

# Documento di ePolicy

## S. ANTONIO ABATE - I.C. MASCOLO

VIA GIOVANNI XXIII 26/28 - 80057 - SANT'ANTONIO ABATE

Napoli (NA) - Campania

Data di approvazione: 23/09/2024 - 09:10

# 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

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

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

### Capitolo 4 - Segnalazione e gestione dei casi

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

## 1.1 Scopo dell'ePolicy

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

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

La competenza digitale è una competenza chiave del cittadino europeo come indicato dal Consiglio Europeo (Raccomandazione del 2018) che permette ad ogni cittadino di esercitare i propri diritti all'interno degli ambienti digitali (ONU - [Commento Generale 25](#): I diritti dei minori negli ambienti digitali).

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

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

La stesura del documento ePolicy da parte dell'I.C. "**M. Mascolo-A. De Curtis**" nasce dalla profonda consapevolezza di voler fornire alla comunità educante una buona conoscenza rispetto ai contenuti di educazione alla cittadinanza digitale, per consentire loro di essere al passo con le innovazioni che la nuova tecnologia propone e soprattutto di avere adeguate competenze e precise regole di comportamento rispetto all'uso sicuro di internet.

Gli obiettivi educativi perseguiti dal Dirigente Scolastico, dall'animatore digitale, dal referente del bullismo e cyberbullismo e dai docenti sono quelli di favorire il benessere in rete e sviluppare negli allievi il giusto senso critico che permetta loro di ragionare sui propri comportamenti e atteggiamenti nel mondo virtuale, in modo che possano portare avanti il proprio consapevole punto di vista e di non seguire gli stereotipi comuni, soltanto per uniformarsi a ciò che si propone come tendenza del momento.

---

## 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'impegno 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.

L'attuazione del documento ePolicy è favorita attraverso una serie di azioni condivise da parte di tutto il personale scolastico predisposto alla sua implementazione, affinché si possa realizzare la più completa osservanza delle indicazioni legislative, organizzative, sociali e relazionali ivi presenti.

**Il Dirigente Scolastico** garantisce l'assolvimento dei compiti pertinenti al proprio specifico ruolo.

**Il Responsabile della protezione dei dati (RPD)** conosce l' ePolicy, fornisce e attua la propria consulenza, tenendo conto degli obblighi derivanti dal **GPDR** e ne sorveglia il suo espletamento. Condividerà con gli utenti coinvolti nel mondo della scuola un documento nel quale saranno delineate le procedure da utilizzare pertinenti al trattamento dei dati personali.

**Il personale ATA** è coinvolto nelle pratiche di prevenzione e di implementazione dell'ePolicy e sarà tenuto a segnalare eventuali episodi di bullismo/cyberbullismo.

**L'animatore digitale e la comunità di pratica avranno** cura di vigilare sul corretto utilizzo delle tecnologie da parte degli studenti e delle studentesse.

**Il referente per il bullismo e cyberbullismo** ha il compito di proporre corsi di formazione relativi a specifiche tematiche per i docenti, gli allievi/le allieve e le famiglie, ha inoltre la responsabilità di gestire secondo precise procedure i casi di emergenza, in sinergia con il Dirigente Scolastico, i docenti del consiglio di classe coinvolto e interagisce nel momento in cui vi sia l'esigenza, con le agenzie pubbliche esterne preposte a esplicitare determinati

compiti.

**Gli enti esterni pubblici e privati**, le associazioni possono essere coinvolte nel processo educativo e apportare consulenze pertinenti al fine di rendere maggiormente consapevoli, in determinati ambiti di conoscenza tutti i componenti della scuola.

**Tutti gli insegnanti** hanno la responsabilità di fornire agli alunni competenze in merito all'educazione civica digitale, integrandole nelle proprie discipline di studio e accompagnano gli studenti nei percorsi di apprendimento laboratoriali come l'uso della LIM o di altri dispositivi tecnologici, assicurandosi che tutto avvenga con la massima sicurezza.

---

## 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 svolgersi in un anno e perseguiti negli anni a seguire.**

Considerata l'importanza e la trasversalità dell'ePolicy si ritiene utile integrarlo nei documenti che disciplinano il funzionamento del nostro Istituto, per cui nel corrente anno scolastico 2024/2025 sarà aggiunto al **Regolamento d'Istituto** che rappresenta il principale punto di riferimento normativo dell'Istituzione Scolastica; le indicazioni in esso contenute consentiranno di delineare le norme comportamentali e le procedure di utilizzo delle Tecnologie e della Comunicazione in

ambito scolastico. Sarà ulteriormente integrato nel **Patto di Corresponsabilità** scuola famiglia, puntualizzando l'impegno da parte dell'istituto di organizzare eventi formativi e informativi a beneficio dei genitori/tutori e dall'altro l'impegno di questi ultimi a partecipare in maniera proficua a tali eventi.

### **Azioni da svolgersi in tre anni**

Il documento ePolicy rientrerà a fare parte del Piano triennale dell'offerta formativa già a partire dal corrente anno scolastico e nell'arco dei tre anni che seguiranno sarà applicato con maggiore cognizione e responsabilità.

## **1.4 Condivisione e comunicazione dell'ePolicy**

### **Il paragrafo dettaglia i seguenti aspetti:**

1. il curriculum sulle competenze digitali per la comunità educante (il DigComp2.2);
2. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative;
3. Come comunicare e condividere l'epolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

### **1. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative;**

L'efficacia dell'ePolicy è direttamente proporzionale a livello di conoscenza e diffusione all'interno della comunità scolastica ivi comprese le famiglie. Il documento rappresenta il canale interno privilegiato per informare, responsabilizzare e collaborare sui temi della rete e delle tecnologie a scuola con l'intera comunità scolastica.

In tal senso, il documento è accompagnato da versioni, allegare e sintetiche, all'interno delle quali sono individuati gli elementi principali del documento; una versione è diretta agli studenti ed una è diretta alle famiglie con un linguaggio e una presentazione dei contenuti adeguata, flessibile e chiara. La versione sintetica rivolta agli studenti è inserita all'interno delle attività didattiche dell'educazione alla cittadinanza mentre la versione per le famiglie è consegnata nel corso dei colloqui scuola-famiglia.

Il documento è altresì pubblicato sul sito della scuola ed inserito nel Patto di corresponsabilità.

### **2. Come comunicare e condividere l'ePolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).**

La presenza dell'ePolicy nell'Istituto scolastico è garanzia, per il territorio, della presenza di un presidio informato, sensibile e attento sulla rete e le tecnologie in relazione con i più giovani.

In questo senso l'Istituto può rappresentare per le Istituzioni del territorio, le aziende, e le realtà del Terzo Settore un luogo di confronto privilegiato e di sperimentazione per tutti coloro che intendono costruire progetti di cittadinanza digitale rivolte ai più giovani.

A tal fine l'adozione dell'ePolicy è comunicata all'USR di riferimento e al Municipio (servizi istruzione e servizi sociali)

attraverso gli allegati sintetici progettati che indicano gli elementi del documento e le prospettive per la comunità.

La condivisione e la comunicazione dell'ePolicy all'interno della comunità scolastica viene fatta perseguendo le tre buone pratiche suggerite dall'attività di monitoraggio, che lo staff di generazioni connesse ha realizzato in alcune scuole negli anni precedenti.

Il Referente ePolicy insieme al Referente per il bullismo e il cyberbullismo e all'animatore digitale andranno nelle classi, per un tempo di circa dieci minuti e specificare che esistono regolamenti riguardanti l'educazione civica digitale, come anche tutta una serie di iniziative relative alla sicurezza online, ma l'elemento più importante da sottolineare è quello che la scuola è aperta ad ascoltare le esperienze di ogni singolo studente anche se negative.

---

## 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

L'Istituto intende mettere in campo una serie di piani di azione per rendere l'epolicy operativo e appunto programmatico. Si provvederà alla formazione dei docenti, degli studenti, delle studentesse e delle famiglie, previa somministrazione di uno specifico monitoraggio a cura del referente Epolicy. Successivamente si intendono realizzare dei piani di azione autoprodotti nei quali saranno inserite le caratteristiche peculiari dell'utenza scolastica e le necessità specifiche proprie del territorio, creando al contempo relazioni di connessione con le realtà esterne, che sicuramente potranno permettere alla scuola di arricchire il proprio bagaglio culturale in termini di cittadinanza digitale e promuoverne altri per l'intera comunità. In questa azione si farà riferimento al kit didattico di generazioni

connesse.

---

## 1.6 - Le risorse di Generazioni Connesse

### Risorse di Generazioni Connesse:

- [Kit Didattico](#)
- Area formazione (per docenti, famiglie, studenti/sse con ePolicy)
- Canale [Youtube](#) (webinar, video-stimolo, serie per target differenti)
- Canale [TikTok](#)
- Canale [Instagram](#)
- Canale [Facebook](#)

Le risorse che generazioni connesse (di seguito elencate) propone per il mondo dei giovani, delle loro famiglie e per il team scolastico saranno utilizzate per condividere l'ePolicy e le scelte personali definite dalla scuola per promuovere una cittadinanza digitale attiva all'interno dell'intera comunità scolastica.

### **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.

La sensibilizzazione, la prevenzione e il rispetto per la dignità della persona sono elementi determinanti, affinché nel nostro Istituto si possa creare il giusto benessere psicofisico, indispensabile per ogni essere umano. Diventa così, importante riflettere sulle caratteristiche della comunicazione online (ad esempio come cambia l'empatia! Come si gestiscono le emozioni online! Come si trasformano gli atteggiamenti e comportamenti protetti dal filtro dello schermo!) ed è essenziale anche prevenire episodi di cyberbullismo, di hate speech (linguaggio d'odio) come anche fenomeni come il sexting e l'adescamento, che si manifestano in rete, strettamente collegati all'educazione all'affettività e alla sessualità.

Altra questione centrale è la disinformazione che riguarda le cosiddette fake news, che è un'area strettamente collegata alle nuove questioni sull'intelligenza artificiale e agli algoritmi: questi due fattori entrano in gioco quando si scelgono i contenuti che ognuno di noi visualizza in base alla propria cronologia, ai nostri like, alle nostre condivisioni. Lavorare su questo tema diventa un obiettivo fondamentale per il futuro della democrazia, proprio per la capacità che possono avere questi sistemi di indirizzarci verso determinati contenuti piuttosto che altri. Infine, parlando di cittadinanza, per gli studenti è fondamentale che conoscano i loro diritti e imparare a declinarli nel mondo online: la Convenzioni sui Diritti dell'Infanzia dell'Adolescenza può essere la guida per orientare i percorsi di prevenzione

Gli ingredienti centrali che la scuola mette in atto per prevenire e sensibilizzare sono:

- la formazione dei docenti poiché queste tematiche sono in continua evoluzione;
- l'utilizzo del DigComp che contiene le indicazioni europee sulle competenze digitali, si tratta di una guida che ci fornisce gli indicatori utili a costruire un curriculum verticale sulla competenza digitale;
- il coinvolgimento della famiglia che in sinergia con la scuola e propensa ad accettare le iniziative proposte può sensibilizzare i propri figli/e, promuovere messaggi educativi in linea con la formazione che ricevono in ambito scolastico da rendere così, la prevenzione molto più efficace.
- infine, coinvolgere la comunità educante del territorio (istituzioni locali, organizzazioni, società sportive) aumenta ancora l'efficacia dei percorsi.

## 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.

L'Istituto pone attenzione alle indicazioni che il progetto Generazioni Connesse suggerisce a supporto del lavoro dell'ePolicy, infatti ha previsto per i docenti e studenti di ogni segmento scolastico di elaborare un curriculum digitale a partire dalla scuola dell'infanzia fino alla secondaria di primo grado. Si tratta di un percorso didattico verticale pensato per gli studenti e le studentesse teso a sviluppare e potenziare, le cosiddette "competenze digitali" in ottica trasversale (su più livelli, anni e gradi di istruzione) ed interdisciplinare. Lo scopo è quello di favorire la capacità dell'uso dei dispositivi digitali non solo da un punto di vista strettamente tecnico, ma anche e soprattutto da un punto di vista etico, responsabile e critico utile allo sviluppo della cittadinanza digitale tramite la progettazione e la sperimentazione di percorsi, attività e laboratori in aula dedicate al digitale tra opportunità, rischi e sfide del prossimo futuro.

Questi percorsi potranno essere svolti sia durante l'orario curricolare che extracurricolare, da singole classi o anche da gruppi di studio/lavoro dell'Istituto su un tema coerente con le tecnologie e lo sviluppo delle competenze digitali.

Inoltre si potranno incrociare o inserire tali percorsi con quelli della legge 20 agosto 2019, n. 92 (introduzione dell'insegnamento scolastico dell'educazione civica) che all'articolo 5 prevede di affrontare l'educazione alla cittadinanza digitale.

### LINK di riferimento

- <https://www.curricolidigitali.it>

- <https://ec.europa.eu/social/main.jsp?langId=it&catId=89&newsId=10193&furtherNews=yes>
- [https://joint-research-centre.ec.europa.eu/digcomp\\_en](https://joint-research-centre.ec.europa.eu/digcomp_en)
- [https://www.generazioniconnesse.it/\\_file/documenti/ECD/ECD-2022/pillole/edu-ai-media/Digcomp%202.2.docx.pdf](https://www.generazioniconnesse.it/_file/documenti/ECD/ECD-2022/pillole/edu-ai-media/Digcomp%202.2.docx.pdf)
- [https://www.istruzione.it/scuola\\_digitale/allegati/2016/Allegato\\_1Avviso\\_Curricoli\\_Digitali.pdf](https://www.istruzione.it/scuola_digitale/allegati/2016/Allegato_1Avviso_Curricoli_Digitali.pdf)
- [https://digcompedu.cnr.it/DigCompEdu\\_ITA\\_FINAL\\_CNR-ITD.pdf](https://digcompedu.cnr.it/DigCompEdu_ITA_FINAL_CNR-ITD.pdf)

---

## 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.

Sarà utile e proficuo utilizzare il KIT didattico in quanto è strutturato nelle 5 aree del syllabo dell'Educazione Civica digitale. È composto di 40 pillole teoriche e 32 schede didattiche che affrontano tematiche come il cyberbullismo, il sexting, la web reputation e molte altre. E' basato sulla metodologia **EAS - Episodi di apprendimento situato** - sviluppata dal CREMIT ed è in grado di offrire al docente un quadro metodologico efficace ed operativo per costruire una lezione, che comprenda al suo interno le diverse dimensioni utili all'apprendimento: **problem setting, learning by doing e learning by reflecting**. E' disegnato sul **framework europeo di riferimento per le competenze digitali DigComp 2.2** in questo modo i docenti, nello svolgimento della singole lezioni, potranno integrare i suggerimenti proposti con il curriculum verticale già utilizzato e con le indicazioni sull'educazione civica digitale che utilizzano lo stesso riferimento.

# 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.

L'Istituto è dotato di un DPO esterno alla scuola, nell'espletamento del suo mandato che informa e fornisce una serie di consulenze all'Istituzione scolastica e ai suoi dipendenti, in merito alla normativa in materia di protezione dei dati personali. Inoltre sorveglia che all'interno della scuola tale normativa venga rispettata. Infine tra i suoi compiti rientra anche l'attività di formazione del personale scolastico e la possibilità di rilasciare pareri e comunque fungere da punto di contatto tra Autorità Garante per la Protezione dei Dati Personali e la comunità scolastica.

---

## 3.2 - Strumenti di comunicazione online (PUA)

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

sensibili di ciascuno, in particolar modo degli alunni e delle alunne.

Il nostro Istituto in ottemperanza con la normativa vigente si attiene al documento P.U.A (Politica di Uso Accettabile) per l'uso di dispositivi mobili a scuola.

L'utilizzo dei device avviene in maniera responsabile e avendo cura sia degli apparati fisici, che dell'integrità dei software in essi installati.

Sulla base di tali presupposti e per motivi di sicurezza, agli utenti è vietato:

- utilizzare i dispositivi per finalità personali o comunque non correlati con attività didattiche o di studio;
- collegare dispositivi esterni (memorie USB, hard disk, ecc.) è possibile solo con l'autorizzazione dei docenti;
- installare e disinstallare i programmi o modificarne le impostazioni;
- copiare, caricare o scaricare musica, film, programmi e qualsiasi altro materiale non legato alla didattica o vincolato da copyright o comunque in conflitto con le norme del codice civile e penale riguardanti il diritto d'autore, la privacy, la divulgazione di materiale offensivo, pedo-pornografico etc....

#### **Accesso al Wi-Fi**

- Nel caso in cui i dispositivi in dotazione all'istituto abbiano accesso alla rete WiFi, le credenziali per l'accesso alla rete sono riservate ai docenti che consentiranno agli alunni l'utilizzo. Tali credenziali devono essere gestite con la massima cautela e riservatezza

#### **Utilizzo degli strumenti di didattica digitale**

- l'accesso alle piattaforme didattiche dell'istituto deve essere consentito esclusivamente previa autenticazione informatica e autorizzazione degli insegnanti.

#### **Registro elettronico**

- L'accesso al registro elettronico viene abilitato per docenti, genitori e studenti tramite credenziali di accesso da custodire con la dovuta diligenza. Il registro elettronico deve essere utilizzato esclusivamente per le finalità istituzionali predeterminate dall'istituto (es. Caricamento e lettura voti, assenze, avvisi, ecc.)

#### **Responsabilità**

- E' fondamentale che gli utenti siano pienamente consapevoli dei rischi a cui si espongono durante l'utilizzo dei dispositivi dell'istituto.
- I docenti sono responsabili dell'utilizzo dei dispositivi informatici e hanno l'obbligo di sorvegliare e responsabilizzare gli studenti e le studentesse rispetto ad un uso consapevole e sicuro.
- Gli utenti non devono lasciare incustoditi i dispositivi informatici e devono provvedere alla disconnessione del proprio account al termine dell'utilizzo.

## 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 nostra comunità scolastica si affaccia volentieri all'eventualità di aprire un dialogo sul cosiddetto BYOND "Bring your own device" (Porta il tuo dispositivo a scuola) e riflettere appunto sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti dell'utilizzo dei dispositivi elettronici personali (tablet e computer, così come stabilito dalla normativa vigente del ministro Giuseppe Valditara) durante le attività didattiche. Considerando anche sia gli aspetti positivi che le eventuali criticità per la didattica; affinché ciò avvenga occorre la collaborazione tra la scuola digitale, le famiglie e gli enti locali. Nell'approcciarsi a questa nuova idea di didattica seguirà le indicazioni di indirizzo MIUR, collaborerà con l'AGID e il Garante per la Privacy e svilupperà apposite linee guida che garantiscano sicurezza ed efficacia.

### Link di riferimento

- Presentazione <https://prezi.com/view/HNXf66xL1jx7Cv4sF3PM/>
- Alcune app per poter sfruttare le potenzialità dei dispositivi: <http://www.edutopia.org/blog/the-epic-byod-toolchest-vicki-davis>
- BYOD in classe. Una lezione sulla crisi del '29: <https://www.youtube.com/watch?v=J2Y4iPKhTuQ>

### Allegati.

- [Decalogo Device Piano d'Azioni 6 - PNSD](#)

## 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 minore 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.

Vigilare sulla comunità scolastica e attenzionare i casi di sospetto o conclamato bullismo o cyberbullismo che si verificano in essa, sono compiti dell'intera collettività educante; per aiutare gli alunni e le alunne a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola prevede alcuni strumenti di segnalazione ad hoc:

- un indirizzo e-mail del docente Referente: [saferinternetscuolamascolo@gmail.com](mailto:saferinternetscuolamascolo@gmail.com);
- una casella/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- eventuale sportello di ascolto da supporto per alunni e genitori.

Inoltre, gli alunni e le alunne possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Creare un ambiente sicuro che garantisca il benessere psicofisico di ognuno è fondamentale per cui occorre una corretta informazione/formazione e una sensibilizzazione di tutti gli adulti coinvolti e l'utilizzo di tutti i possibili strumenti di comunicazione, con l'obiettivo di condividere e rendere informata tutta la comunità scolastica. Tale comunicazione può essere condivisa attraverso assemblee scolastiche, collegio docenti, il sito della scuola o anche tramite la stampa e l'affissione di locandine all'interno e all'esterno della scuola stessa.

L'obiettivo è che tutta la comunità scolastica sia informata di questa procedura. In questo modo tutti i soggetti presente nell'Istituto possano osservare ciò che accade nelle dinamiche interpersonali, così da poter agire immediatamente nei confronti di atti non opportuni e in modo tale da poter scongiurare conseguenze a lungo termine ben più gravi, in quanto negative per il benessere e la crescita armonica dei minori coinvolti.

Il gruppo incaricato della gestione delle segnalazioni e le procedure di intervento nello specifico, è formato dal Dirigente Scolastico, dal responsabile anti bullismo e cyberbullismo, dai servizi e dagli enti del territorio. I servizi e gli enti del territorio vengono coinvolti nel momento in cui la segnalazione fa riferimento a un caso di particolare gravità.

Il Referente per la prevenzione e il contrasto del Bullismo e del Cyberbullismo provvede a raccogliere in modo sistematico e continuativo le segnalazioni in merito a fatti di bullismo. La gestione dei casi rilevati andrà differenziata a seconda della loro gravità: è opportuna la condivisione a livello di Consiglio di Classe di ogni episodio rilevato. Alcuni avvenimenti di lieve rilevanza possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi possono essere affrontati informando il Dirigente Scolastico e convocando genitori e alunno/a per riflettere insieme su quanto accaduto e individuare una strategia comune per affrontarlo e rimediare. Per le situazioni più gravi si informerà il Dirigente Scolastico che, nel caso di reati veri e propri, effettuerà la denuncia all'autorità giudiziaria.

Tale procedura ha lo scopo di indicare le modalità operative per la gestione delle segnalazioni relative agli episodi di bullismo e cyberbullismo che permettano di affrontare e contrastare i due fenomeni.

**Link di riferimento**

- Helpline - Fondazione S.O.S Il Telefono Azzurro ETS [www.azzurro.it](http://www.azzurro.it)
- Clicca e Segnala- Fondazione S.O.S Il Telefono Azzurro ETS <https://azzurro.it/clicca-e-segnala/>
- Stop - It Save the Children Italia ETS <https://stop-it.savethechildren.it/>

### Allegati

- [Leaflet - Telefono Azzurro Poster - Telefono Azzurro Gestione dei Casi.](#)

---

## 4.2 - Quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale (ex [art. 357 c.p.](#)) in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Il Codice Penale Italiano, all'[art. 357](#), definisce il pubblico ufficiale come colui che esercita una "pubblica funzione legislativa, giudiziaria o amministrativa". Questa definizione si estende ai docenti nel momento in cui sono impegnati nell'esercizio delle loro funzioni all'interno degli istituti scolastici.

La Corte di Cassazione, con la sentenza [n. 15367/2014](#), ha ribadito la qualifica di pubblico ufficiale per l'insegnante, estendendo tale riconoscimento non solo alla tenuta delle lezioni, ma anche a tutte le attività connesse. Questo include, ad esempio, gli incontri con i genitori degli allievi.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite da un team di docenti composto da:

1. Dirigente
2. Docente referente,
3. L'animatore digitale (secondo il Piano Nazionale per la Scuola Digitale, abbreviato in PNSD, introdotto dalla Legge 107/2015)
4. Referente bullismo (ex. Legge Italiana Contro il Cyberbullismo, l. 71/2017)
5. Altri docenti già impegnati nelle attività di promozione dell'educazione civica.

Le situazioni di pregiudizio presunto o reale possono richiedere il supporto e l'intervento di esperti esterni alla scuola.

**Come descritto nelle procedure di questa sezione, si potrebbero palesare due macro - casi:**

**CASO A (SOSPETTO)** - Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente. La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, il Dirigente e i docenti coinvolti procedono alla valutazione del caso (valutare l'invio o meno della relazione agli organi giudiziari preposti) e agiscono tramite percorsi di sensibilizzazione.

**CASO B (EVIDENZA)** - Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente. La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, si procede alla valutazione approfondita e alla verifica di quanto segnalato, avviando (se appurato la rilevanza penale) la procedura giudiziaria con denuncia all'autorità giudiziaria per attivare un procedimento penale.

Qualora si rilevasse un fatto riconducibile alla fattispecie di reato, l'insegnante - nel ruolo di pubblico ufficiale - non deve procedere con indagini di accertamento ma ha sempre l'obbligo di segnalare l'evento all'autorità giudiziaria. (ex. l. 71/2017). Con autorità competente si intendono:

- Procure Ordinarie: nel caso in cui il minore/i sia la vittima/e e il presunto autore del reato sia maggiorenne,
- Procura Minorile: in caso il presunto autore del reato sia minorenni.

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

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

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

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

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

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

### **Strumenti a disposizione di studenti/esse**

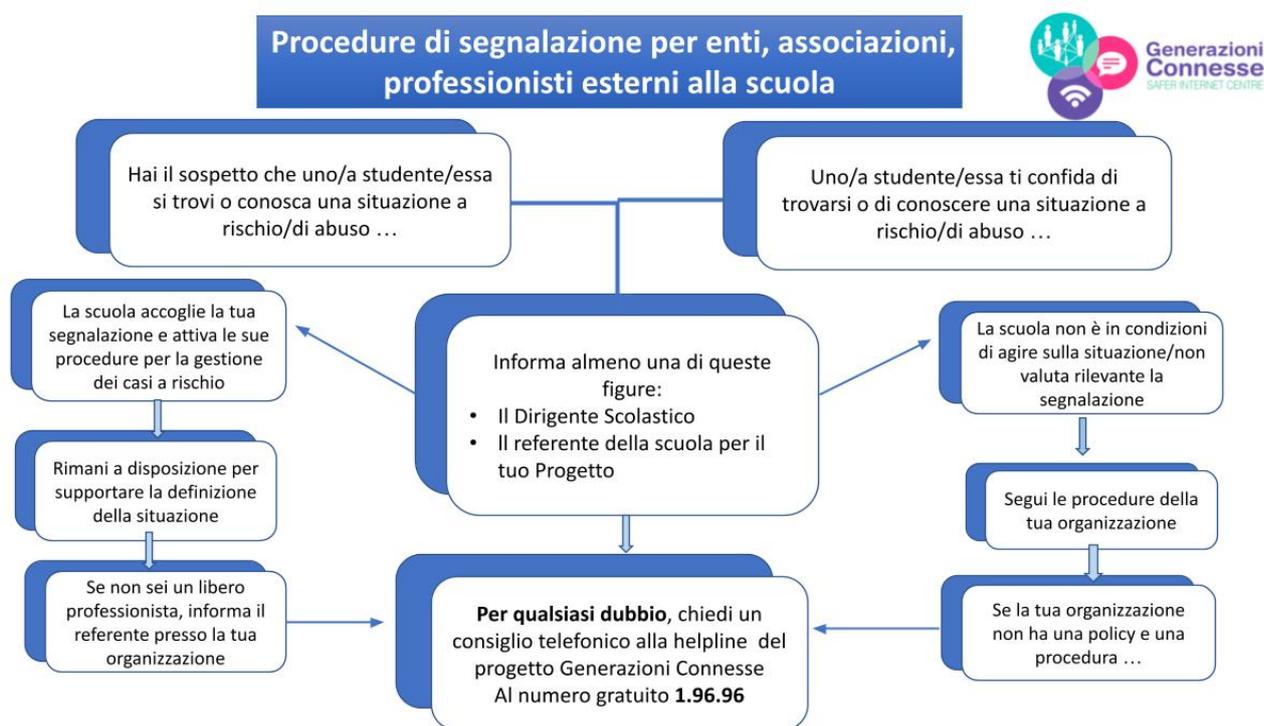
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono

testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola; sportello di ascolto con professionisti; docente referente per le segnalazioni.

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

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

## Procedure



## Procedure interne: cosa fare in caso di evidenza di Cyberbullismo



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

Se non è già stato fatto, avvisa il referente per il cyberbullismo (e/o il team antibullismo) che attiva le procedure ("Corso 4" della piattaforma ELISA) e il Dirigente Scolastico.  
Ricordare sempre che in base alla legge 71-2017:

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

Il DS (e/o il team antibullismo):

- informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto) su quanto accade e condivide informazioni e strategie.
- Informa i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy)
- Attiva il consiglio di classe.

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

### NELLE CLASSI

Il team antibullismo collabora coi docenti della classe per realizzare l'intervento nella classe: a seconda della situazione valuta se

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

A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla Polizia Postale:

a) contenuto; b) modalità di diffusione.

Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).

## Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



Il docente riceve una segnalazione (da un genitore, un altro studente ...) o sospetta che stia accadendo qualcosa a uno/a studente/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

Condividi con il referente o al team antibullismo: si attiva il processo di attenzione e valutazione a cura del referente.

- Insieme si valuta se è il caso
- di avvisare il consiglio di classe;
  - di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.

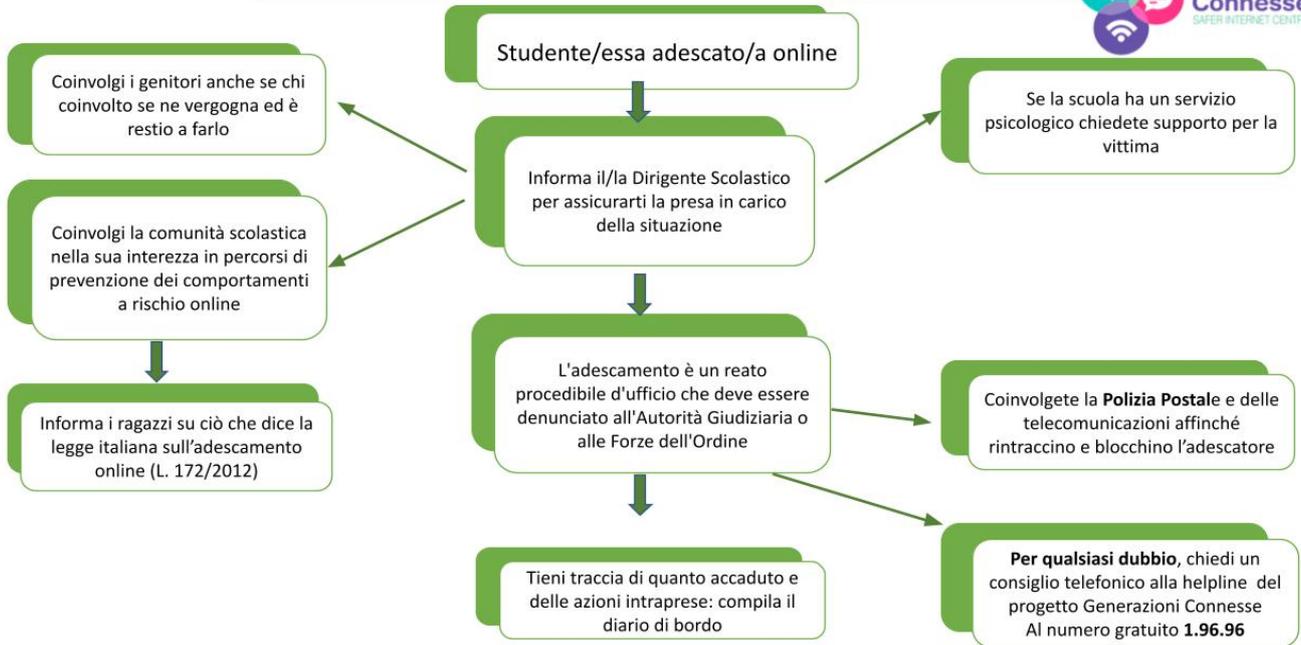
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

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

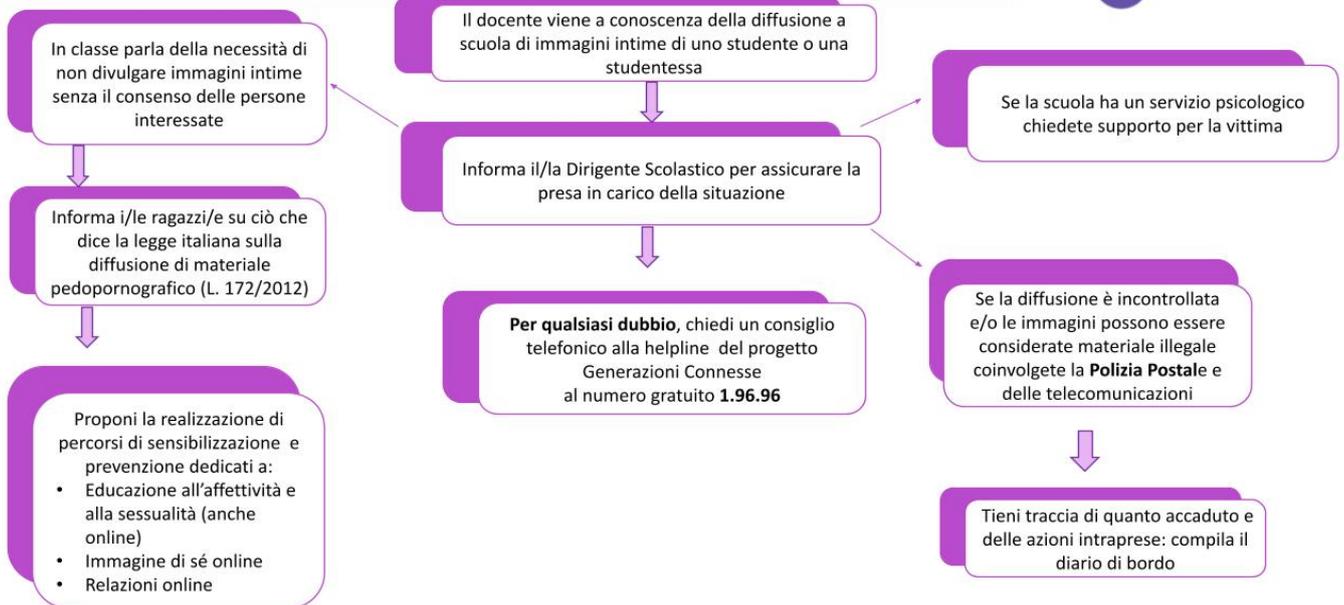
**Se emergono evidenze passa allo schema successivo**

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

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



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



E' stato più volte ribadito che per affrontare i rischi collegati all'uso di tecnologie digitali l'Istituto si avvale di un team specializzato. Questo team include il docente referente, l'animatore digitale come definito dal piano nazionale per la scuola digitale e dal referente bullismo e cyberbullismo. L'animatore digitale è incaricato di promuovere l'uso consapevole e positivo delle tecnologie digitali fungendo così da punto di riferimento per studenti, studentesse e colleghi.

Il referente per il bullismo, come da legge 71 del 2017, ha il compito di affrontare e prevenire situazioni di bullismo e di cyberbullismo garantendo così un supporto e un intervento tempestivo. E' fondamentale nel momento cui ci si rapporti con un caso di particolare gravità far riferimento all'intervento di esperti esterni. L' approccio multidisciplinare assicura che la scuola possa fornire effettivamente un supporto completo e specializzato attingendo anche a conoscenze e competenze esterne.

Un esempio è l'Helpline del Telefono Azzurro, un servizio gratuito telefonico che può offrire aiuto anche a docenti e insegnanti in caso di situazioni di particolare gravità o dubbi.

Se un docente sospetta che all'interno della sua classe si stia verificando un episodio di cyberbullismo, di sexting o di adescamento online è cruciale che intervenga tempestivamente segnalando il sospetto, in modo dettagliato scritto al referente per il cyberbullismo o al team di docenti specializzati.

Questo team, una volta raccolta appunto tale segnalazione, la discute e la condivide con il dirigente scolastico. Insieme si valuta attentamente il caso e si decide eventualmente se è necessario coinvolgere organi giudiziari o di pianificare azioni di sensibilizzazione mirate.

Si farà riferimento ad esperti esterni qualora il caso sia di particolare delicatezza e complessità. Questi professionisti con la loro esperienza specifica possono fornire consulenza, supporto psicologico o legale e contribuire a una gestione efficace del caso facendo in modo quindi che ogni azione sia intrapresa con la massima attenzione e competenza. Indipendentemente dall'esito di questa valutazione di questo caso la scuola può valutare di avvalersi di percorsi di sensibilizzazione per educare gli studenti sull'importanza del rispetto reciproco della sicurezza online, della prevenzione del cyberbullismo e del bullismo coinvolgendo così tutta l'intera comunità scolastica in un dialogo costruttivo.