



Documento di ePolicy

I.C. PARMIGIANINO

PIAZZALE RONDANI1 - 43125 - PARMA
Parma (PR) - Emilia-Romagna
Data di approvazione: 22/06/2026 - 09:04

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.

Il documento di e-Policy non rappresenta un protocollo isolato, integrandosi con il Piano Triennale dell'Offerta Formativa (PTOF) e con il Regolamento di Istituto, rafforza il Patto Educativo di Corresponsabilità tra scuola e famiglia. L'obiettivo è creare un ambiente digitale sicuro e inclusivo, dove la tecnologia supporti l'innovazione didattica e il benessere relazionale, limitando i rischi di isolamento e l'esposizione a contenuti inappropriati.

L'adozione di questo documento coinvolge tutta la comunità educante — docenti, personale ATA, genitori e studenti — nella condivisione di una cittadinanza digitale fondata sul rispetto reciproco, sulla tutela della privacy e sulla responsabilità anche negli ambienti virtuali.

Azioni da realizzare entro l'anno scolastico

Le attività previste riguardano l'adozione dell'ePolicy e il suo raccordo con la normativa vigente:

- **Allineamento normativo:** verifica della coerenza dell'ePolicy con i regolamenti d'istituto e aggiornamento del Regolamento di Istituto e del PTOF in un'ottica di cittadinanza digitale.
- **Formazione docenti, genitori, studenti, personale ATA:** promozione della partecipazione ai percorsi formativi della piattaforma "Generazioni Connesse".
- **Aggiornamento del Patto educativo:** condivisione con le famiglie delle disposizioni relative all'uso consapevole delle tecnologie e alla tutela della privacy.
- **Informazione alla comunità scolastica:** diffusione di una circolare esplicativa rivolta a docenti, personale ATA e famiglie per presentare finalità e impegni dell'ePolicy.
- **Monitoraggio iniziale:** definizione di procedure per la raccolta di feedback e l'individuazione di eventuali criticità legate all'uso delle tecnologie.

Azioni da realizzare nel triennio

Il piano è finalizzato a rafforzare la cultura della cittadinanza digitale responsabile e dell'inclusione tecnologica.

Primo anno - Attivazione formazione e sensibilizzazione

- Attivazione di percorsi formativi per docenti e personale ATA sui temi del benessere digitale, della sicurezza online e della prevenzione dei rischi connessi all'uso delle tecnologie (*già in atto*).
- Inserimento nel curriculum di attività dedicate alla cittadinanza digitale, al rispetto reciproco e all'uso consapevole degli ambienti virtuali (*già in atto*).

Secondo anno - Consolidamento formazione

- Promozione di progetti di didattica innovativa che valorizzino la tecnologia come strumento di inclusione e

partecipazione.

Terzo anno - Valutazione e aggiornamento

- Monitoraggio dell'efficacia dell'ePolicy e revisione del documento in relazione all'evoluzione delle tecnologie digitali.
- Somministrazione di questionari a studenti e famiglie per valutare il livello di benessere digitale e l'impatto delle azioni realizzate.

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.

La piena efficacia dell'ePolicy dipende dalla collaborazione attiva e continuativa di tutte le componenti della comunità scolastica. Dirigenza, docenti, personale scolastico, studenti e famiglie condividono la responsabilità di promuovere un ambiente digitale sicuro, inclusivo e rispettoso, contribuendo ciascuno, secondo il proprio ruolo, alla prevenzione dei rischi e alla diffusione di comportamenti consapevoli nell'uso delle tecnologie.

Cronoprogramma delle azioni

Primo anno - Formazione e avvio

- Consolidamento di un gruppo di lavoro per l'aggiornamento e il monitoraggio dei documenti ePolicy (in base alle necessità rilevate dai questionari e alle nuove normative) e per la promozione di attività di formazione e sensibilizzazione sull'uso sicuro, consapevole e responsabile delle tecnologie digitali
- Formazione del personale su privacy, sicurezza online, riconoscimento dei segnali di disagio e procedure di segnalazione (*già in atto*).

Il corpo docente ha partecipato nel tempo a percorsi di formazione nell'ambito del Piano Nazionale per la Scuola Digitale (PNSD), promossi dall'USR Emilia-Romagna attraverso il Servizio Marconi TSI, nonché a iniziative formative organizzate dall'Ambito 4 USR ER, dalla piattaforma SOFIA e da programmi ministeriali dedicati (PON, ELISA, DM 66/2024).

Grazie alla partecipazione continuativa a tali percorsi, la maggior parte dei docenti di ruolo possiede una solida base di competenze digitali e metodologiche per l'integrazione delle tecnologie nella didattica.

- Avvio delle attività didattiche e utilizzo sistematico dei materiali di "Generazioni Connesse".

Secondo anno - Consolidamento e partecipazione

- Rafforzamento del coinvolgimento delle famiglie e di tutta la comunità scolastica attraverso incontri e laboratori tematici.

Terzo anno - Valutazione e revisione

- Realizzazione di una nuova autovalutazione d'istituto.
- Analisi dei risultati raggiunti e revisione dell'ePolicy in un'ottica di miglioramento continuo.

Tutti i soggetti esterni che operano nell'Istituto sono tenuti a rispettare il Regolamento d'Istituto e le disposizioni relative all'utilizzo dei dispositivi personali e delle dotazioni tecnologiche scolastiche.

L'uso dei dispositivi deve avvenire esclusivamente per finalità coerenti con il contesto educativo, evitando comportamenti impropri o non conformi durante le attività con studenti e studentesse.

È inoltre obbligatorio rispettare la normativa in materia di privacy e protezione dei dati personali, con particolare attenzione ai minori. Non è consentita la diffusione o condivisione non autorizzata di immagini, video, registrazioni o contatti personali.

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.

Azioni da svolgere entro un'annualità scolastica

- **Aggiornamento del Regolamento d'Istituto** con l'inserimento di riferimenti alle infrazioni digitali e ai comportamenti online.
- **Integrazione del Patto Educativo di Corresponsabilità** con un'appendice dedicata all'uso sicuro della rete e alla corresponsabilità educativa delle famiglie.
- **Definizione e diffusione dei protocolli di accesso** alle risorse digitali, con indicazione di modalità d'uso, limiti e responsabilità.
- **Inserimento dell'ePolicy nel PTOF** come riferimento per le attività di Educazione Civica Digitale.

Azioni da svolgere nel triennio

Primo anno - Formazione e organizzazione

- Formazione dei docenti sulla gestione dei comportamenti online e sulle misure educative e riparative.
- Verifica dell'efficacia dei protocolli di accesso ai laboratori e dei sistemi di filtraggio della rete.

Secondo anno - Monitoraggio e partecipazione

- Aggiornamento del Piano per la Didattica Digitale Integrata in coerenza con l'ePolicy.
- Organizzazione di incontri e workshop per le famiglie e tutta la comunità scolastica sul tema della corresponsabilità

educativa digitale.

Terzo anno - Valutazione e revisione

- Verifica dell'applicazione delle procedure e dei regolamenti aggiornati.
- Revisione dell'ePolicy sulla base delle nuove indicazioni normative e delle innovazioni tecnologiche.

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.

Diffusione e attuazione dell'ePolicy

L'Istituto promuove la diffusione e l'applicazione dell'ePolicy coinvolgendo attivamente personale scolastico, studenti e famiglie.

Azioni di diffusione

- Pubblicazione dell'ePolicy sul sito istituzionale.
- Approvazione del documento da parte del Collegio dei Docenti e del Consiglio d'Istituto.
- Inserimento dell'ePolicy nel PTOF.
- Presentazione del documento alle famiglie durante le assemblee di classe.
- Sottoscrizione del Patto Educativo di Corresponsabilità integrato con l'ePolicy.
- Affissione di una versione semplificata nei laboratori e negli spazi comuni.
- Predisposizione di una versione "child friendly" per gli studenti.

Informazione agli studenti

Gli studenti vengono informati che:

- l'utilizzo di Internet e dei dispositivi digitali è soggetto a supervisione da parte dei docenti;
- l'accesso alla rete deve essere autorizzato secondo le procedure previste;
- le regole per la sicurezza online sono disponibili in aule e laboratori;
- ogni utente è responsabile dell'uso dei dispositivi e del rispetto delle norme d'Istituto.

Azioni educative

- Percorsi e momenti di confronto sull'uso consapevole delle tecnologie digitali.
- Attività di sensibilizzazione sui rischi della rete e sulla prevenzione del cyberbullismo.
- Utilizzo di materiali e metodologie adeguati all'età degli alunni.

Formazione del personale

- Uso sicuro e responsabile delle tecnologie digitali.
- Tutela della privacy e trattamento dei dati personali (GDPR).
- Prevenzione e gestione dei rischi online.

Monitoraggio

- Il Team Antibullismo e dell'Emergenza cura la redazione e l'aggiornamento dell'ePolicy.
- Il team per l'innovazione supervisiona gli aspetti tecnici e il monitoraggio delle risorse digitali.

Gestione delle infrazioni alla ePolicy

La scuola gestisce le violazioni della ePolicy attraverso interventi educativi e, ove necessario, mediante provvedimenti disciplinari, nel rispetto del principio di proporzionalità e in relazione alla gravità dei comportamenti rilevati.

Infrazioni da parte degli studenti

Costituiscono infrazione:

- la diffusione online di immagini o video di compagni senza consenso o con contenuti offensivi, denigratori o lesivi della dignità personale;
- la condivisione non autorizzata di dati personali;

- la diffusione di messaggi offensivi, denigratori o finalizzati all'esclusione;
- l'invio o la condivisione di contenuti digitali finalizzati all'emarginazione o al danno relazionale.

In presenza di tali comportamenti saranno tempestivamente informati il Dirigente Scolastico e la famiglia dell'alunno.

In relazione alla gravità dell'infrazione potranno essere adottati i seguenti provvedimenti: richiamo verbale, nota disciplinare, sospensione dalle attività didattiche e, nei casi previsti, segnalazione alle autorità competenti.

Infrazioni da parte del personale

Qualora la violazione sia commessa da personale dipendente, saranno applicate le misure previste dalla normativa vigente e dai codici di comportamento del personale della Pubblica Amministrazione.

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

I piani di azione previsti dall'IC Parmigianino definiscono gli interventi previsti nel triennio per promuovere la conoscenza e l'applicazione dell'ePolicy. Eventuali violazioni delle regole saranno gestite attraverso misure educative e disciplinari proporzionate alla gravità dei comportamenti, nel rispetto del Regolamento d'Istituto e sotto il coordinamento del Dirigente Scolastico, in collaborazione con i Consigli di Classe e gli organi competenti.

Piano triennale delle attività ePolicy

1° Anno - Avvio

- Presentazione e diffusione dell'ePolicy.
- Rilevazione dei bisogni formativi di docenti e famiglie.
- Avvio delle attività didattiche e integrazione dell'ePolicy nei documenti d'Istituto.
- Definizione delle procedure di segnalazione.

2° Anno - Consolidamento

- Formazione di docenti, studenti e famiglie.
- Sviluppo dei percorsi di Educazione Civica Digitale.
- Monitoraggio delle abitudini digitali e dei bisogni formativi.

3° Anno - Valutazione e aggiornamento

- Verifica dell'efficacia delle azioni realizzate.
- Monitoraggio dell'applicazione dell'ePolicy.
- Revisione e aggiornamento del documento.

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](#)

L'ePolicy è oggetto di monitoraggio e aggiornamento periodico, in particolare in seguito a cambiamenti normativi, organizzativi o tecnologici. La revisione del documento è affidata al Team per l'epolicy e viene effettuata in raccordo con i processi di autovalutazione dell'Istituto. Il Regolamento d'Istituto e il Patto Educativo di Corresponsabilità sono periodicamente verificati e aggiornati in coerenza con le disposizioni e le Linee Guida ministeriali.

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.

L'utilizzo delle tecnologie digitali da parte di studenti, docenti e famiglie deve fondarsi su consapevolezza, responsabilità e uso critico degli strumenti e degli ambienti online. Per questo l'Istituto promuove percorsi di educazione digitale finalizzati a favorire comportamenti corretti e sicuri nella rete.

In tale prospettiva, l'Istituto attua azioni di prevenzione e contrasto al cyberbullismo con l'obiettivo di:

- promuovere un ambiente scolastico sicuro e inclusivo, anche negli spazi digitali;
- sviluppare competenze di cittadinanza digitale responsabile;
- prevenire comportamenti scorretti, offensivi o lesivi online;
- sostenere le vittime, responsabilizzare gli autori e favorire la cultura della segnalazione e dell'aiuto reciproco.

Le problematiche relative alle tematiche in oggetto, che si sono manifestate nell'Istituto, sono state prese in carico dal Dirigente, dai Referenti d'Istituto della Commissione bullismo e dai vari Consigli di Classe che hanno attivato momenti di confronto e dialogo con gli alunni coinvolti, insegnanti e genitori per ripristinare rapporti di condivisione e di benessere scolastico.

Ai sensi della Nota ministeriale n. 482 del 18/02/21 e della recente Legge 70 del 17/05/24 sono stati istituiti:

- Referenti d'Istituto della Commissione per la prevenzione e contrasto del bullismo e del cyberbullismo
- Protocollo d'intervento d'Istituto per gli episodi segnalati di bullismo e cyberbullismo (Il Collegio docenti con delibera n. 9 del 12/05/2023 e il Consiglio d'Istituto, con delibera n. 30 del 16/05/2023, hanno istituito e adottato il Protocollo d'intervento in caso di casi di bullismo e cyberbullismo)
- Team delle emergenze (elenco inserito nel documento Protocollo d'intervento d'Istituto)
- Cassetta delle segnalazioni: per messaggi di prima segnalazione;
- Attivazione di indirizzo di posta elettronica dedicato per inviare le prime segnalazioni - Email: prevenireeducareallrelazioni@icparmigianino.it

L'Istituto Comprensivo Parmigianino opera da alcuni anni attraverso il progetto **"Prevenire, educare alle relazioni"**, in relazione alle problematiche attuali del bullismo e del cyberbullismo sia in ottica preventiva che normativa. Di seguito le collaborazioni con istituzioni e associazioni esterne per la realizzazione di progetti nell'ottica della prevenzione e sensibilizzazione per il contrasto di tali fenomeni:

- Forze dell'Ordine: Polizia Postale, Polizia di Stato, Arma dei Carabinieri, Polizia Ferroviaria (Polfer Bologna) con il progetto *"Train to Be Cool"*, Prefettura di Parma;
- Avvocati della Camera Penale di Parma;
- Fondazione Carolina (Dott. Picchio);
- Fondazione Cornoni, con il coinvolgimento di artisti del teatro e della danza;
- Dott. Andrea Bilotto – A.I.C.S. (Associazione Italiana Prevenzione al Cyberbullismo e al Sexting), Presidente AICS e psicologo scolastico;
- Compagnia teatrale *Teatro del Cerchio*;
- Associazioni ed enti del territorio: Protezione Civile SEIRS, associazioni di volontariato, AUSL e altre realtà territoriali.

L'Istituto aderisce inoltre a iniziative e percorsi educativi quali:

- collaborazione e scambio culturale nell'ambito del progetto *"Bullismo e Cyberbullismo - Buone pratiche"* con il Collège Chantenay di Nantes (Francia);
- progetto *"Patente di Smartphone - Educare alla Cittadinanza Digitale"*;
- *Cinema in classe*: attività guidate con il supporto della piattaforma d'Istituto;
- collaborazione con lo scrittore Raffaele Capperi.

Istituzione di TAVOLO PERMANENTE E TEAM ANTIBULLISMO D'ISTITUTO

Componenti:

- Dirigente Scolastico (Presidente);
- Docenti collaboratori del Dirigente Scolastico;
- Docenti Referenti di plesso;
- Docenti Funzioni Strumentali per l'inclusione;
- Docenti referenti per il contrasto al bullismo e cyberbullismo;
- Docenti facenti parte del Team antibullismo e Emergenze;
- n. 2 Rappresentanti dei genitori nel Consiglio d'Istituto.

L'IC Parmigianino, inoltre, ha riproposto la propria candidatura all'ottenimento del finanziamento per il contrasto del fenomeno del cyberbullismo L.234/2021 - **"Click rete 3.0 3 scuole, una comunità educante, zero tolleranza al cyberbullismo"** (finanziamento già ottenuto nell'a.s. 2023/2024 dal titolo "Prevenire, educare alle relazioni") in collaborazione con due istituti comprensivi del territorio (IC Bocchi e IC Sorbolo) per l'edizione 2026.

È un progetto educativo integrato finalizzato alla prevenzione e al contrasto del bullismo e del cyberbullismo attraverso lo sviluppo di competenze civiche, digitali, relazionali ed emotive. Il progetto coinvolge studenti, docenti, famiglie e territorio in un'azione sistemica di promozione del benessere scolastico e della cittadinanza digitale responsabile. Le attività prevedono laboratori esperienziali, peer education, incontri con esperti della sicurezza digitale, forze dell'ordine, psicologi e associazioni del territorio. Gli studenti saranno protagonisti nella realizzazione di campagne di sensibilizzazione, podcast, performance artistiche, video e prodotti multimediali destinati alla comunità scolastica. Il progetto mira a creare una cultura del rispetto

on line e off line, favorendo comportamenti responsabili, inclusivi e consapevoli nell'utilizzo delle tecnologie digitali.

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.

Azioni di sensibilizzazione

Per gli studenti

- Percorsi educativi sull'uso consapevole e responsabile di Internet, dei social network e della messaggistica digitale.
- Attività di riflessione sul rispetto reciproco, l'empatia e le conseguenze dei comportamenti online.
- Partecipazione a iniziative e giornate dedicate alla sicurezza in rete e alla cittadinanza digitale.

Per i docenti

- Formazione sul riconoscimento precoce di situazioni di disagio e di rischio online.
- Aggiornamento sulle dinamiche del cyberbullismo e sugli strumenti digitali, anche attraverso i percorsi di Generazioni Connesse.
- Condivisione di strategie educative e procedure di intervento comuni.

Per le famiglie

- Incontri informativi sull'uso sicuro delle tecnologie digitali e sui principali rischi della rete.
- Supporto per una gestione consapevole dei dispositivi e degli ambienti digitali.
- Promozione del dialogo educativo tra genitori e figli sull'utilizzo delle tecnologie.

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.

Attività didattiche e prevenzione

L'Istituto prevede, all'interno del curriculum, attività dedicate alla cittadinanza digitale e alla sicurezza in rete, adeguate all'età degli alunni. Tali percorsi mirano a sviluppare una maggiore consapevolezza nell'uso delle tecnologie e dei dispositivi digitali.

Per supportare docenti e studenti vengono utilizzati i materiali e i kit didattici di Generazioni Connesse, che offrono risorse educative, attività laboratoriali e strumenti di approfondimento sui temi della sicurezza online, del benessere digitale e della cittadinanza responsabile. Le proposte possono essere adattate alle esigenze delle classi e personalizzate per favorire la partecipazione di tutti gli alunni.

Regolamento d'Istituto

- Definizione dei comportamenti non consentiti negli ambienti digitali.
- Individuazione delle relative misure educative e disciplinari.

Presenza educativa

- Promozione di un uso corretto e responsabile delle tecnologie digitali.
- Vigilanza e attenzione anche negli ambienti digitali collegati alle attività scolastiche, quali piattaforme didattiche e strumenti di comunicazione online.

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.

Tutela della privacy e trattamento dei dati

Le famiglie ricevono l'informativa sul trattamento dei dati personali e rilasciano le eventuali autorizzazioni previste per l'utilizzo di immagini, video e lavori degli alunni nell'ambito delle attività scolastiche.

Il personale scolastico è tenuto a rispettare le norme sulla privacy e non può acquisire o diffondere immagini, audio o video degli studenti tramite dispositivi personali o canali non istituzionali. Eventuali utilizzi a fini didattici sono consentiti esclusivamente previa autorizzazione della scuola e nel rispetto delle procedure previste.

L'Istituto garantisce il trattamento dei dati personali in conformità alla normativa vigente, adottando adeguate misure di sicurezza per la protezione delle informazioni.

Il trattamento dei dati personali riguarda unicamente le finalità istituzionali della scuola per le quali vengono raccolti solo i dati strettamente necessari. Essi saranno trattati con o senza l'ausilio di strumenti elettronici e comunque automatizzati secondo le modalità e le cautele previste dall'art. 13 del D.Lgs 196/2003 e ss.mm.ii., e conservati per il tempo necessario all'espletamento delle attività amministrative e istituzionali.

L'accesso al Registro Elettronico è riservato ai soggetti autorizzati mediante credenziali personali. I sistemi informatici dell'Istituto sono protetti attraverso procedure di autenticazione, gestione delle password e strumenti di sicurezza informatica.

L'accesso alla documentazione amministrativa è disciplinato dalla normativa vigente e consentito esclusivamente ai soggetti che dimostrino un interesse legittimo e qualificato.

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.

A seguito del confronto con il DPO dell'Istituto, si precisa che la "Politica di Uso Accettabile" (AUP) non costituisce un adempimento obbligatorio previsto dalla normativa vigente, ma uno strumento organizzativo che le istituzioni scolastiche possono adottare nell'ambito della propria autonomia.

L'Istituto ha pertanto scelto di disciplinare l'utilizzo delle risorse digitali e della rete attraverso i documenti regolamentari già in vigore, senza adottare uno specifico documento AUP.

L'Istituto Comprensivo Parmigianino di Parma dispone di accesso a Internet tramite rete cablata e rete Wi-Fi, disponibili in tutti i plessi delle scuole primarie e della scuola secondaria. I laboratori informatici utilizzano prevalentemente la connessione Wi-Fi per l'accesso alla rete.

L'utilizzo della rete interna ed esterna (Internet) è consentito esclusivamente per finalità didattiche e per lo svolgimento delle attività connesse alle esigenze degli uffici amministrativi.

L'Istituto promuove l'alfabetizzazione digitale e informatica, riconoscendo Internet come strumento di apprendimento, inclusione e accesso alle risorse educative.

I docenti vigilano sul corretto utilizzo della rete da parte degli studenti, accompagnandoli nelle attività online, definendo obiettivi chiari di ricerca e favorendo l'acquisizione di competenze nella selezione, gestione e utilizzo consapevole delle risorse digitali.

L'Istituto disciplina inoltre l'utilizzo dei laboratori informatici mediante specifiche norme finalizzate a garantire un uso corretto, responsabile e sicuro di Internet.

Gli studenti sono tenuti a:

1. utilizzare Internet esclusivamente per finalità didattiche;
2. non scaricare musica, video, applicazioni o software senza preventiva autorizzazione del docente;
3. non accedere ai social network o ad altri canali social durante le attività scolastiche;
4. non utilizzare giochi online o installati localmente;
5. salvare sempre i propri elaborati e file nelle cartelle personali, di classe o negli spazi cloud istituzionali (es. Google Drive), evitando il salvataggio sul desktop o nelle cartelle dei programmi utilizzati. Il personale incaricato della manutenzione potrà eliminare file salvati in posizioni non autorizzate al fine di garantire il corretto funzionamento

delle postazioni;

6. custodire con riservatezza le credenziali di accesso ai computer e agli account personali;
7. non inviare fotografie personali o di altri senza autorizzazione;
8. richiedere sempre il consenso del docente prima di scaricare documenti o materiali da Internet;
9. chiedere l'autorizzazione del docente prima di iscriversi a concorsi online o comunicare dati relativi alla scuola;
10. informare immediatamente il docente qualora ricevano immagini, contenuti o messaggi inappropriati od offensivi, evitando in ogni caso qualsiasi risposta;
11. segnalare tempestivamente al docente il reperimento accidentale di contenuti non adeguati durante la navigazione e riferire immediatamente qualunque richiesta di incontro proveniente da persone conosciute online, ricordando che gli utenti della rete potrebbero non corrispondere alla propria identità dichiarata. Prima di inviare comunicazioni elettroniche di classe è necessario rivolgersi al docente;
12. non caricare, copiare o distribuire materiale reperito online senza autorizzazione del docente o del responsabile di laboratorio;
13. non diffondere in rete dati personali propri o di altri, né informazioni organizzative o funzionali riferite all'Istituto.

Sanzioni

Il mancato rispetto delle presenti disposizioni comporterà l'applicazione delle sanzioni disciplinari previste dal Regolamento d'Istituto e potrà incidere negativamente sulla valutazione del comportamento e, ove pertinente, sul profitto nella disciplina interessata.

Comunicazione istituzionale e utilizzo degli strumenti digitali

L'Istituto Comprensivo Parmigianino di Parma ha adottato la piattaforma **Google Workspace for Education** per il personale ATA, per i docenti di tutti gli ordini di scuola e per gli alunni della scuola primaria e della scuola secondaria di primo grado.

Gli studenti sono tenuti a rispettare quanto previsto dal **Regolamento per l'utilizzo di Google Workspace for Education**, pubblicato e consultabile sul sito istituzionale della scuola.

La comunicazione istituzionale in modalità digitale avviene attraverso i seguenti canali ufficiali:

- la posta elettronica istituzionale (pric83600p@icparmigianino.it);
- il registro elettronico;
- il sito web dell'Istituto (<https://icparmigianino.edu.it/>), all'interno del quale è presente una sezione dedicata alle comunicazioni alle famiglie, costantemente aggiornata per garantire una tempestiva diffusione delle informazioni rivolte ai genitori.

L'Istituto non utilizza canali ufficiali di social network per le comunicazioni istituzionali.

La scuola promuove tuttavia lo sviluppo delle competenze digitali e della cittadinanza digitale attraverso attività educative e percorsi formativi dedicati all'utilizzo consapevole, corretto e sicuro degli strumenti digitali e dei social network, con particolare attenzione al rispetto della netiquette, alla tutela della privacy, alla sicurezza online e alla responsabilità nei comportamenti in rete.

Si è ritenuto di inserire nella presente ePolicy un paragrafo specificamente dedicato all'utilizzo dell'Intelligenza Artificiale a scuola, volto a promuoverne un uso consapevole e a definirne principi, ambiti di applicazione e responsabilità.

Intelligenza Artificiale Generativa a scuola

L'intelligenza artificiale generativa è una tecnologia sempre più diffusa che può costituire uno strumento didattico se utilizzata in modo critico, consapevole e trasparente. Le nuove Linee Guida ministeriali stabiliscono il modello di introduzione dell'IA basato su centralità della persona, equità e inclusione.

L'uso dell'IA generativa a scuola deve sempre avvenire con finalità didattiche, sotto la supervisione del docente, nel rispetto della normativa sulla protezione dei dati personali dei minori, in coerenza con le policy dei principali fornitori di servizi di IA e con la normativa italiana ed europea sulla protezione dei dati personali (GDPR), che vieta l'utilizzo di molti strumenti di IA sotto i 14 anni.

L'utilizzo di strumenti di IA generativa è consentito con il consenso di chi esercita la responsabilità genitoriale per trattamento dei dati personali legati all'IA, esclusivamente in modalità supervisionata dal docente (per la primaria) e solo con autorizzazione esplicita del docente (per la secondaria), attraverso piattaforme didattiche certificate e conformi ai limiti di età previsti dalla normativa. In questo contesto, la scuola agisce come "deployer" e si assume la responsabilità di scegliere strumenti conformi.

Norme comportamentali

Gli studenti e le studentesse:

- utilizzano strumenti di IA generativa solo per finalità didattiche e dopo esplicita autorizzazione del docente;
- non utilizzano l'IA per sostituirsi nello svolgimento autonomo di compiti, verifiche o altre attività di valutazione, salvo diversa indicazione del docente;
- dichiarano sempre quando un elaborato è stato prodotto con il supporto dell'IA, specificando quale strumento è stato utilizzato e in che modo;
- non creano contenuti falsi, manipolati o offensivi (deepfake, immagini alterate, audio contraffatti) che ritraggono compagni, docenti o altre persone;
- non diffondono contenuti generati dall'IA spacciandoli per propri senza indicarne la fonte;
- mantengono un approccio critico verso i contenuti generati dall'IA, consapevoli che possono contenere errori, imprecisioni o bias;
- rispettano la privacy propria e altrui, evitando di inserire dati personali sensibili negli strumenti di IA generativa.

I docenti:

- educano gli studenti e le studentesse all'uso critico e consapevole dell'IA, illustrandone potenzialità, limiti e rischi (allucinazioni, bias algoritmici, questioni etiche);
- progettano e conducono attività didattiche che integrino l'IA in modo trasparente, etico e pedagogicamente fondato, privilegiando strumenti che si basano su fonti caricate e verificate dal docente;
- verificano l'originalità e la rielaborazione personale degli elaborati degli studenti, segnalando al Dirigente Scolastico eventuali usi fraudolenti o non autorizzati;
- si impegnano a non caricare sulle piattaforme online non in linea con il GDPR e il Regolamento (UE) 2024/1689 (AI Act) eventuali foto, video, testi scritti a mano o registrazioni vocali degli alunni, in quanto considerati dati biometrici che potrebbero essere riutilizzati per l'addestramento dei modelli;
- si aggiornano sulle evoluzioni tecnologiche e sulle implicazioni educative dell'IA generativa, partecipando a percorsi di formazione specifici.

Infrazioni alla ePolicy

L'utilizzo non autorizzato o fraudolento di strumenti di intelligenza artificiale generativa costituisce infrazione al presente documento e comporta l'applicazione di sanzioni educative e/o disciplinari graduate in base alla gravità della violazione, analogamente a quanto previsto per le altre infrazioni relative all'uso delle tecnologie digitali (vedi paragrafo 1.5).

Saranno considerate infrazioni, in particolare:

- l'uso dell'IA per copiare o falsificare compiti e verifiche senza autorizzazione;
- la creazione e diffusione di deepfake o contenuti manipolati che ledono la dignità e la reputazione di compagni, docenti o altre persone;
- la presentazione di elaborati interamente generati dall'IA come lavori propri, senza dichiarazione e senza rielaborazione personale;
- la condivisione di contenuti falsi o disinformativi generati dall'IA.

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.

Utilizzo dei dispositivi digitali

L'Istituto riconosce il valore educativo delle tecnologie digitali quando utilizzate per finalità didattiche e nel rispetto delle regole condivise. In conformità alle disposizioni ministeriali e al Regolamento d'Istituto, non è consentito l'utilizzo di dispositivi personali non autorizzati, quali smartphone e smartwatch, durante l'orario scolastico.

La scuola privilegia la fornitura diretta dei dispositivi tecnologici necessari alle attività didattiche, al fine di garantire uniformità degli strumenti, pari opportunità di accesso e una gestione più efficace degli aspetti organizzativi, tecnici e di sicurezza, limitando il ricorso alla pratica del BYOD (Bring Your Own Device).

L'Istituto Comprensivo Parmigianino di Parma, in coerenza con il Piano Nazionale Scuola Digitale (PNSD) - Azione #6, che promuove l'integrazione dei dispositivi personali nelle attività didattiche in collaborazione con famiglie ed enti del territorio, e nel rispetto della nota ministeriale n. 5275 dell'11/07/2024, disciplina l'utilizzo di PC e tablet personali secondo le seguenti disposizioni.

1. Agli studenti è consentito l'utilizzo di dispositivi personali esclusivamente per finalità didattiche, previo consenso delle famiglie e autorizzazione del docente.
2. Gli studenti sono responsabili della custodia dei propri dispositivi; la scuola non risponde di eventuali danni, smarrimenti o furti.
3. Durante l'orario scolastico è vietato l'utilizzo dei dispositivi per finalità personali (messaggistica, chiamate,

navigazione non autorizzata, giochi o attività non connesse alla didattica).

4. La realizzazione di fotografie, video o registrazioni audio è consentita esclusivamente previa autorizzazione del docente.
5. Eventuali registrazioni o contenuti prodotti nell'ambito scolastico non possono essere pubblicati o diffusi su canali diversi da quelli istituzionalmente autorizzati.

Azioni previste per l'anno scolastico 2025/2026

- monitorare l'utilizzo dei dispositivi personali da parte di studenti, docenti e personale ATA;
- raccogliere contributi e promuovere momenti di consultazione con docenti, studenti e famiglie per la definizione e l'aggiornamento delle indicazioni e dei regolamenti sull'uso dei dispositivi digitali personali;
- organizzare attività formative rivolte a personale, studenti e famiglie sui temi delle tecnologie digitali, della protezione dei dati personali e della cittadinanza digitale;
- promuovere percorsi dedicati all'accesso sicuro a Internet e all'utilizzo consapevole delle tecnologie digitali (cybersecurity).

Azioni previste per il triennio successivo

- consolidare il monitoraggio periodico dell'utilizzo dei dispositivi personali all'interno dell'Istituto;
- aggiornare regolamenti e procedure sulla base dei risultati emersi dalle consultazioni e dalle pratiche adottate;
- mantenere percorsi continuativi di formazione e sensibilizzazione rivolti a personale, studenti e famiglie sui temi della cittadinanza digitale, della protezione dei dati personali e della sicurezza informatica;
- rafforzare la cultura dell'uso responsabile delle tecnologie digitali e dell'accesso consapevole alla rete.

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.

Le procedure standardizzate per la segnalazione e la gestione dei comportamenti online a rischio, definite nel **Protocollo di emergenza nei casi di bullismo e cyberbullismo - A.S. 2025/2026**, costituiscono un riferimento operativo per tutto il personale dell'IC Parmigianino nell'individuazione, presa in carico e gestione delle situazioni critiche.

Le procedure adottate dall'IC Parmigianino individuano le figure responsabili della segnalazione e della gestione dei casi, prevedendo il coinvolgimento del referente per il contrasto al bullismo e cyberbullismo, del Dirigente Scolastico e, ove necessario, la collaborazione con enti e servizi del territorio.

Le procedure sono condivise con l'intera comunità scolastica attraverso incontri dedicati, comunicazioni istituzionali, pubblicazioni sul sito della scuola e altri strumenti ritenuti efficaci, al fine di favorire l'emersione delle situazioni a rischio e promuovere un ambiente scolastico sicuro e attento al benessere di studenti e studentesse.

Il personale docente del nostro Istituto, quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione le procedure standardizzate definite nel **Protocollo di emergenza nei casi di bullismo e cyberbullismo - A.S. 2025/2026** (link di seguito riportato).

[Protocollo di emergenza potenziali casi di bullismo e cyberbullismo A.S. 2025/2026](#)

Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola.

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

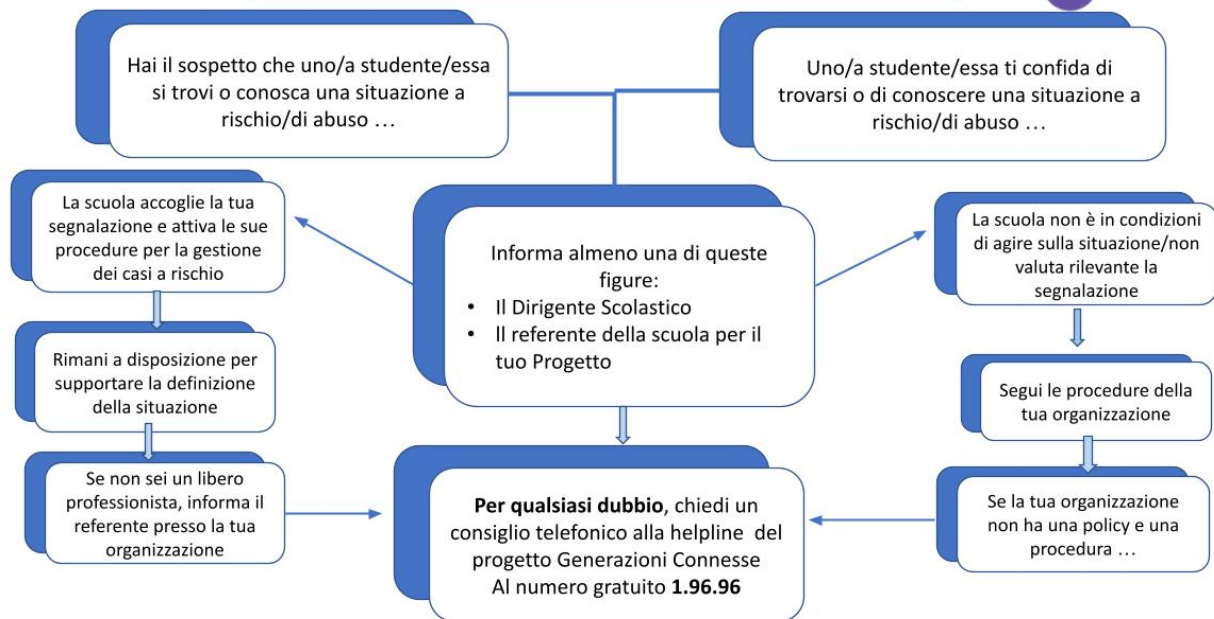
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

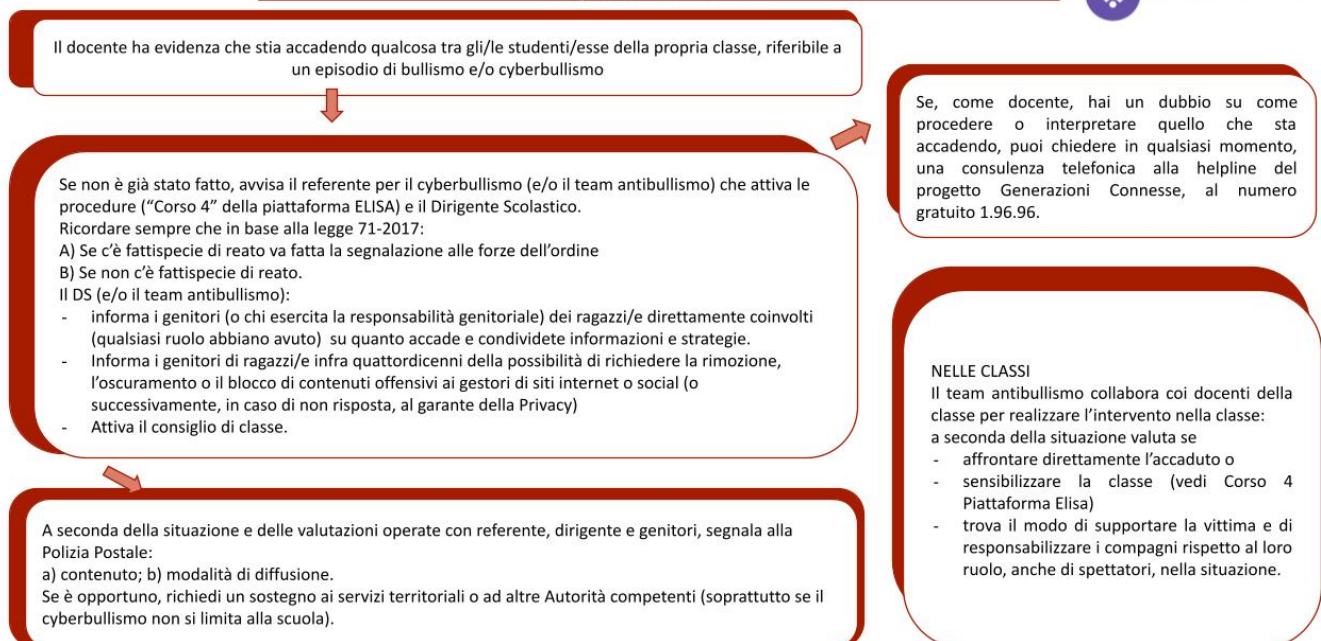
Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle [Linee di Orientamento per la prevenzione e il contrasto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



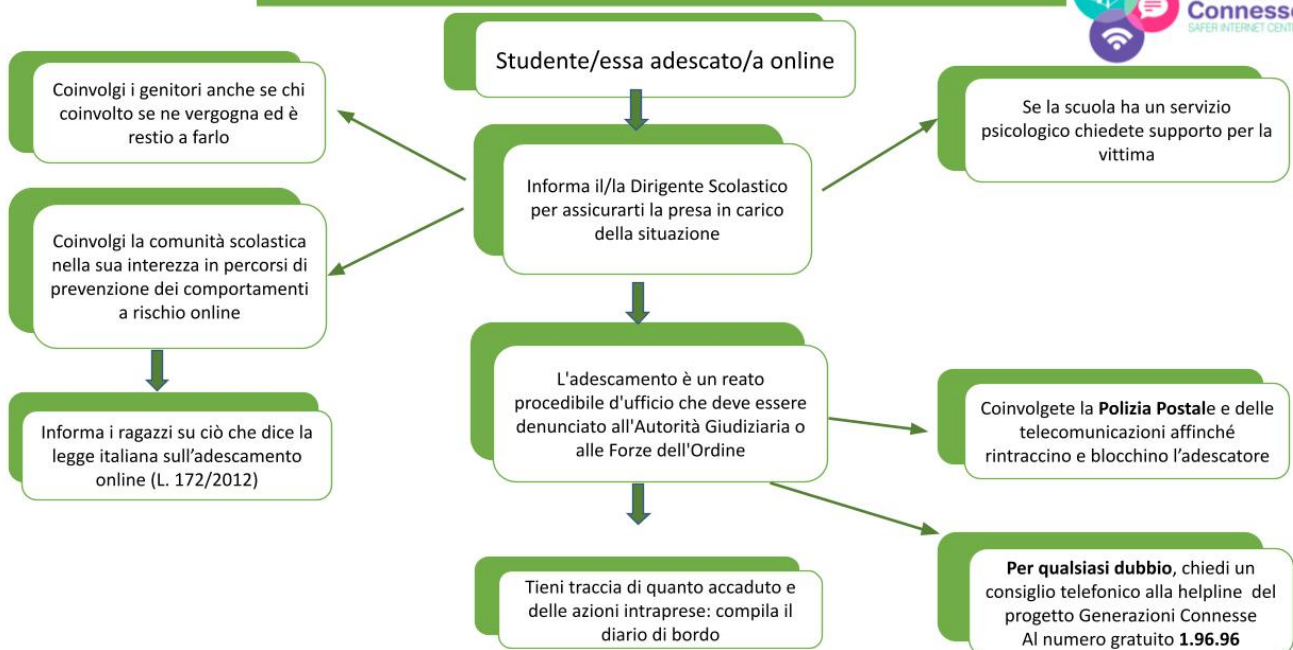
Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

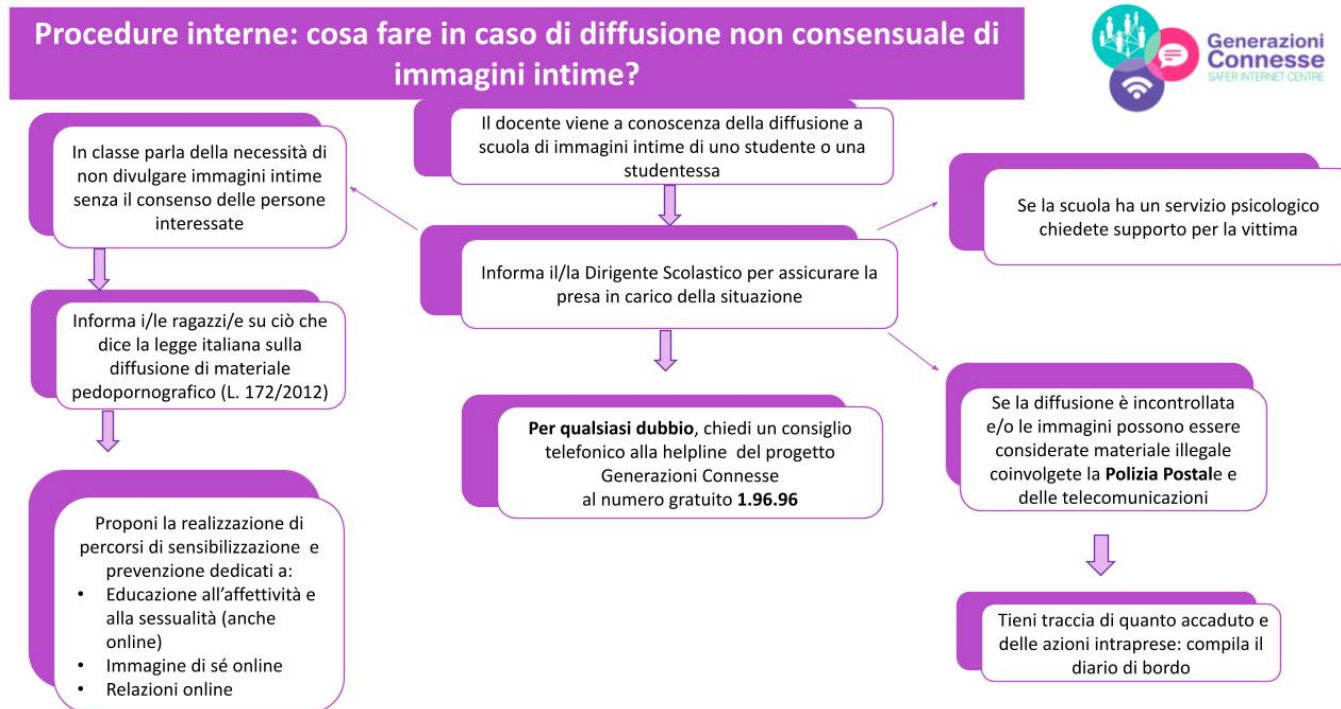


Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



Procedure interne: cosa fare in caso di Adescamento Online?





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, l'IC Parmigianino prevede i seguenti strumenti di segnalazione:

- un indirizzo e-mail specifico per le segnalazioni (disponibile sul sito della scuola);
- una "cassetta" per la raccolta di segnalazioni anonime inserita in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.
- **PROTOCOLLO DI EMERGENZA NEI CASI DI BULLISMO E CYBERBULLISMO**
A.S. 2025/2026 - [Protocollo di emergenza potenziali casi di bullismo e cyberbullismo A.S. 2025/2026](#)

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