



# Documento di ePolicy "COSSALI" - ORZINUOVI

VIA MILANO 83 - 25034 - ORZINUOVI  
Brescia (BS) - Lombardia  
Data di approvazione: 08/05/2026 - 14:28

# Cap 1 - Lo scopo della ePolicy

---

## 1.1 Scopo della ePolicy

### Capitolo 1 - Presentazione dell'ePolicy

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

### Capitolo 2 - Sensibilizzazione e prevenzione

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

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

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

### Capitolo 4 - Segnalazione e gestione dei casi

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

## 1.1 Scopo dell'ePolicy

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

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

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

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

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

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

Attraverso la presente E-policy, il nostro Istituto si dota di uno strumento operativo e strategico per l'intera comunità educante. L'obiettivo è garantire un approccio alle tecnologie che sia consapevole, critico ed efficace, promuovendo azioni mirate a valorizzare le opportunità digitali e a prevenire i rischi connessi.

L'E-policy definisce le linee guida per promuovere il benessere in Rete, stabilendo regole chiare per l'utilizzo delle TIC (Tecnologie dell'Informazione e della Comunicazione) a scuola. Il documento pone le basi per percorsi formativi sull'uso delle tecnologie digitali e per attività di sensibilizzazione continua.

In linea con le direttive del MIM sull'Educazione Civica Digitale, il documento si pone i seguenti obiettivi:

1. salvaguardare la sicurezza e la privacy degli studenti e di tutto il personale scolastico;
2. supportare il personale nell'adozione di modalità di lavoro sicure, etiche e responsabili;
3. definire aspettative comportamentali e codici di condotta per l'uso di Internet a scopo didattico e personale;
4. prevenire e contrastare ogni forma di abuso online, con particolare attenzione al fenomeno del cyberbullismo;
5. rafforzare la consapevolezza che comportamenti illeciti o pericolosi non sono ammissibili e comporteranno l'adozione delle opportune sanzioni disciplinari o azioni giudiziarie.

Il presente testo è parte integrante e coerente con i seguenti documenti d'Istituto:

- regolamento di Istituto;
- regolamento e Protocollo anti-bullismo e cyberbullismo;
- piano Scolastico per la Didattica Digitale Integrata (ex PNSD);
- patto di Corresponsabilità Educativa;
- piano Triennale dell'Offerta Formativa (PTOF).

---

## 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 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.

In coerenza con quanto sopra descritto, l'Istituto definisce modalità operative condivise per il coordinamento tra le diverse figure coinvolte, al fine di garantire efficacia, tempestività e uniformità degli interventi.

In particolare:

- le diverse figure operano in modo integrato, nel rispetto delle rispettive competenze, attraverso il coordinamento del Dirigente Scolastico e del Team antibullismo;
- le segnalazioni e la gestione dei casi avvengono secondo procedure condivise, con il coinvolgimento del Referente bullismo e cyberbullismo, del Consiglio di Classe e, ove necessario, delle altre figure di sistema;
- tutte le azioni intraprese sono oggetto di tracciabilità e verbalizzazione, nel rispetto della normativa sulla protezione dei dati personali;
- gli interventi sono orientati, ove possibile, a finalità educative, preventive e riparative, in coerenza con il Regolamento di Istituto e la normativa vigente;

- è garantito il raccordo con i servizi territoriali e con le Autorità competenti nei casi che lo richiedano;
- la collaborazione tra scuola, famiglie e studenti è promossa come elemento essenziale per l'efficacia delle azioni educative.

---

## 1.3 Integrazione ePolicy nei documenti scolastici

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

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

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

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

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

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

Il nostro Istituto ha integrato l'ePolicy all'interno del sistema documentale d'istituto attraverso un processo partecipato che ha coinvolto il Collegio Docenti e il Consiglio d'Istituto.

Nello specifico:

- aggiornamento Regolamenti: sono state inserite clausole specifiche nei Regolamenti riguardanti l'uso dei dispositivi personali, della AI e delle dotazioni tecnologiche, definendo le responsabilità per studenti e personale;
- patto di Corresponsabilità: è stato integrato un comma relativo al rispetto dell'identità digitale altrui, impegnando le famiglie a monitorare l'uso dei social network fuori dall'orario scolastico per prevenire fenomeni di cyberbullismo;
- la scuola ha previsto moduli trasversali di Educazione Civica Digitale per ogni ordine di grado, focalizzati sulla gestione della privacy e sulla verifica delle fonti (fake news);
- formazione famiglie: l'Istituto aderisce a reti di scuole con l'obiettivo di programmare annualmente incontri formativi,

in modalità webinar o in presenza, avvalendosi della collaborazione di esperti esterni e delle Forze dell'Ordine (Polizia Postale) per supportare i genitori nella gestione dei rischi della Rete;

- monitoraggio: la Commissione ePolicy, effettua una revisione annuale del documento per adeguarlo all'evoluzione delle tecnologie e dei bisogni educativi emersi durante l'anno scolastico.

## 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.



Al fine di rendere l'ePolicy uno strumento vivo e condiviso, il nostro Istituto ha adottato le seguenti modalità operative:

- diffusione e Accessibilità: il documento è pubblicato in un'apposita sezione del sito web e inviato a tutte le famiglie tramite il Registro Elettronico all'inizio di ogni anno scolastico;
- curriculum DigComp 2.2: l'Istituto ha recepito il quadro europeo DigComp 2.2 integrando nei percorsi di Educazione Civica attività specifiche sulla sicurezza dei dati e sull'analisi critica delle informazioni online, calibrate per le diverse fasce d'età degli alunni;
- iniziative con il Territorio: l'Istituto aderisce a reti di scuole al fine di programmare annualmente incontri formativi, in modalità webinar o in presenza, avvalendosi della collaborazione di esperti esterni e delle Forze dell'Ordine (Polizia Postale) per supportare i genitori nella gestione dei rischi della Rete;
- feedback e revisione: durante gli incontri periodici con i rappresentanti dei genitori, viene riservato uno spazio di confronto per raccogliere osservazioni sull'efficacia delle informative prodotte, permettendo un aggiornamento costante del linguaggio utilizzato per renderlo sempre più accessibile alle famiglie.

## 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

Il nostro Istituto, al fine di rendere operativo il programma triennale di educazione civica digitale, ha definito il seguente cronoprogramma di azioni specifiche:

Azioni per l'anno scolastico in corso (consolidamento e avvio):

- revisione documentale: integrazione delle norme comportamentali nei Regolamenti in base alla normativa vigente.

Azioni per il secondo anno (formazione e coinvolgimento):

- consultazione studentesca: realizzazione di laboratori partecipati con gruppi di studenti per tradurre le regole dell'ePolicy in un 'Codice Etico Digitale' scritto con il loro linguaggio;
- formazione Peer-to-Peer: implementazione di modelli di 'Peer Education' in cui gli studenti più grandi formano i più piccoli sull'uso responsabile dei social network e del gaming online;

- iniziative di Prevenzione: attivazione di percorsi formativi integrati nel curriculum di Educazione Civica, focalizzati sulla protezione dei dati personali, avvalendosi dei materiali didattici del portale Generazioni Connesse.
- avvio di un sistema di monitoraggio interno per intercettare precocemente dinamiche di esclusione o disagio riconducibili al cyberbullismo.

Azioni per il terzo anno (sviluppo e rete territoriale):

- potenziamento competenze: consolidamento dei progetti sulla Cittadinanza Digitale Attiva e sulla Legalità, in collaborazione con la Polizia Postale e associazioni del Terzo Settore specializzate nel supporto psicologico online;
- valutazione dell'impatto: Inserimento degli esiti del monitoraggio dell'ePolicy all'interno del Rapporto di Autovalutazione (RAV), per misurare il miglioramento del clima scolastico e della consapevolezza digitale dell'intera comunità educante.

---

## 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](#)

## 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.

In coerenza con quanto sopra delineato, l'Istituto integra il quadro generale attraverso azioni strutturate e continuative finalizzate a rendere la sensibilizzazione e la prevenzione pratiche educative quotidiane e condivise.

#### **Integrazione nel curriculum e nelle progettualità di Istituto.**

Le tematiche della cittadinanza digitale, della sicurezza in rete e del benessere digitale sono integrate:

- nei percorsi di Educazione Civica, in linea con la Legge 92/2019;
- nelle discipline, in ottica trasversale;
- nei progetti di Istituto dedicati alla prevenzione e all'uso consapevole delle tecnologie.

Le attività sono calibrate per età e indirizzo e comprendono, tra l'altro:

- educazione alla privacy e alla protezione dei dati personali;
- sviluppo del pensiero critico rispetto alle informazioni online;
- riflessione su identità digitale, reputazione e responsabilità;
- uso consapevole delle tecnologie emergenti, inclusa l'intelligenza artificiale.

#### **Azioni educative per gli studenti.**

L'Istituto promuove interventi continuativi rivolti agli studenti, quali:

- attività laboratoriali, simulazioni e analisi di casi reali;
- percorsi di peer education e responsabilizzazione attiva;
- incontri con esperti esterni e Forze dell'Ordine;
- iniziative di sensibilizzazione su cyberbullismo, uso scorretto dei social e rischi della rete.

Particolare attenzione è riservata agli studenti in situazione di fragilità o coinvolti in episodi critici, anche attraverso percorsi educativi personalizzati.

#### **Coinvolgimento delle famiglie.**

L'Istituto promuove il coinvolgimento delle famiglie mediante:

- incontri informativi e formativi online;
- condivisione di materiali e linee guida sull'uso consapevole dei dispositivi.

### **Formazione del personale scolastico**

Sono previsti momenti di formazione e aggiornamento per i docenti e il personale scolastico su:

- cittadinanza digitale e sicurezza online;
- gestione educativa e disciplinare di situazioni legate all'uso improprio delle tecnologie;
- integrazione didattica delle competenze digitali.

### **Collegamento con le azioni di prevenzione e gestione dei casi.**

Le attività di sensibilizzazione e prevenzione sono strettamente connesse ai protocolli di Istituto per:

- la prevenzione e il contrasto del cyberbullismo;
- la gestione delle segnalazioni e delle situazioni critiche;
- l'attivazione di percorsi educativi e riparativi, anche in caso di sanzioni disciplinari.

### **Monitoraggio e aggiornamento.**

L'Istituto prevede momenti periodici di monitoraggio dell'efficacia delle azioni intraprese, attraverso:

- raccolta di feedback da parte di studenti, famiglie e docenti;
- confronto negli organi collegiali;
- aggiornamento annuale delle strategie e degli strumenti adottati.

---

## **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.

Per realizzare tali obiettivi, l'Istituto utilizza e valorizza le risorse messe a disposizione a livello nazionale e internazionale, adottando un approccio strutturato e progressivo allo sviluppo delle competenze digitali.

Il DigComp 2.2, framework europeo per le competenze digitali, costituisce la cornice di riferimento per l'individuazione delle aree di competenza e dei traguardi formativi, non solo per gli studenti ma anche per docenti e famiglie, in un'ottica di comunità educante.

In particolare, il framework consente di organizzare in modo sistemico i percorsi relativi a:

- alfabetizzazione su dati e informazioni;
- comunicazione e collaborazione online;
- creazione di contenuti digitali;
- sicurezza (privacy, protezione dei dati, benessere digitale);
- problem solving e uso consapevole delle tecnologie.

All'interno di tale cornice, l'Istituto progetta e realizza percorsi formativi specifici rivolti agli studenti, finalizzati allo sviluppo di una cittadinanza digitale consapevole, critica e responsabile.

Per quanto riguarda gli studenti, tali percorsi trovano sviluppo nel curriculum di Educazione Civica, ai sensi della Legge 92/2019, e si integrano trasversalmente nelle discipline.

Il curriculum è strettamente connesso all'ePolicy di Istituto, che ne rappresenta il riferimento operativo e valoriale: le attività didattiche sono progettate in coerenza con i principi, i regolamenti e le scelte educative in esso contenute.

In ogni classe è previsto almeno un modulo didattico specifico annuale, calibrato in base all'età degli studenti e al percorso di studi, dedicato ai temi della sicurezza in rete, dell'uso consapevole delle tecnologie e della cittadinanza digitale.

Tali attività possono avvalersi anche dei kit didattici e delle risorse proposte dal progetto Generazioni Connesse, al fine di favorire una maggiore conoscenza, partecipazione e consapevolezza da parte degli studenti.

Le azioni previste nel curriculum sono inoltre integrate da:

- attività laboratoriali e metodologie attive (debate, analisi di casi, simulazioni);
- percorsi di peer education;
- momenti di confronto guidato su esperienze reali legate all'uso delle tecnologie.

I regolamenti e le attività sviluppate sul tema della prevenzione, presenti nell'ePolicy, costituiscono parte integrante e continuativa delle azioni di disseminazione, sensibilizzazione e formazione promosse dall'Istituto, contribuendo alla costruzione di un ambiente digitale sicuro, inclusivo e rispettoso.

---

## 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.

# 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.

In attuazione del quadro normativo sopra richiamato, l'Istituto adotta misure organizzative, tecniche e procedurali volte a garantire la sicurezza, l'integrità e la riservatezza dei dati personali trattati attraverso le infrastrutture e le strumentazioni ICT in uso.

### Gestione dell'infrastruttura digitale.

L'Istituto cura la gestione e la sicurezza dell'infrastruttura ICT (reti, dispositivi, piattaforme e servizi digitali) attraverso:

- sistemi di protezione della rete (firewall, filtri dei contenuti, antivirus e sistemi di aggiornamento);
- gestione controllata degli accessi alle reti interne e alle piattaforme digitali;
- utilizzo di credenziali personali e non cedibili per l'accesso ai servizi;
- procedure di backup periodico dei dati e di ripristino in caso di perdita o incidente;
- monitoraggio e manutenzione periodica dei sistemi.

### Misure di sicurezza e protezione dei dati

In conformità al GDPR, l'Istituto adotta misure tecniche e organizzative adeguate, tra cui:

- limitazione dell'accesso ai dati ai soli soggetti autorizzati (principio di minimizzazione e necessità);
- protezione dei dispositivi digitali mediante password sicure e sistemi di autenticazione;
- aggiornamento costante dei software e dei sistemi operativi;
- gestione sicura degli archivi digitali e dei dati sensibili;
- definizione di procedure per la gestione di eventuali data breach (violazioni dei dati personali).

### Organizzazione e responsabilità



L'Istituto definisce e aggiorna un organigramma privacy, individuando ruoli e responsabilità in materia di trattamento dei dati, tra cui:

- il Dirigente Scolastico quale Titolare del trattamento;
- il Responsabile della Protezione dei Dati (DPO/RPD);
- i soggetti autorizzati al trattamento (docenti, personale ATA, amministrativi);
- eventuali Responsabili esterni del trattamento (fornitori di servizi digitali, piattaforme).

Tutti i soggetti coinvolti operano secondo istruzioni precise e sono adeguatamente formati.

### **Formazione e consapevolezza**

L'Istituto promuove azioni di formazione rivolte al personale scolastico finalizzate a:

- garantire una corretta gestione dei dati personali;
- prevenire comportamenti a rischio (es. uso improprio di strumenti digitali, condivisione non autorizzata di dati);
- diffondere buone pratiche di sicurezza informatica.

### **Utilizzo delle strumentazioni digitali**

L'utilizzo di dispositivi e strumenti digitali (computer, tablet, LIM, piattaforme online) avviene nel rispetto di:

- finalità didattiche e istituzionali;
- normativa vigente in materia di protezione dei dati personali;
- regolamenti di Istituto e indicazioni contenute nell'ePolicy.

L'Istituto promuove un uso responsabile e consapevole delle tecnologie, anche in relazione ai dispositivi personali eventualmente utilizzati (BYOD), se consentiti.

### **Monitoraggio e aggiornamento**

Le misure adottate sono oggetto di verifica periodica e aggiornamento, anche in relazione:

- all'evoluzione normativa;
- ai rischi emergenti in ambito digitale;
- alle indicazioni delle autorità competenti (es. Garante per la protezione dei dati personali).

---

## **3.2 - Strumenti di comunicazione online (PUA)**

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

La Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) costituisce parte integrante dell'ePolicy di Istituto e si configura come uno strumento operativo volto a regolamentare l'utilizzo delle infrastrutture digitali e della rete, sia in ambito scolastico sia nell'ambito delle attività didattiche svolte online o a distanza.

Pur richiamando i principi storicamente contenuti nel Documento Programmatico sulla Sicurezza (DPS), oggi non più obbligatorio, la P.U.A. si inserisce nel più ampio sistema di gestione della protezione dei dati personali previsto dal Regolamento (UE) 2016/679 (GDPR) e dal D.lgs. 196/2003, come modificato dal D.lgs. 101/2018.

### **Finalità della P.U.A.**

La P.U.A. ha la finalità di:

- promuovere un uso consapevole, responsabile e sicuro delle tecnologie digitali;
- prevenire comportamenti scorretti o illeciti nell'utilizzo della rete;
- tutelare i dati personali e i diritti di tutti i soggetti coinvolti;
- garantire un utilizzo delle risorse digitali coerente con le finalità educative e istituzionali della scuola.

### **Ambito di applicazione**

Le regole definite nella P.U.A. si applicano a:

- studenti e studentesse;
- personale docente e ATA;
- collaboratori, esperti esterni e professionisti che operano a qualsiasi titolo nell'Istituto.

### **Comportamenti non consentiti.**

In coerenza con quanto già previsto, la P.U.A. individua e vieta comportamenti quali:

- accesso, ricerca o diffusione di contenuti non coerenti con le finalità educative della scuola;
- utilizzo della rete per finalità non didattiche (es. gioco online non autorizzato, uso improprio dei dispositivi);
- realizzazione o diffusione di contenuti offensivi, discriminatori o lesivi della dignità altrui;
- violazione della normativa sulla protezione dei dati personali e della privacy;
- violazione dei diritti d'autore e uso illecito di materiali digitali;
- utilizzo delle tecnologie per finalità illecite o dannose (es. cyberbullismo, accesso abusivo a sistemi informatici).

### **Tutela dei dati e responsabilità.**

La P.U.A. richiama espressamente il rispetto delle normative vigenti in materia di protezione dei dati personali, con particolare attenzione alla tutela degli studenti e delle studentesse.

Tutti gli utenti della rete scolastica sono tenuti a:

- utilizzare credenziali personali in modo corretto e riservato;
- non condividere dati sensibili senza autorizzazione;
- rispettare le indicazioni fornite dall'Istituto in materia di sicurezza digitale.

### **Valenza educativa.**

La P.U.A. non ha solo funzione regolativa, ma rappresenta uno strumento educativo volto a sviluppare negli studenti competenze di cittadinanza digitale, favorendo comportamenti responsabili anche al di fuori del contesto scolastico.

### **Collegamento con ePolicy e regolamenti.**

La P.U.A. si integra con:

- l'ePolicy di Istituto;
- il Regolamento di Istituto;
- il Patto di corresponsabilità educativa;
- i protocolli di prevenzione e gestione di situazioni critiche (es. cyberbullismo).

Essa costituisce pertanto un riferimento condiviso per tutte le azioni di prevenzione, sensibilizzazione e gestione dell'uso delle tecnologie.

---

## 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.

La presente ePolicy integra e coordina le disposizioni già presenti nei Regolamenti di Istituto in materia di utilizzo dei dispositivi digitali personali (BYOD - Bring Your Own Device), nel rispetto delle indicazioni ministeriali e delle Linee guida per l'uso consapevole delle tecnologie a scuola.

L'Istituto promuove un approccio equilibrato che valorizzi le potenzialità didattiche dei dispositivi digitali, favorendone un uso consapevole, responsabile e finalizzato all'apprendimento, nel rispetto delle regole condivise e della tutela dei dati personali.

L'Istituto si impegna inoltre a promuovere momenti di confronto all'interno della comunità scolastica (docenti, studenti, famiglie) al fine di aggiornare periodicamente la regolamentazione, tenendo conto delle evoluzioni tecnologiche e delle esigenze educative.

## 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.

In coerenza con quanto sopra descritto, l'Istituto integra le procedure di segnalazione e gestione dei casi garantendo:

- la tempestività, riservatezza e tracciabilità delle segnalazioni, anche attraverso l'utilizzo di apposita modulistica e verbalizzazione degli interventi;
- la tutela della vittima, con particolare attenzione alla prevenzione di eventuali ritorsioni e alla gestione protetta delle informazioni;
- una presa in carico non esclusivamente disciplinare, ma orientata anche a finalità educative e riparative, in coerenza con la normativa vigente;
- il coinvolgimento del Team antibullismo e delle figure di riferimento dell'Istituto per la valutazione e gestione dei casi;
- la collaborazione con i servizi territoriali e, nei casi previsti, con le Autorità competenti, nel rispetto degli obblighi di legge;
- il raccordo con i Regolamenti di Istituto e con il Patto di corresponsabilità educativa.

## 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.

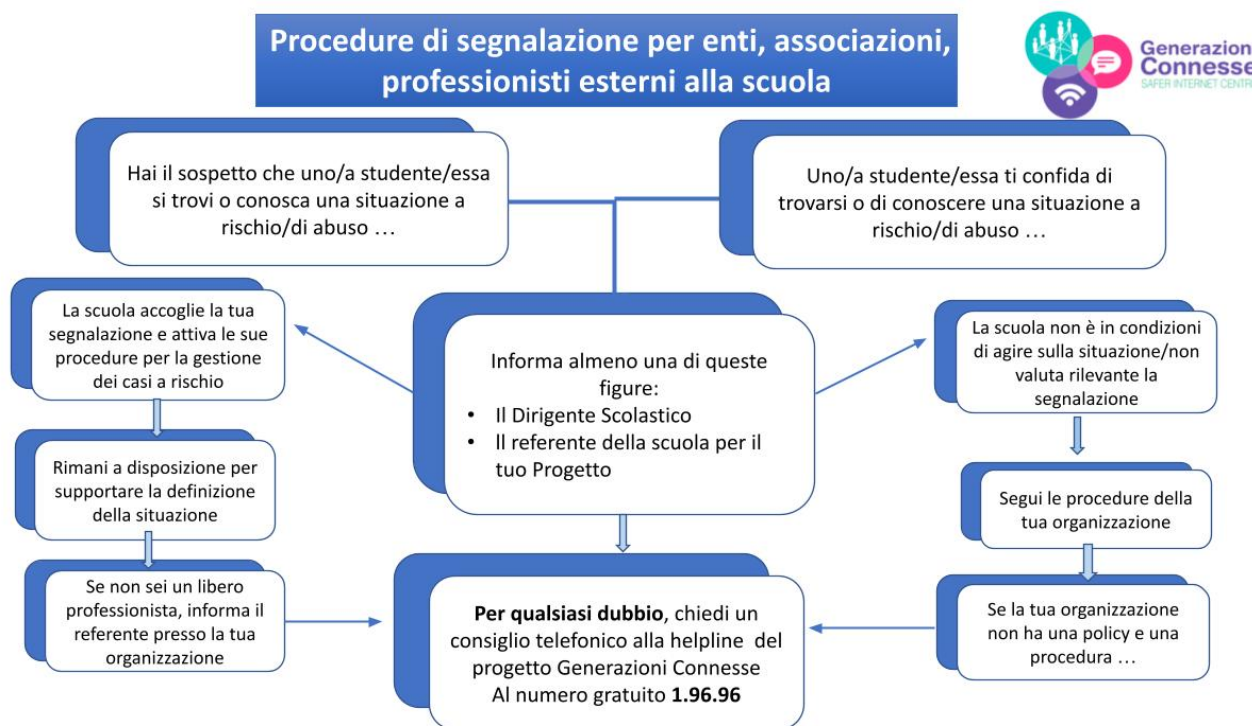
## Strumenti a disposizione di studenti/esse

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 condividente 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.

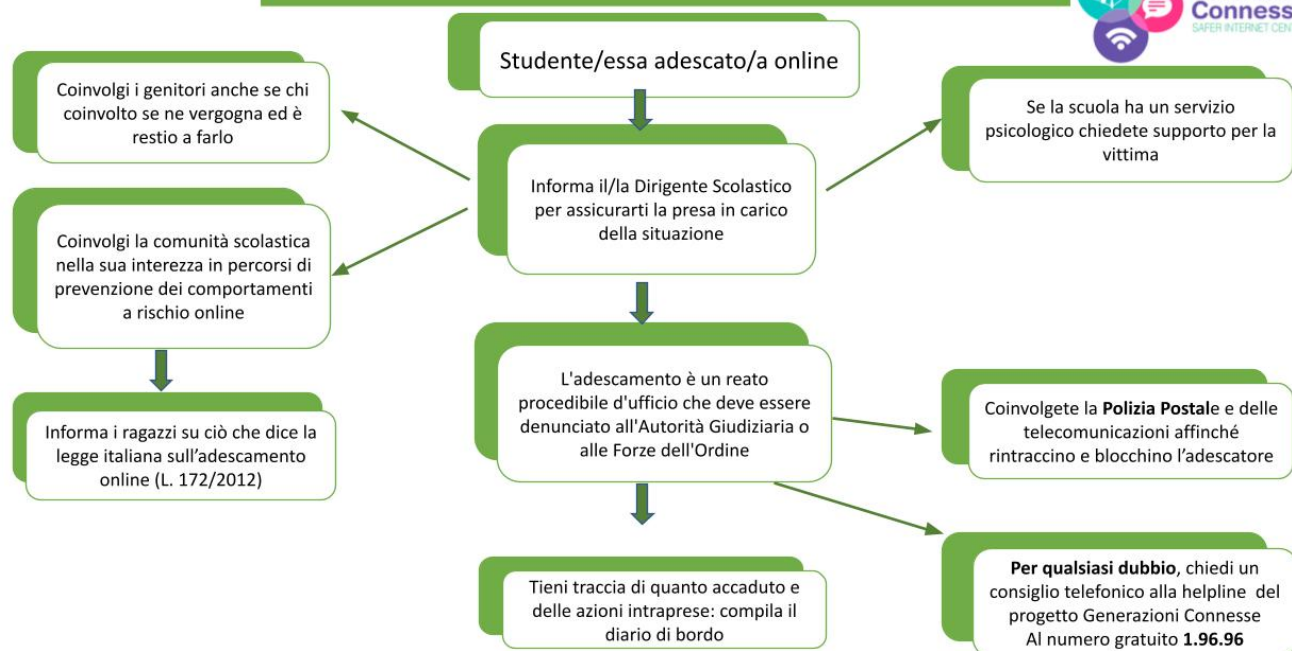
Scarica le linee di orientamento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo

**Se emergono evidenze passa allo schema successivo**

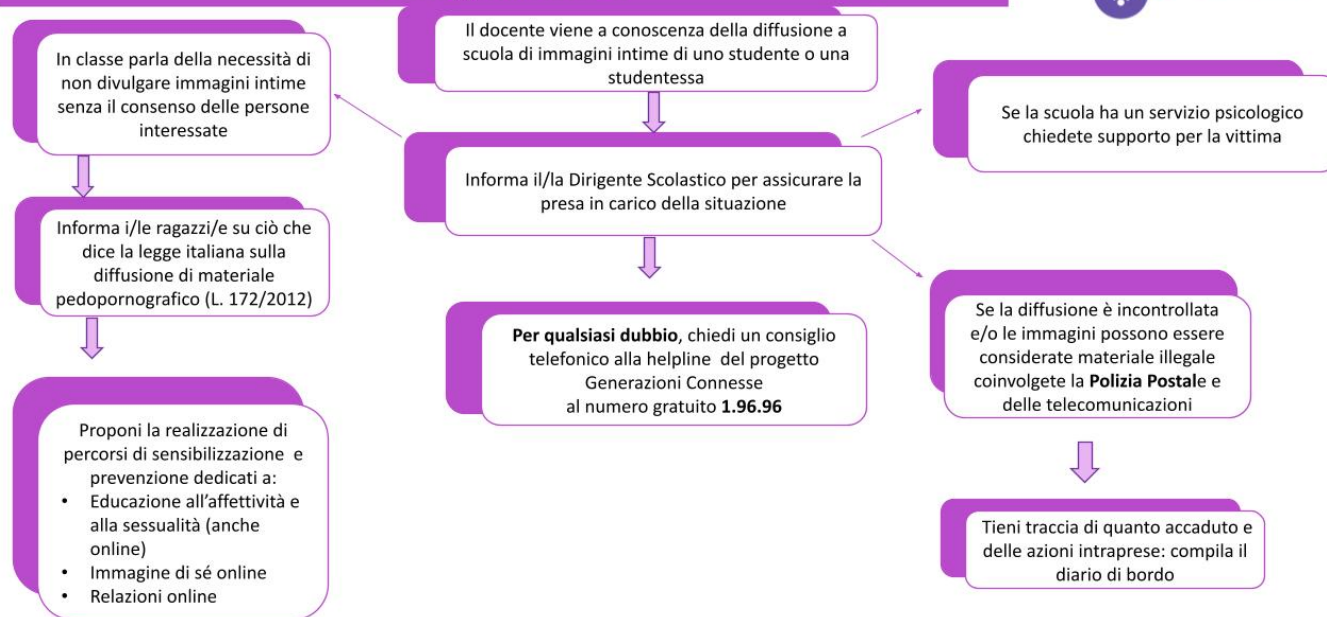
Ricorda a studenti/esse che possono chiedere in qualsiasi momento una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 o via chat



## Procedure interne: cosa fare in caso di Adescamento Online?



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



In coerenza con quanto sopra descritto, l'Istituto definisce modalità operative condivise per la gestione delle segnalazioni e dei casi, al fine di garantire efficacia, uniformità di intervento e tutela di tutti i soggetti coinvolti.

In particolare:

- le segnalazioni sono formalizzate tramite apposita modulistica interna e trasmesse tempestivamente al Referente e al Team antibullismo;
- tutte le fasi di gestione del caso sono oggetto di verbalizzazione e tracciabilità, nel rispetto della normativa sulla protezione dei dati personali;
- il Team antibullismo, in raccordo con il Dirigente Scolastico, coordina la presa in carico del caso e definisce le azioni educative, preventive ed eventualmente disciplinari;
- è garantito il coinvolgimento del Consiglio di Classe, in relazione alle competenze educative e valutative;
- gli interventi sono orientati, ove possibile, a finalità educative e riparative, anche attraverso percorsi di cittadinanza attiva e responsabilizzazione;
- nei casi di particolare gravità, è previsto il raccordo con i servizi territoriali e, ove necessario, con le Autorità competenti, nel rispetto degli obblighi di legge;
- l'Istituto promuove strumenti di segnalazione accessibili e diversificati (docenti di riferimento, sportello di ascolto, canali dedicati), garantendo la tutela della riservatezza.