

I.I.S. - "MARIANO IV D'ARBOREA" - OR  
Prot. 0006638 del 15/04/2025  
IV (Uscita)



## Documento di ePolicy

# I.I.S. "MARIANO IV D'ARBOREA"

VIA MESSINA N. 19 - 09170 - ORISTANO  
Oristano (OR) - Sardegna  
Data di approvazione: 15/04/2025 - 12:16

# 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.

### **Premessa**

L'Istituto di Istruzione Superiore Mariano IV d'Arborea di Oristano si impegna a promuovere un ambiente scolastico sicuro, inclusivo e responsabile, adottando misure per prevenire e contrastare fenomeni di bullismo e cyberbullismo. Il documento di E-Policy, redatto in conformità alle linee guida della piattaforma Generazioni Connesse, persegue i seguenti obiettivi di carattere generale:

- Prevenire e contrastare il bullismo e il cyberbullismo;
- Promuovere l'uso consapevole e responsabile delle tecnologie digitali;
- Favorire la collaborazione tra scuola, famiglie e comunità;
- Definire ruoli e responsabilità di tutti i soggetti coinvolti.

Per perseguire gli obiettivi sopra indicati, una funzione chiave è attribuita alle Tecnologie dell'Informazione e della Comunicazione (TIC) che rappresentano, infatti, strumenti fondamentali nel processo di apprendimento degli studenti e delle studentesse e rivestono anche un ruolo educativo rilevante.

Le Competenze Digitali sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle competenze per l'apprendimento permanente e, considerando il contesto sociale ed educativo attuale, sempre più complesso, risulta di particolare importanza per ogni Istituto scolastico, la necessità di redigere un documento programmatico, quale quello della ePolicy, volto a promuovere le competenze digitali, stimolando un uso positivo e consapevole delle tecnologie, sia da parte dei ragazzi e ragazze, che da parte degli adulti coinvolti nel processo educativo (Raccomandazione del Consiglio Europeo- 22 maggio 2018).

Una maggiore Competenza digitale, infatti, avrebbe il risultato di prevenire situazioni problematiche, facilitare il riconoscimento, la gestione e il monitoraggio di episodi legati ad un uso scorretto degli strumenti tecnologici che potrebbero essere, o diventare, situazioni di emergenza.

Attraverso la redazione del documento di ePolicy il nostro Istituto vuole, da un lato realizzare uno strumento operativo a cui tutti i soggetti coinvolti, alunni, alunne e adulti appartenenti alla comunità educante potranno fare riferimento per un uso consapevole ed efficace della tecnologia, dall'altro, programmare specifiche azioni di educazione e formazione riguardo alle opportunità e ai rischi connessi all'uso della rete e delle tecnologie in generale. Inoltre, poiché come emerge dalle Linee di Orientamento per azioni di prevenzione e contrasto al Bullismo e Cyberbullismo, nota 2519,15/04/2015, e infine la legge n°71 del 2017 recante "Disposizioni a tutela dei minori per la prevenzione e il contrasto del bullismo e cyberbullismo", per il successo di queste azioni e la effettiva promozione del benessere nella comunità scolastica è decisiva la collaborazione tra scuola, famiglia ed enti territoriali, il presente documento elaborato nell'ambito del progetto "Generazioni Connesse" si prefigge l'obiettivo di coinvolgere tutte le componenti della comunità scolastica: il personale della scuola, gli alunni e le alunne, le famiglie e, quando necessario, esperti eventualmente appartenenti ad enti territoriali, con l'intento di definire l'insieme dei regolamenti, linee di azione e attività da porre in essere per facilitare e promuovere l'utilizzo delle TIC nella

didattica e attraverso lo sviluppo delle competenze digitali determinare anche una prevenzione rispetto ai rischi delle tecnologie digitali.

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

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

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

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

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

### IL DIRIGENTE SCOLASTICO

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

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

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

L'animatore digitale e il Team per l'Innovazione digitale sono co-responsabili, con il referente ePolicy, dell'attuazione dei piani di azione in particolare in riferimento alla formazione dei docenti. Sono inoltre responsabili del controllo all'accesso da parte degli studenti delle Tic

## **IL REFERENTE PER IL BULLISMO E CYBERBULLISMO**

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

## **IL TEAM ANTIBULLISMO E PER L'EMERGENZA**

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

### **Il Team ha il compito di:**

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

## **I/LE DOCENTI**

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

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

Referente per il Cyberbullismo e Bullismo e al Consiglio di Classe per definire strategie di intervento condivise.

## **RESPONSABILE DELLA PROTEZIONE DEI DATI**

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

## **IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)**

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

## **GLI STUDENTI E LE STUDENTESSE**

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

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

## **I GENITORI/ADULTI DI RIFERIMENTO**

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

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

## **GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI**

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

problematiche e ad assicurarne la tempestiva individuazione e presa in carico.

## **Il Dirigente scolastico**

Il ruolo del Dirigente Scolastico è quello primario di garantire l'attuazione della ePolicy attraverso diverse strategie e azioni precise quali:

- 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, eventualmente integrandola ed inserendola nelle misure di sicurezza più generali dell'intero Istituto;
- fornire sistemi per un uso sicuro delle TIC, internet, i suoi strumenti ed ambienti e garantire alla popolazione scolastica la sicurezza di navigazione tramite internet utilizzando adeguati sistemi informatici e filtri;
- assumere la responsabilità della gestione dei dati e della sicurezza delle informazioni e garantire che l'Istituto adotti delle buone pratiche nella gestione dei dati stessi;
- tutelare la scuola e garantire agli utenti la sicurezza di navigazione utilizzando adeguati sistemi informatici e servizi di filtri Internet;
- promuovere per il personale scolastico, docente e non, una formazione adeguata sulla sicurezza online perché ciascuno sia tutelato nell'esercizio del proprio ruolo;
- garantire adeguate valutazioni di rischio nell'usare strumenti e le TIC, effettuate in modo che comunque quanto programmato possa soddisfare le istanze educative e didattiche dichiarate nel PTOF di Istituto;
- promuovere la realizzazione di un sistema che assicuri il monitoraggio e il controllo interno della sicurezza online in collaborazione con le figure di sistema;
- conoscere e attuare le procedure necessarie in caso di grave incidente di sicurezza online.

## **Animatore Digitale e Team per l'Innovazione Digitale**

All'interno dell'Istituto non è al momento presente un Animatore Digitale designato ma il ruolo viene svolto da docenti collaboratori a vario titolo con la Dirigenza. L'individuazione e la nomina di un Animatore Digitale e di un Team per l'Innovazione Digitale sono obiettivi prossimi per l'Istituto. Tali figure saranno co-responsabili, con il referente ePolicy, dell'attuazione dei piani di azione con particolare riferimento agli aspetti e alle azioni relative alla formazione di docenti e personale scolastico primariamente. Saranno inoltre responsabili del monitoraggio e della verifica di un accesso adeguato alle TIC da parte degli studenti e studentesse.

## **Referente per il bullismo e cyberbullismo**

Il Referente per il bullismo e cyberbullismo coordina le attività di prevenzione, contrasto, intervento e monitoraggio di eventuali casi segnalati. Questa attività, una volta che siano definiti i membri del Team per l'Innovazione Digitale/Team ePolicy e l'Animatore Digitale, sarà svolta in collaborazione per garantire una efficace e coordinata attuazione dei piani di azione previsti. Il referente, nella sua azione, si avvale della collaborazione di partner esterni alla scuola come ad esempio Servizi Sociali, Forze dell'ordine, centri di aggregazione giovanile del territorio, associazioni sportive e figure di riferimento come esperti del settore (pedagogisti e psicologi). Coordina inoltre la valutazione, la gestione e il monitoraggio dei casi eventualmente segnalati.

## **Team antibullismo e per l'emergenza**

All'interno dell'Istituto non è al momento presente un Team antibullismo e per l'emergenza ma il ruolo viene svolto dai due docenti referenti e da altri docenti che collaborano a vario titolo con i referenti e con la Dirigenza. La nomina e l'adeguata formazione di un Team antibullismo e per l'emergenza sono obiettivi prossimi per l'Istituto. Tale gruppo di lavoro opererà 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) e avrà il compito di coadiuvare il Dirigente Scolastico nella definizione degli interventi di prevenzione e nella gestione dei casi eventualmente segnalati di bullismo e cyberbullismo. Avrà inoltre il compito di promuovere la conoscenza delle dinamiche tipiche di questi fenomeni negli studenti e studentesse, nei genitori, nel personale scolastico e negli adulti appartenenti alla comunità educante, allo scopo di stimolare una maggiore consapevolezza dei fattori protettivi e di rischio relativi. Avrà infine il ruolo chiave di assicurarsi che tutta la comunità scolastica sia pienamente informata della esistenza del team, della presenza e del ruolo dei docenti referenti, delle modalità di segnalazione di casi e delle procedure stabilite per la gestione e il monitoraggio di questi, in modo che chiunque possa far riferimento con fiducia, nel caso di situazioni che necessitino di una richiesta di attenzione, o semplicemente per avere informazioni sul tema. Unitamente a queste attività, promuoverà la redazione e l'applicazione della ePolicy e il monitoraggio di eventuali segnalazioni.

## **Docenti**

I/le docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Tale ruolo si esplica mediante diverse azioni:

- In ottica di cittadinanza digitale, integrano la propria disciplina con approfondimenti, promuovendo l'uso delle tecnologie digitali nella didattica;
- accompagnano e supportano 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
- Sensibilizzano gli studenti informandoli sui rischi legati alla condivisione di informazioni personali, immagini mediante dispositivi tecnologici e li aiutano a riconoscere siti, applicazioni o comportamenti potenzialmente dannosi.
- Promuovono un uso consapevole della rete e degli strumenti informatici
- Monitorano eventuali comportamenti a rischio e segnalano al Dirigente Scolastico, al referente o al team (secondo le modalità previste dall'Istituto) qualunque problematica, violazione o abuso, anche online, che veda coinvolti studenti e studentesse dandone tempestiva comunicazione per definire strategie di intervento condivise.

## **Responsabile della protezione dei dati**

Il Responsabile della protezione dei dati (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

## **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.

## **Studenti e 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, rispettando le regole di convivenza digitale e segnalando, quando necessario, episodi di bullismo e cyberbullismo nella maniera adeguata. 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 studenti e delle studentesse, inoltre, sono informati del documento di ePolicy e invitati a costruire i piani di azione utili per la promozione del benessere e l'uso consapevole delle TIC.

### **Famiglie: genitori e adulti di riferimento**

I Genitori, in continuità con l'Istituto scolastico con il quale collaborano attivamente, 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. A tal fine, l'Istituto si propone di promuovere il coinvolgimento dei rappresentanti di genitori/adulti di riferimento all'interno del percorso di definizione e implementazione dell'ePolicy.

### **Enti esterni pubblici e privati - associazioni**

Enti esterni pubblici e privati, il mondo dell'associazionismo, in particolare le associazioni sportive, Forze dell'Ordine, psicologi e pedagogisti collaborano attivamente con l'Istituto scolastico per la promozione del benessere, l'adozione di buone pratiche che riguardano l'uso delle tecnologie e il mantenimento di un ambiente positivo e protettivo contro i fenomeni di bullismo e cyberbullismo. In quest'ottica, collaboreranno alla realizzazione di iniziative con carattere formativo, educativo e di sensibilizzazione, rivolte non solo agli alunni ma all'intera comunità scolastica, in linea con quanto indicato nel documento di ePolicy.

---

## **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.

In occasione del nuovo aggiornamento del PTOF e dei regolamenti di Istituto, compreso quello di disciplina, che si sta realizzando in questo momento, il documento ePolicy verrà integrato con essi. All'integrazione di tali documenti e alla disseminazione delle informazioni riportate in essi verrà dato risalto e rilevanza adeguata in modo che tutta la comunità scolastica sia edotta sulla loro esistenza, sul loro ruolo e sulle procedure e principi in essi riportati.

---

## 1.4 Condivisione e comunicazione dell'ePolicy

**Il paragrafo dettaglia i seguenti aspetti:**

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

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

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

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

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

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

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

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

A tal fine l'adozione dell'ePolicy è comunicata all'USR di riferimento e al Municipio (servizi istruzione e servizi sociali) attraverso gli allegati sintetici progettati che indicano gli elementi del documento e le prospettive per la comunità.

A seguito della redazione del documento ePolicy, esso verrà condiviso con tutta la comunità scolastica in modo che ciascuno sia informato, non soltanto della esistenza dello stesso, ma anche dei suoi contenuti con particolare attenzione alle procedure e principi in esso riportati. Al centro del processo di divulgazione ci saranno, ragionevolmente, gli studenti e le studentesse per i quali saranno sottolineati i compiti, le funzioni e le attività reciproche. Il documento ePolicy verrà inoltre condiviso con il personale, docente e non docente afferente alla scuola in modo che ciascuno possa utilizzarlo come base per formarsi e per applicare le indicazioni utili al raggiungimento degli obiettivi in esso contenuti. Essenziale per la condivisione, anche con le famiglie e eventuali altri adulti con ruolo educativo associati, sarà la pubblicazione del documento sul sito istituzionale della scuola, unitamente agli altri documenti relativi ai regolamenti e al patto di corresponsabilità. Il documento sarà approvato dal collegio docenti e dal consiglio d'Istituto. Le norme adottate e sottoscritte dalla scuola in materia di sicurezza e utilizzo delle tecnologie digitali e l'ePolicy verranno pubblicate sul sito web della scuola.

---

## 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 monitoraggio e l'eventuale aggiornamento del documento verranno affidati al Dirigente Scolastico il quale si avvarrà per tale scopo del contributo dei docenti e collaboratori che si occupano della gestione della tecnologia nell'Istituto e, in futuro, costituiranno il Team digitale (con la designazione di un Animatore Digitale); ruolo chiave in queste attività sarà svolto anche dai referenti per il bullismo e cyberbullismo e dai docenti che apparterranno al team per le emergenze, unitamente ad altri membri appartenenti alla comunità scolastica.

L'I.I.S. Mariano IV d'Arborea si prefigge di sviluppare a partire dall'anno scolastico 2024-2025 e nel corso dei 3 anni successivi i seguenti obiettivi:

- Realizzazione di un evento di presentazione del documento ePolicy ai docenti
- Realizzazione di un evento di presentazione del documento agli studenti/e e alle famiglie
- Organizzare uno o più incontri di sensibilizzazione sui rischi online e utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/e
- Realizzazione di iniziative formative e informative sull'uso delle tecnologie e di prevenzione ai fenomeni di bullismo e cyberbullismo con il coinvolgimento di figure esperte
- Pianificazione e realizzazione di progetti sulla Peer Education sulle tematiche della sicurezza online
- Organizzazione nella scuola di laboratori sull'educazione alle relazioni e alle emozioni rivolto agli studenti/e
- Diffusione del documento negli ambienti scolastici, tra studenti, personale scolastico e componente genitoriale.

---

## 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 fornite dalla piattaforma Generazioni Connesse saranno utilizzate a scopo formativo, informativo, divulgativo in linea con gli obiettivi in esse individuati.

## Cap 2 - Sensibilizzazione e prevenzione

---

### 2.1 - Sensibilizzazione e prevenzione

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

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

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

L'utilizzo delle tecnologie nei vari ambiti della vita degli studenti ha un notevole impatto sulla loro quotidianità: non si parla più di "essere on line" ma sarebbe più adeguato dire che i ragazzi vivono una realtà "on life".

Un così diffuso utilizzo determina anche un rilevante rischio associato.

Questo si configura come la possibilità per il minore di commettere azioni online che possano danneggiare se stessi o altri, essere vittima diretta o indiretta di tali azioni, agire come spettatore di azioni lesive.

Oltre alle tutele già messe in atto da parte degli enti deputati alla vigilanza in questo settore, è di fondamentale importanza che il minore sia in grado di riconoscere questi fenomeni e saperli distinguere tra loro, individuare eventuali situazioni o comportamenti di allarme e possa, di conseguenza, saper adottare le strategie migliori da utilizzare in primis per proteggere se stesso e, altrettanto, per arginare tali situazioni, contenerle e soprattutto prevenirle.

E' importante che gli alunni/e abbiano gli strumenti idonei per riconoscere possibili situazioni di rischio e segnalarle ad un adulto di riferimento.

Risulta evidente pertanto come gli interventi di sensibilizzazione e prevenzione giochino un ruolo cruciale per ridurre fenomeni o situazioni di rischio.

Nel caso della sensibilizzazione si tratta di azioni e interventi che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno) ma anche illustrare le possibili soluzioni o i comportamenti da adottare. Attività di sensibilizzazione dovrebbero raggiungere il maggior numero di persone possibili ed coinvolgere tutta la comunità scolastica.

Diverse azioni di sensibilizzazione sono già state condotte e il nostro Istituto si prefigge di ampliare ulteriormente questo tipo di interventi coinvolgendo anche altre istituzioni ed enti del territorio, nonché figure professionali di riferimento nel settore. Sarà di fondamentale importanza la formazione di un gruppo di alunni come peer educators.

Nel caso della prevenzione, si tratta di un insieme di attività, azioni e interventi attuati con lo scopo di promuovere le competenze digitali, allo scopo di evitare l'insorgenza dei rischi legati all'utilizzo delle tecnologie digitali e quindi ridurre i rischi per la sicurezza degli studenti e studentesse, unitamente alle azioni di promozione del benessere psicologico e delle relazioni positive.

## 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 la formulazione del Curriculum di educazione alla Cittadinanza Digitale, previsto per gli alunni, il nostro Istituto utilizzerà come traccia per programmare e sviluppare gli interventi formativi, quanto indicato nel documento ePolicy. Nell'anno scolastico 2024-2025, sfruttando quanto previsto dai percorsi finanziati dalla Regione Sardegna nell'ambito del progetto "PROGRESSI - progetti per il recupero e il supporto agli studenti nell'innovazione", sono stati realizzati nel nostro Istituto diversi interventi rivolti agli alunni e al personale docente. Tali interventi sono stati calibrati sulla base di una antecedente ricognizione dei bisogni della scuola ed hanno avuto lo scopo di formare i docenti sull'innovazione tecnologica mentre quelli dedicati agli alunni, seppur con lo stesso intento formativo, sono stati realizzati perseguendo anche uno scopo educativo e di sensibilizzazione all'utilizzo consapevole e corretto delle tecnologie, specialmente per promuovere il benessere dei ragazzi e prevenire fenomeni di bullismo e cyberbullismo. In linea con quanto già realizzato e con quanto indicato nell'ePolicy, il nostro Istituto porterà avanti anche nel prossimo futuro percorsi volti a promuovere le competenze digitali, la formazione e l'educazione su queste tematiche che permetterà così la progettazione e la compilazione di un curriculum digitale.

Tali percorsi, unitamente agli obiettivi relativi e al dettaglio delle competenze previste saranno nel prossimo futuro parte integrante del PTOF e includeranno competenze relative a:

- **Dimensione Tecnologica:** in particolare con lo stimolo alla riflessione sul potenziale delle tecnologie digitali come STRUMENTI per la risoluzione di problemi quotidiani, onde evitare automatismi che abbiano conseguenze incerte, attraverso una adeguata comprensione delle regole dello strumento
- **Dimensione Cognitiva:** in particolare con l'attenzione sulla capacità di cercare informazioni in Rete in modo adeguato, utilizzarle in maniera proficua, valutare con spirito critico e senso di responsabilità la loro eventuale condivisione, saperne valutare la credibilità e affidabilità.
- **Dimensione Etica e Sociale:** in particolare con riferimento alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui, usando le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri; inoltre, questa competenza si declina nella promozione dello sviluppo di particolari attività di tipo sociocomunicativo e partecipativo al fine dell'acquisizione di una consapevolezza adeguata sui diritti e doveri personali, relativi alla comunicazione online.

Nella realizzazione di tutti gli interventi, l'Istituto farà riferimento al quadro normativo previsto dal Piano Nazionale Scuola Digitale (PNSD).

## 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.

Nella realizzazione di tutti gli interventi formativi ed educativi previsti del presente documento ePolicy e in quelli che saranno delineati, programmati e realizzati nel prossimo futuro, l'Istituto si avvarrà di utili strumenti messi a disposizione da Istituzioni, Enti e Associazioni. In particolare, il Kit Didattico fornito dalla piattaforma Generazioni Connesse sarà una base solida di partenza per la realizzazione di numerosi interventi.

# 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.

Prendendo in considerazione quanto riportato sul sito del Garante della Privacy, nel quale si sottolinea il ruolo cruciale delle scuole nell'educazione e formazione dei giovani primariamente al rispetto dei valori fondanti di una società e, in riferimento all'uso delle tecnologie digitali come nuove forme di comunicazione, al rispetto dei diritti come la riservatezza e la dignità della persona, il nostro Istituto ritiene di fondamentale importanza dedicare energie, risorse e tempo agli interventi di formazione di docenti e alunni sul corretto uso di questi strumenti. Gli stessi sono infatti imprescindibili ausili per la didattica e possono essere considerati degli importanti facilitatori nei processi di inclusione, in particolare per integrare, sviluppare e potenziare i diversi stili di apprendimento e lo spettro dei bisogni di apprendimento dei diversi studenti. Un utilizzo adeguato da parte dei docenti costituisce un modello positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti. E' da segnalare, inoltre, che il PNSD promuove e valorizza il buon uso delle TIC nella didattica, estendendo il concetto di scuola da luogo fisico a spazio di apprendimento virtuale.

In un ambiente di apprendimento così delineato, risulta ancora più essenziale la necessità di tutelare adeguatamente i dati personali degli utenti coinvolti nel processo educativo e formativo. In linea con questa necessità rilevante, il nostro istituto fa riferimento alla normativa vigente, in particolare al regolamento( UE) 2016/6797, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. In tale ottica l'Istituto promuove percorsi formativi per tutta la comunità scolastica sul tema dell'uso consapevole delle tecnologie digitali e sulla prevenzione di rischi online.

Tutti i modelli per le informative relative all'utilizzo dei dati personali sono disponibili sul sito della scuola e vengono fornite agli interessati, corredate di un'adeguata spiegazione, quando necessario. Ad esempio, al momento dell'iscrizione, viene sottoposto ai genitori degli alunni, o a chi ne esercita la potestà genitoriale, la liberatoria relativa ad un eventuale utilizzo di immagini a scopo didattico-istituzionale.

Per quanto riguarda l'utilizzo dei dispositivi informatici e l'accesso ad internet a scopo didattico, si fa riferimento a quanto indicato nell'art.2 della dichiarazione dei diritti ad Internet, elaborata dalla commissione costituita il 27 ottobre 2014 presso

la Camera dei Deputati.

In tale dichiarazione, l'accesso a Internet viene indicato come un diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale e che questo accesso deve essere operato in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale, poiché le Istituzioni Pubbliche sono tenute a promuovere e garantire il superamento di ogni forma di divario, tra i quali anche quello digitale, potenzialmente determinato dal genere, dalle condizioni economiche, o situazioni di vulnerabilità personale e disabilità; in linea con tali considerazioni, il nostro Istituto si impegna a promuovere e garantire questo diritto con azioni mirate sulla base delle necessità dei diversi utenti.

Per le norme di accesso ad internet e l'utilizzo di dispositivi, strumenti informatici e delle TIC in generale, si rimanda al Regolamento di Istituto e al Patto di Corresponsabilità già elaborati e alle loro future modifiche.

---

## 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.

Come indicato nei paragrafi precedenti, l'utilizzo di strumenti, dispositivi e tecnologie digitali è diventato imprescindibile per le attività didattiche e per costruire ambienti di apprendimento sempre più inclusivi ed efficaci che integrino le strategie didattiche tradizionali con quelle più recenti. Un ambiente di apprendimento così dinamico e flessibile promuove la comunicazione, la collaborazione e lo sviluppo delle soft skills che risultano essenziali nella società liquida attuale.

Gli strumenti di comunicazione interna nel nostro Istituto possono essere così riassunti:

- Registro elettronico (ARGO/ DIDUP) con funzionalità dedicate ai diversi utenti (alunni, famiglia e docenti)
- Sito web della scuola
- Account mail Istituzionale G-SUITE for edu per Alunni/e e Docenti con dominio @marianoquarto.edu.it
- Piattaforma G-SUITE for education ed in particolare gli applicativi: Classroom, Drive, Calendar, Meet

Per quanto riguarda le chat informali fra colleghi, fra docenti e genitori e alunni non esiste una vera e propria regolamentazione e si rimanda a principi di correttezza, educazione e rispetto basati sul "buon senso".

## 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.

Per questa tematica si rimanda al regolamento d'Istituto già esistente che disciplina l'uso dei dispositivi personali in classe a seconda dei vari usi anche in considerazione del fatto che il BYOD già a partire dall'anno scolastico 2015/16 rientrava nelle priorità del Piano Nazionale Scuola Digitale.

## 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.

La segnalazione dei casi relativi all'uso improprio delle tecnologie digitali è un aspetto fondamentale, specialmente per un'istituzione scolastica e per la comunità educante in generale. Il nostro Istituto sta elaborando un piano di azione strutturato in cui siano coinvolte diverse figure professionali sia interne che esterne anche al fine di definire una procedura condivisa che renda il più efficiente e funzionale possibile il processo di segnalazione, gestione e monitoraggio dei casi degni di attenzione. Tale protocollo sarà inserito come già indicato nei regolamenti di Istituto e ad esso sarà data un'adeguata visibilità in modo che tutta la comunità scolastica possa trarne il relativo beneficio.

In linea con questo possiamo indicare come problematiche degne di segnalazione quelle collegate ai seguenti aspetti:

#### **- Cyberbullismo**

La legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo", nell'art.1 comma 2, definisce il cyberbullismo come:

"Qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti online aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso o la loro messa in ridicolo".

La stessa legge e le relative linee di Orientamento per la prevenzione e il contrasto del cyberbullismo indicano i ruoli, le responsabilità e azioni utili nella gestione dei casi sopra indicati.

Ruolo fondamentale nelle suddette linee guida è attribuito ai seguenti aspetti:

- Formazione del personale scolastico, e in particolare di un referente per ogni autonomia scolastica
- Sviluppo delle competenze digitali da inserire tra gli obiettivi formativi prioritari (L.107-2015)
- Promozione di un ruolo attivo degli studenti e ex studenti in attività di peer education su questi temi: interventi che prevedano l'educazione tra pari si sono dimostrati di estrema efficacia in numerosi studi scientifici
- Elaborazione e previsione di misure a sostegno e rieducazione dei minori coinvolti, eventualmente con la partecipazione di enti e figure professionali anche esterne alla scuola
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti al bullismo e cyberbullismo con la chiara indicazione di eventuali relative sanzioni disciplinari commisurate alla gravità degli atti compiuti.
- Nomina di un Referente e costituzione di un Team per le emergenze che sia adeguatamente formato e possa coordinare le varie attività relative.

#### **- Hate speech**

Il fenomeno di "incitamento all'odio" o "discorso d'odio" indica discorsi, (post, immagini, commenti) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "Hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale e di disabilità) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo sempre più diffuso, richiede l'attenzione anche delle Istituzioni scolastiche che possono intervenire per prevenirlo e contrastarlo promuovendo il dialogo educativo e il benessere nella comunità scolastica con

alcune strategie tra cui:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di incitamento all'odio in particolare legati alla razza, al genere, orientamento sessuale e disabilità
- promuovere la partecipazione civica e l'impegno anche attraverso i media digitali e i social network
- favorire una presa di parola consapevole e costruttiva da parte dei giovani

#### **- Dipendenza da Internet e gioco online**

La dipendenza da internet e gioco on line, al pari di altri comportamenti patologici associabili a fenomeni da dipendenza, è frequentemente caratterizzato da isolamento sociale, problematiche che si evidenziano anche a livello scolastico, sia da un punto di vista del rendimento scolastico che della disciplina, che si associano spesso a sintomi da astinenza e irrefrenabile necessità di utilizzo della rete. In merito a problematiche di questo tipo, la scuola svolge un ruolo educativo e formativo che può sensibilizzare i diversi utenti, promuovendone il benessere e riducendo così eventuali fattori di rischio. Azioni che l'Istituto ha già intrapreso in passato e intende incrementare ulteriormente in ottica preventiva comprendono:

- Azioni di sensibilizzazione che coinvolgano con esperti in materia (ad esempio psicologi, Forze dell'Ordine)
- Incontri formativi sull'utilizzo sicuro della rete e sui rischi online

#### **- Sexting**

Il Sexting è fra i rischi più diffusi, connessi ad un uso poco consapevole della rete.

Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti mediati sessualmente espliciti che possono rientrare, data l'età degli utenti coinvolti, all'interno del fenomeno della pedopornografia. Le conseguenze di un utilizzo improprio di materiale di questo tipo hanno ovviamente rilevanti implicazioni oltre che da un punto di vista legale, anche per quanto riguarda le implicazioni emotive, sociali e personali relative ai protagonisti delle immagini. Anche in questo caso, l'educazione, la formazione e il dialogo educativo, anche con figure professionali esperte di riferimento gioca un ruolo chiave nei meccanismi preventivi e protettivi. Pertanto, il nostro Istituto si impegna a promuovere, sostenere e stimolare qualunque iniziativa formativa in tal senso, ad esempio mediante la realizzazione di attività progettuali e collaborazione con esperti, tra i quali primariamente la Polizia Postale, realizzando interventi dormativi rivolti a tutta la comunità scolastica: docenti, alunni, genitori, personale scolastico.

#### **- Adescamento online**

Adescamento on line o Grooming, (dall'inglese "Groom", curare - prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenzialmente abusanti utilizzano per indurre i minori e potenzialmente vittime a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Azioni di questo tipo sfruttano frequentemente gli strumenti messi a disposizione dalla rete e i luoghi virtuali dove spesso si verificano tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatapp, telegram etc.), i siti e le app di Teen Dating (siti di incontri per adolescenti). L'esito di questi contatti virtuali può risultare poi in contatti dal vivo e può avere, oltre che finalità sessuali, finalità di ricatto di vario genere nei confronti della vittima.

Anche in questo caso, la scuola ha un compito formativo ed educativo rilevante e le strategie da adottare a scopo preventivo e protettivo sono corrispondenti a quelle indicate in precedenza.

#### **- Pedopornografia**

La pedopornografia online è un reato (art.600-ter comma 3 del C.P.) che consiste nel produrre, divulgare, diffondere e pubblicizzare anche per via telematica immagini o video ritraenti minori coinvolti in comportamenti sessualmente espliciti, concreti o simulati, o qualsiasi rappresentazione degli organi sessuali per fini soprattutto sessuali.

La legge n° 269 del 3 agosto del 1998, insieme alle successive modifiche contenute nella legge n°38 del 6 febbraio 2006,

costituiscono una tappa fondamentale nella definizione e predisposizione di strumenti utili per contrastare i fenomeni di sfruttamento sessuale a danno dei minori introducendo anche il "reato di pornografia minorile virtuale" (artt 600 ter e 600 quater C.P) che si verifica quando il materiale pedopornografico rappresenta immagini relative a minori, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Il tema della pedopornografia è estremamente delicato e in quanto tale deve essere trattato con le dovute cure, utilizzando un linguaggio e modalità adeguati alla maturità, anche in considerazione della fascia di età, degli utenti. Anche in questo caso, la scuola si propone di attivare azioni di sensibilizzazione, educazione e formazione su questi temi, rivolte a tutta la comunità scolastica, sfruttando oltre che la collaborazione di enti e professionisti specializzati, anche promuovendo i servizi di "Generazioni Connesse".

---

## 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.

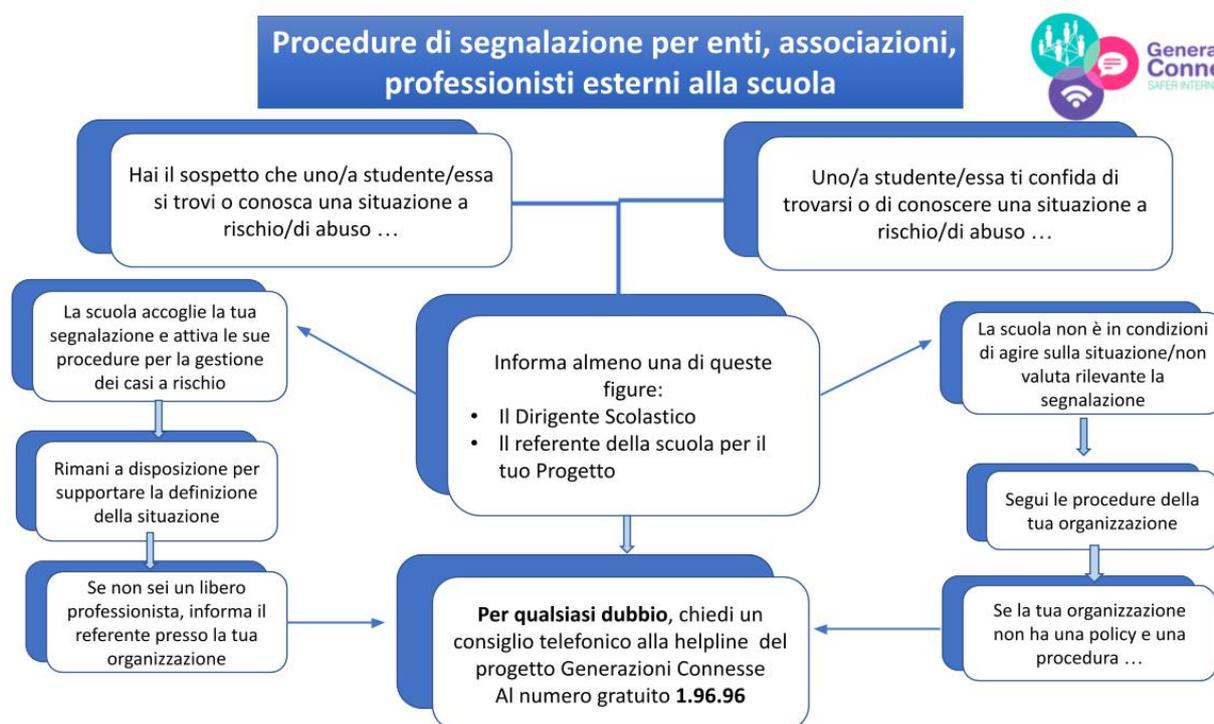
### **Strumenti a disposizione di studenti/esse**

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 condividete informazioni e strategie.
- Informa i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy)
- Attiva il consiglio di classe.

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.

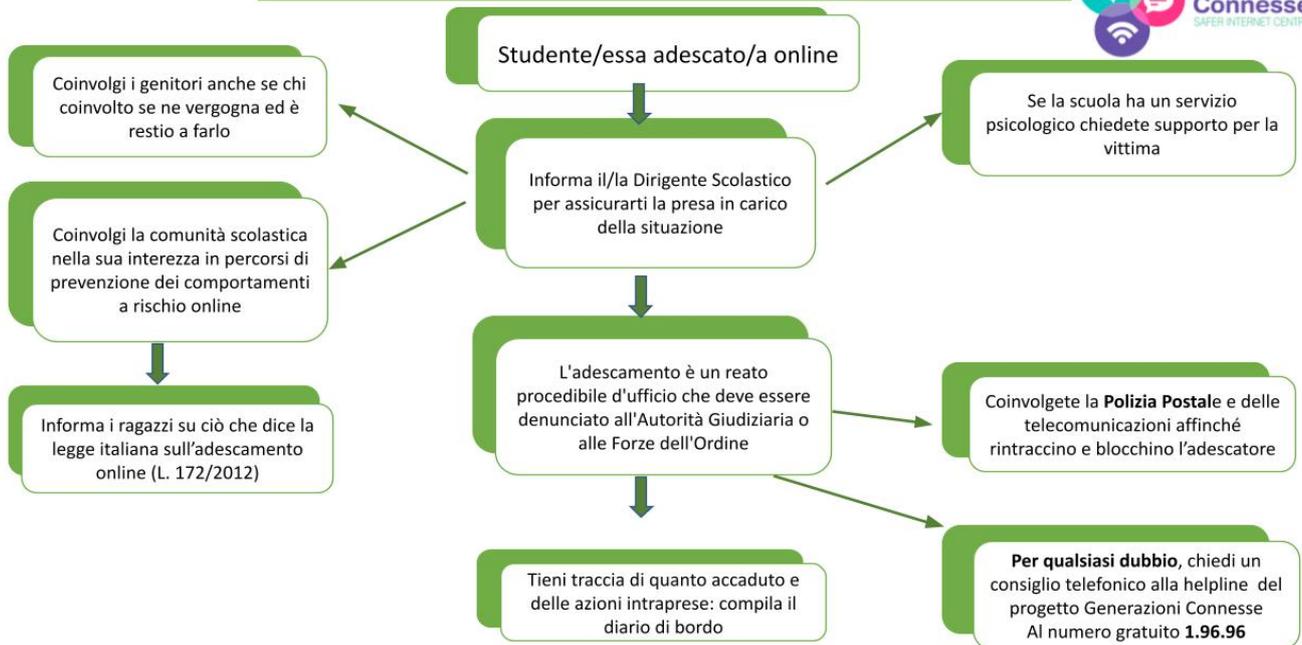
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

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

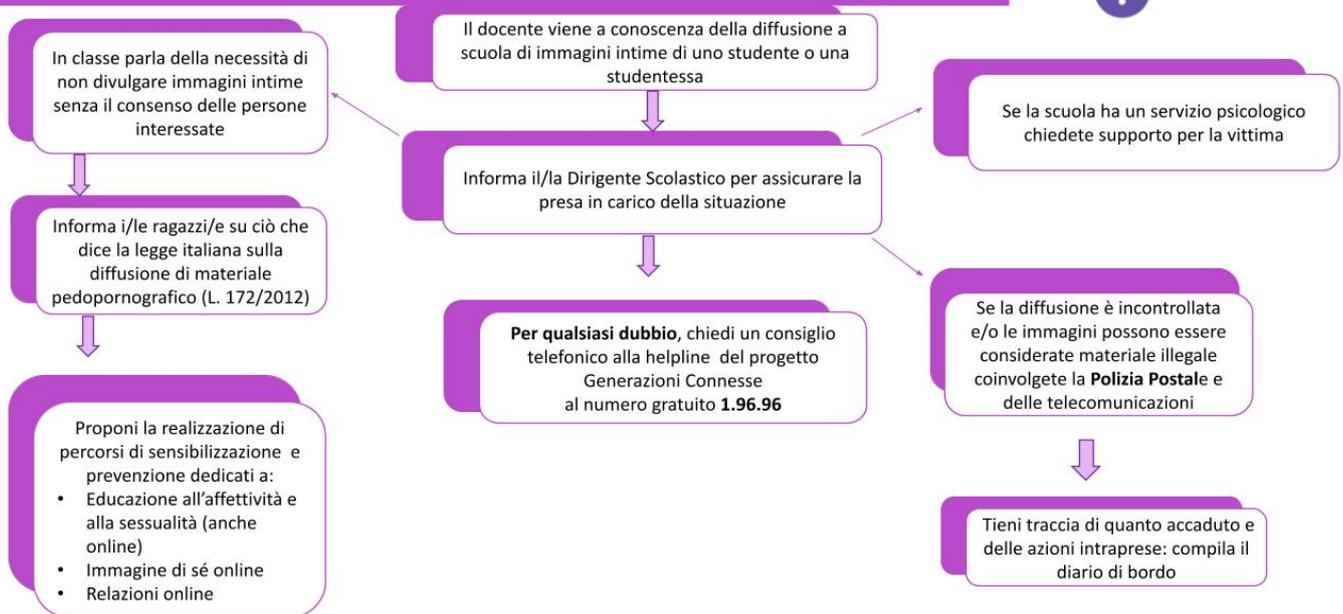
**Se emergono evidenze passa allo schema successivo**

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 aggiunta alle attività di sensibilizzazione, educazione e formazione con scopo preventivo e protettivo, già indicate nelle precedenti sezioni, la scuola si impegna nell'arco dei prossimi tempi di definire, attivare, diffondere e monitorare un sistema di segnalazione adeguato ed efficiente. La segnalazione di eventi o situazioni potenzialmente rilevanti è infatti un aspetto cruciale per l'integrazione delle diverse azioni e l'efficacia delle strategie.

A seguito della designazione del Team per le emergenze, l'Istituto si propone, oltre che l'integrazione e l'aggiornamento dei vari regolamenti di Istituto, anche la predisposizione di adeguati sistemi di segnalazione che possono essere di seguito riassunti:

- Modulo di segnalazione adeguatamente strutturato, versatile, semplice da compilare e adeguatamente informativo per la segnalazione degli eventuali casi rilevanti, anche riferiti a problematiche differenti
- Indirizzo mail ufficiale e specifico per le segnalazioni o per la richiesta di informazioni, utile per tutta la comunità scolastica
- Scatola Box per la raccolta di segnalazioni anonime inserita in un' area strategica dell'Istituto
- Sportello di ascolto con personale qualificato come psicologo e/o pedagogo.

A seguito della segnalazione, il Team per le emergenze prenderà in carico il caso e ne effettuerà una gestione secondo le procedure stabilite, tenendo conto anche delle attività di monitoraggio da mettere in atto a seguito della gestione dei singoli casi.

Alle procedure relative alle modalità di gestione e monitoraggio delle segnalazioni e dei singoli casi sarà data opportuna visibilità e le stesse saranno comunicate e condivise con tutta la comunità scolastica in modo che ciascuno sia opportunamente informato e possa contare sul supporto delle figure di riferimento, in ogni condizione necessaria.

Poiché a seguito di alcune segnalazioni potrebbe rendersi necessario l'intervento o il coinvolgimento di altre figure quali enti o istituzioni, Forze di Polizia (in particolare la Polizia Postale), o altri servizi presenti sul territorio, sarà cruciale effettuare una adeguata mappatura di tali professionalità e prendendo come riferimento per consultazione il Vademecum di "Generazioni Connesse".

Rilevante sarà ovviamente il ruolo di supporto svolto dall'Ufficio Scolastico Regionale il quale promuove continuamente attività di formazione per il personale docente e sostiene attivamente tutte le attività di prevenzione promosse dai diversi Istituti scolastici sui temi di bullismo, cyberbullismo e pericoli della rete.

Il coinvolgimento della Azienda Sanitaria Locale sarà preso in considerazione qualora fosse necessario fornire supporto a ipotetiche vittime coinvolte in situazioni problematiche come precedentemente indicato.

Ruolo cruciale avrà il continuo scambio e confronto con i Servizi Sociali competenti e, qualora si rendesse necessario, con figure afferenti al Tribunale dei Minorenni.