolo è **osservazione, segnalazione e tutela dei minori**.

3. Ruolo dei genitori

I genitori possono e devono segnalare episodi sospetti o evidenti:

- Al Dirigente Scolastico
- Al docente coordinatore o referente ePolicy
- Al team antibullismo tramite le procedure interne

La collaborazione tra scuola e famiglia è fondamentale per la protezione dei bambini.

4. Strumenti a disposizione

Per permettere ai bambini di segnalare eventuali situazioni problematiche:

- **Indirizzo e-mail dedicato** alle segnalazioni
- **Box per segnalazioni anonime** in spazi visibili della scuola
- **Sportello di ascolto** con docenti referenti o professionisti
- **Colloqui individuali** con docenti e referenti

Questi strumenti servono anche per monitorare i fenomeni, attivare percorsi educativi, giornate di sensibilizzazione e progetti di **peer education**.

5. Supporto esterno

In caso di necessità, docenti, genitori o studenti possono rivolgersi a:

- **Helpline Generazioni Connesse - 19696**
- **Chat online del progetto Generazioni Connesse**

Questi strumenti forniscono supporto e consulenza su episodi di bullismo, cyberbullismo o altri rischi online.