



# Documento di ePolicy

PDIC84700V

IC NOVENTA PADOVANA G.SANTINI

VIA VALMARANA33 - 35027 - NOVENTA PADOVANA - PADOVA (PD)

DANIELA BELLABARBA

PDIC84700V - PDIC84700V - REGISTRO PROTOCOLLO - 0005352 - 29/09/2022 - IV.1 - U

# Capitolo 1 - Introduzione al documento di ePolicy

---

## 1.1 - Scopo dell'ePolicy

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.

Le "competenze digitali" sono fra le abilità chiave all'interno del [Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente](#) e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

## Argomenti del Documento

1. **Presentazione dell'ePolicy**
  1. Scopo dell'ePolicy
  2. Ruoli e responsabilità
  3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
  4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
  5. Gestione delle infrazioni alla ePolicy
  6. Integrazione dell'ePolicy con regolamenti esistenti
  7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
2. **Formazione e curriculum**
  1. Curriculum sulle competenze digitali per gli studenti
  2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
  3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
  4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
  1. Protezione dei dati personali
  2. Accesso ad Internet
  3. Strumenti di comunicazione online
  4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
  1. Sensibilizzazione e prevenzione
  2. Cyberbullismo: che cos'è e come prevenirlo
  3. Hate speech: che cos'è e come prevenirlo
  4. Dipendenza da Internet e gioco online
  5. Sexting
  6. Adescamento online
  7. Pedopornografia
5. **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

## Perché è importante dotarsi di una E-policy?

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi

all'uso di Internet.

L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

---

## 1.2 - Ruoli e responsabilità

Affinché l'E-policy 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.

Nell'ambito di questa ePolicy sono individuati i seguenti ruoli e le principali responsabilità correlate:

IL DIRIGENTE SCOLASTICO:

- È garante della sicurezza, anche online, di tutti i membri della comunità scolastica.
- Promuove la cultura della sicurezza online attivando, con la collaborazione del Referente di Istituto per il bullismo /cyberbullismo, percorsi di formazione per la sicurezza e le problematiche connesse all'utilizzo della RETE sia online che offline.
- Garantisce l'esistenza di un sistema/protocollo per il monitoraggio e il controllo interno della sicurezza online.
- Gestisce e interviene nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali da parte degli studenti e delle studentesse.

L'ANIMATORE DIGITALE:

Con l'inizio dell'a.s. 2022/2023

- Promuove percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" collaborando con la commissione "generazioni connesse".
- Monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola collaborando con la commissione "generazioni connesse".
- Promuove l'utilizzo delle TIC nella didattica in collaborazione con la commissione "generazioni connesse".

**IL REFERENTE BULLISMO E CYBERBULLISMO:**

Con l'inizio dell'a.s. 2022/2023

- Coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e cyberbullismo, avvalendosi anche delle Forze di Polizia, delle associazioni e degli enti territoriali.

**I DOCENTI:**

- Integrano parti del curriculum disciplinare con approfondimenti sull'uso responsabile delle TIC e della RETE.
- Servendosi delle tecnologie digitali nella didattica (LIM o altri dispositivi tecnologici) sviluppano le competenze digitali degli allievi facendo sì che gli stessi conoscano e seguano le norme di sicurezza nell'utilizzo del web sia per attività in presenza sia per attività didattiche extracurricolari.
- Segnalano al Dirigente scolastico e ai suoi collaboratori qualunque violazione, anche online, del Regolamento di Istituto secondo la procedura stabilita e conseguentemente segnalano alle famiglie eventuali problematiche emerse in classe nell'utilizzo del digitale e stabiliscono linee comuni di intervento educativo.

**IL PERSONALE ATA:**

- Svolge funzioni di tipo amministrativo, contabile, gestionale e di sorveglianza, connesse alle attività dell'Istituzione scolastica, in collaborazione con il Dirigente scolastico e con il personale docente tutto.

**STUDENTI E STUDENTESSE:**

- Rispettano le norme che disciplinano l'uso corretto e responsabile delle tecnologie digitali, come indicato nel Regolamento di Istituto.
- Adottano le regole di e-safety per evitare situazioni di rischio per sé e per gli altri.

**I GENITORI:**

- Partecipano alle iniziative di sensibilizzazione e formazione organizzate dall'Istituto sull'uso consapevole delle TIC e della RETE, nonché sull'uso responsabile dei device personali.
- Condividono con i docenti le linee educative relative alle TIC e alla RETE, al Regolamento di Istituto e al patto di corresponsabilità educativa.
- Accettano e condividono il documento di ePolicy dell'Istituto.
- Collaborano con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite.

**GLI ENTI EDUCATIVI ESTERNI E LE ASSOCIAZIONI:**

- Osservano le politiche interne sull'uso consapevole della Rete e delle TIC.
- Attivano procedure e comportamenti sicuri per la protezione degli studenti e delle studentesse durante le attività che vengono svolte all'interno della scuola o in cui sono impegnati gli stessi.

---

### ***1.3 - Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto***

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

**Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.**

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

### ***1.4 - Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica***

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/le studenti/esse) si faccia a sua volta promotore del documento.

L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse,

alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

#### CONDIVISIONE E COMUNICAZIONE DEL DOCUMENTO EPOLICY ALLA COMUNITÀ SCOLASTICA ED AI GENITORI DEGLI STUDENTI E DELLE STUDENTESSE:

Le norme adottate e sottoscritte dalla scuola in materia di sicurezza ed utilizzo delle tecnologie digitali, saranno rese note tramite pubblicazione del presente documento sul sito web della scuola.

#### CONDIVISIONE E COMUNICAZIONE DELLA EPOLICY AGLI STUDENTI E ALLE STUDENTESSE:

- All'inizio dell'anno, in occasione dell'illustrazione del Regolamento di Istituto agli alunni da parte dei docenti, verrà presentata la ePolicy insieme ai regolamenti correlati e al patto di corresponsabilità.
- Tutti gli alunni saranno informati che la rete, l'uso di internet e di ogni dispositivo digitale saranno controllati dai docenti responsabili (infanzia, SP, SSPG) e utilizzati solo con la autorizzazione e supervisione dei docenti curricolari.
- L'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule o laboratori con accesso a internet.
- Sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili, con specifico riferimento al contrasto di ogni forma di cyberbullismo.

#### CONDIVISIONE E COMUNICAZIONE DELLA EPOLICY AL PERSONALE SCOLASTICO:

- Le norme adottate dalla scuola in materia di sicurezza dell'uso del digitale saranno discusse dagli organi collegiali e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito istituzionale.
- Il personale scolastico riceverà un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso partecipazione a incontri formativi organizzati dall'Istituto e materiali resi disponibili sul sito istituzionale.

- Tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

#### CONDIVISIONE E COMUNICAZIONE DELLA EPOLICY AI GENITORI:

- In occasione di incontri scuola- famiglia l'istituto informerà i genitori sull'importanza dell'uso consapevole e sicuro delle TIC e di internet.
- Al fine di sensibilizzare le famiglie sui temi dell'uso delle TIC saranno organizzati incontri informativi per presentare e condividere la presente ePolicy.

La ePolicy, redatta dalla Commissione "Generazione Connesse" e approvata dal collegio Docenti e dal Consiglio di Istituto, sarà inserita all'interno del PTOF.

---

## **1.5 - Gestione delle infrazioni alla ePolicy**

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

#### DISCIPLINA DEGLI ALUNNI:

Le potenziali infrazioni in cui potrebbero incorrere gli alunni, relativamente alla fascia di età considerata, nell'utilizzo delle tecnologie digitali e di internet durante la didattica sono le seguenti:

- Uso della RETE per giudicare, infastidire, offendere, denigrare, impedire a qualcuno di esprimersi o partecipare, esprimersi in modo volgare usando il turpiloquio invio incauto o senza permesso di foto o altri dati personali (indirizzo di casa, numero di telefono).
- Condivisione online di immagini o video di compagni/e e del personale scolastico senza il loro esplicito consenso o che li ritraggono in pose offensive e denigratorie.
- Condivisione di immagini intime e a sfondo sessuale.
- Invio di immagini o video volti all'esclusione di compagni/e.
- Comunicazione incauta e senza permesso con sconosciuti.
- Collegamenti a siti web non adeguati e non indicati dai docenti.

L'azione educativa prevista per gli alunni è rapportata alla fascia di età e al livello di



sviluppo e maturazione personale. Infatti in alcuni casi i comportamenti sanzionabili sono dovuti a fasi critiche transitorie, di cui gli educatori devono tenere conto per il raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno.

Pertanto sono previsti interventi graduali in base all'età e alla gravità delle violazioni:

- Richiamo verbale.
- Richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante).
- Richiamo scritto con annotazione sul registro.
- Convocazione dei genitori da parte dell'insegnante.
- Convocazione dei genitori da parte del Dirigente Scolastico.

Contestualmente sono previsti interventi educativi di rinforzo, anche con l'intervento degli psicologi d'Istituto ("Progetto Cuscino"), rispetto a comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza, di prevenzione e gestione positiva dei conflitti, di conoscenza e gestione delle emozioni.

È inoltre importante intervenire su tutto il contesto classe con attività specifiche educative e di sensibilizzazione.

#### DISCIPLINA DEL PERSONALE SCOLASTICO:

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono diverse e alcune possono determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli allievi:

- Utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di docenza o al profilo professionale.
- Utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale.
- Trattamento dei dati personali e dei dati sensibili degli alunni non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi.
- Diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi.

#### DISCIPLINA DEI GENITORI:

In considerazione dell'età degli studenti e delle studentesse e della loro dipendenza dagli adulti, anche talune condizioni e condotte dei genitori medesimi possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli allievi a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico. Gli atteggiamenti da parte della famiglia meno favorevoli sono:

- La convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non corre rischi.
- Una posizione del computer in una stanza o in una posizione non visibile e

controllabile dall'adulto.

- Una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'uso di cellulare o smartphone.
- Un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei a minori.
- Un utilizzo di cellulari e smartphone in comune con gli adulti che possono conservare in memoria indirizzi di siti o contenuti non idonei a minori.

---

## ***1.6 - Integrazione dell'ePolicy con Regolamenti esistenti***

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

La ePolicy è coerente con quanto stabilito nei Regolamenti vigenti e nel Patto di corresponsabilità.

---

## ***1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento***

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

L'aggiornamento del documento di ePolicy sarà curato dal team "generazioni connesse"

---

## ***Il nostro piano d'azioni***

## IL NOSTRO PIANO D'AZIONI

### AZIONI da svolgere entro 2022/2023:

- Organizzare incontri tra i docenti della commissione “generazioni connesse” volti a presentare il progetto per la stesura finale dell’ePolicy.
- Informare gli studenti/studentesse sui temi dell’epolicy in cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare incontri con specialisti esterni per gli alunni su alcuni temi dell’ePolicy.
- Organizzare incontri con specialisti esterni per i genitori su alcuni temi dell’ePolicy.
- Inserire nel sito della scuola il collegamento alla piattaforma Generazioni Connesse in modo da rendere fruibile il materiale ai docenti dell’istituto, ai genitori degli studenti e agli alunni.
- Presentare ai docenti dell’istituto, ai genitori degli studenti e agli alunni il documento di ePolicy (mediante pubblicazione nel sito o, per gli alunni, in classe)

### AZIONI da svolgere nei prossimi 3 anni:

- Organizzare uno o più incontri volti a monitorare la necessità di integrare il documento dell’ePolicy.
- Informare gli studenti/studentesse sui temi dell’ePolicy in cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare incontri con specialisti esterni per gli alunni su alcuni temi dell’ePolicy.
- Organizzare incontri con specialisti esterni per i genitori su alcuni temi dell’ePolicy.
- Inserire nel sito della scuola il collegamento alla piattaforma Generazioni Connesse in modo da rendere fruibile il materiale ai docenti dell’istituto, ai genitori degli studenti e agli alunni.
- Presentare ai docenti dell’istituto, ai genitori degli studenti e agli alunni il documento di ePolicy (mediante pubblicazione nel sito o, per gli alunni, in classe).

# Capitolo 2 - Formazione e curriculum

---

## 2.1. Curriculum sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più “intuitivo” ed “agile” rispetto agli adulti, ma non per questo sono dotati di maggiori “competenze digitali”.

Infatti, “la competenza digitale presuppone l’interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l’alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l’alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l’essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico” ([“Raccomandazione del Consiglio europeo relativa alla competenze chiave per l’apprendimento permanente”](#), C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curriculum digitale.

Le finalità formative delle TIC possono essere sintetizzate nei seguenti punti:

- Favorire la conoscenza dello strumento pc e/o tablet a scopo didattico.
- Sostenere l'alfabetizzazione informatica.
- Favorire la trasversalità delle discipline.
- Facilitare il processo di apprendimento.
- Favorire il processo di inclusione.
- Fornire nuovi strumenti a supporto dell'attività didattica.
- Promuovere situazioni collaborative di lavoro e di studio.
- Sviluppare creatività e capacità di lavorare in gruppo.
- Promuovere azioni di cittadinanza attiva.
- Utilizzare in modo critico, consapevole e collaborativo la tecnologia.

## ***2.2 - Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica***

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

Il Collegio docenti riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola, sia quelle liberamente scelte dai docenti (anche online) purché restino coerenti con il piano di formazione, come meglio indicato nel PTOF.

L'attenzione all'uso delle TIC nella didattica rende gli apprendimenti più motivanti, coinvolgenti ed inclusivi, con una funzione di guida da parte del docente; inoltre, permette di sviluppare capacità che sono sempre più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza ed il confronto fra pari in modalità asincrona.

La competenza digitale -oggi- è imprescindibile sia per i docenti sia per gli studenti e per le studentesse, e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa ed in grado di venire incontro ai nuovi stili di apprendimento.

---

## ***2.3 - Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali***

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del

territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

I percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali, della prevenzione dei rischi online e delle tecnologie digitali per la didattica, avverrà tramite specifici momenti di aggiornamento definiti e organizzati con il supporto della commissione "generazioni connesse".

I momenti di formazione ed aggiornamento sono dunque formulati secondo un'analisi del fabbisogno formativo del corpo docente sull'utilizzo ed integrazione delle TIC nella didattica.

---

## **2.4. - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità**

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

### **Il nostro piano d'azioni**

#### IL NOSTRO PIANO DI AZIONI

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023):

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi)

- Effettuare un'analisi del fabbisogno formativo di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

PDIC84700V - PDIC84700V - REGISTRO PROTOCOLLO - 0005352 - 29/09/2022 - IV.1 - U

# Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT della e nella scuola

---

## 3.1 - Protezione dei dati personali

*“Le scuole sono chiamate ogni giorno ad affrontare la sfida più difficile, quella di educare le nuove generazioni non solo alla conoscenza di nozioni basilari e alla trasmissione del sapere, ma soprattutto al rispetto dei valori fondanti di una società. Nell'era di Internet e in presenza di nuove forme di comunicazione questo compito diventa ancora più cruciale. È importante riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino”.*

(cfr. <http://www.garanteprivacy.it/scuola>).

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il “corretto trattamento dei dati personali” a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni.

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre.

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare



riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori. A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali.

## 3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola".

Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

Affinché la scuola risponda in modo efficace alle nuove esigenze della società contemporanea, occorre conoscere il più possibile l'infrastruttura tecnologica dell'Istituto, in modo da poterla sfruttare e potenziare in modo coerente con le necessità dei docenti e la visione che la scuola ha rispetto all'uso delle ICT. Per questo è necessario coinvolgere l'animatore digitale e il tecnico informatico.

Infatti, la pianificazione che riguarda l'acquisizione, la gestione e il mantenimento dell'infrastruttura e dei device non può essere pensata se non all'interno della strategia che la scuola intende adottare attraverso l'ePolicy. È necessario, dunque, tenere in considerazione due aspetti:

- Lo status quo, cioè la disponibilità attuale di tecnologia nella scuola e come rendere l'infrastruttura sicura, accessibile ma anche funzionante e adatta allo scopo. Per questo può essere utile avviare progetti pilota che permettano una sperimentazione e un acquisto più razionale e dilazionato degli strumenti, raccordandosi sempre con l'animatore digitale.
- L'analisi dei bisogni della scuola (o del plesso), in relazione alle reali esigenze didattiche e agli obiettivi prefissati. Questo permette di pianificare e di cogliere eventuali occasioni che possono presentarsi sotto forma di bandi, donazioni o finanziamenti.

Gli studenti si impegnano a:

- Utilizzare in modo consapevole e corretto la RETE e i dispositivi telematici, nel rispetto della privacy e della dignità propria e altrui.
- Rispettare le consegne dei docenti.
- Non scaricare materiali e software senza autorizzazione.
- Non utilizzare unità removibili personali senza autorizzazione.
- Tenere spenti i device personali se non con l'autorizzazione del docente.
- Segnalare immediatamente materiali inadeguati ai propri insegnanti.

I docenti si impegnano a:

- Utilizzare la RETE nel modo corretto.
- Non utilizzare device personali se non per uso didattico.
- Formare gli studenti all'uso della RETE.
- Dare consegne chiare e definire gli obiettivi delle attività.
- Monitorare l'uso che gli studenti fanno delle tecnologie.

---

### **3.3 - Strumenti di comunicazione online**

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

Strumenti centrali a disposizione dell'istituto per la gestione di assenze, presenze, valutazioni, prenotazioni di incontri e comunicazioni con le famiglie/studenti sono il registro elettronico e alcune risorse della GSuite.

Il registro elettronico permette di gestire la comunicazione con le famiglie, le quali attraverso di esso possono visualizzare molte informazioni utili, interagendo con la scuola, su:

- Andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari).
- Risultati scolastici (voti, documenti di valutazione).
- Udienze (prenotazioni colloqui individuali).
- Eventi (agenda eventi).
- Comunicazione varie (comunicazioni di classe, comunicazioni personali).

---

### **3.4 - Strumentazione personale**

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/le studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente **ePolicy** contiene 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 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 quanto riguarda l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own

device”) il nostro istituto norma solamente l'uso del cellulare attraverso i Regolamenti di Istituto sia per la SP che per la SSPG.

## **Il nostro piano d'azioni**

### IL NOSTRO PIANO D'AZIONI

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023):

- Organizzare uno o più eventi volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali della protezione dei dati personali.
- Organizzare attività volte a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare un evento volto a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi):

- Organizzare uno o più eventi volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali della protezione dei dati personali.
- Organizzare attività volte a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare un evento volto a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Incentivare l'utilizzo delle TIC in ambito scolastico (docenti ed alunni).

PDIC84700V - PDIC84700V - REGISTRO PROTOCOLLO - 0005352 - 29/09/2022 - IV.1 - U

# Capitolo 4 - Rischi on line: conoscere, prevenire e rilevare

---

## 4.1 - Sensibilizzazione e Prevenzione

Il rischio online si configura come la possibilità per il minore di:

- commettere azioni online che possano danneggiare se stessi o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e contenerli, ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. Ciò è possibile lavorando su aspetti di ampio raggio che possano permettere una riduzione dei fattori di rischio e di conseguenza una minore probabilità che i ragazzi si trovino in situazioni non piacevoli. È importante che abbiano gli strumenti idonei per riconoscere possibili situazioni di rischio e segnalarle ad un adulto di riferimento.

Gli strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio si configurano come interventi di **sensibilizzazione e prevenzione**.

- Nel caso della **sensibilizzazione** si tratta di azioni 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.
- Nel caso della **prevenzione** si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.

I comportamenti a rischio possono essere molteplici ma afferiscono, in base alla fascia di età, a fasi critiche transitorie o alla difficoltà di gestione delle dinamiche di relazione con l'altro che possono riguardare diversi aspetti delle relazioni a seconda dell'età (dimensione della socialità, dell'affettività e della sessualità) o ancora, alla difficoltà di riconoscere il limite tra dimensione di legalità ed utilizzo sicuro delle

tecnologie digitali.

Per questo motivo il nostro Istituto negli anni scorsi ha formalizzato un percorso volto a gestire fasi critiche transitorie di gestione di dinamiche complesse, mediante confronto/relazione con il Sé e l'altro, mediante la dimensione dell'empatia e della socialità. Tale attività è gestita sia dagli insegnanti sia dagli psicologi dell'Istituto che progettano percorsi ad hoc per supportare il singolo alunno, gruppi di alunni o l'intera classe. Il nostro istituto si impegna, anche per il futuro, a proporre questo tipo di percorso.

In questo scenario di attività che supportano la crescita dei nostri studenti, da quest'anno si inseriscono incontri gestiti da "Telefono Azzurro" rivolti alle classi terze, quarte e quinte SP, a tutte le classi della SSPG, ai genitori degli alunni e ai docenti. Questi interventi sensibilizzeranno la comunità scolastica ad un uso positivo e consapevole delle TIC, sia in un'ottica di tutela dai rischi potenziali che di valorizzazione delle opportunità esistenti.

---

## 4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

*"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 on line 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 al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;

- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di [cyberbullismo](#) e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
  - Ha il compito di coordinare le iniziative di prevenzione e contrasto del [cyberbullismo](#). A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
  - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Gli atti di cyberbullismo possono essere suddivisi in due gruppi:

- **Diretto:** il bullo utilizza strumenti di messaggistica istantanea come SMS o MMS, che hanno un effetto immediato sulla vittima poiché diretti esclusivamente alla persona.
- **Indiretto:** il bullo fa uso di spazi pubblici della Rete, come Social network, blog o forum, per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima, anche dal punto di vista psicologico.

Indicatori di segnali che può manifestare una potenziale vittima di cyberbullismo sono:

- Appare nervosa quando riceve un messaggio o una notifica.
- Sembra a disagio nell'andare a scuola o finge di essere malata (ha spesso mal di stomaco o mal di testa).
- Cambia comportamento ed atteggiamento in modo repentino.
- Mostra ritrosia nel dare informazioni su ciò che fa online.
- Soprattutto dopo essere stata online, mostra rabbia o si sente depressa.
- Inizia ad utilizzare sempre meno PC e telefono (arrivando ad evitarli).
- Perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva.
- Il suo rendimento scolastico peggiora.

Finalità condivisa tra scuola e famiglia è intervenire preventivamente ed efficacemente, al fine di evitare, arginare ed eliminare possibili manifestazioni di comportamenti antisociali.

---

## ***4.3 - Hate speech: che cos'è e come***

## ***prevenirlo***

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) 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, di disabilità, eccetera) ai danni di una persona o di un gruppo.

**Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:**

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla 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.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

- Valorizzare la dimensione relazionale dei più giovani, sensibilizzandoli verso capacità di analisi e scelta consapevole, fornire agli studenti gli strumenti necessari per riconoscere gli stereotipi su cui spesso si fondano forme di "hate speech", in particolare legati al gruppo etnico/religioso, al genere, all'orientamento sessuale, alla disabilità.
- Promuovere la partecipazione civica e l'impegno sociale, anche attraverso attività che coinvolgono il territorio dove opera la scuola.

La corresponsabilità con la famiglia è fondamentale nell'azione didattico-educativa della scuola, anche per attivare progettazioni complementari con finalità socio-educative. A tal proposito la Dirigente e i docenti del nostro Istituto investono nei colloqui con le famiglie in quanto reputano che la famiglia svolga un ruolo fondamentale di prevenzione.

---

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



La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

*L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale?*

## 4.5 - 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 medialti sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

La Legge 19 luglio 2019 n. 69, all'articolo 10, ha introdotto in Italia il reato di "revenge porn", ossia la diffusione illecita di immagini o di video sessualmente espliciti.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psico-sessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro e depressione.

---

## 4.6 - Adescamento online

Il **grooming** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di **teen dating** (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

**In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies - l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).**

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

Per riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli segnali che possono essere indicatori importanti, per valutare un cambiamento improvviso nel comportamento di un minore:

- Il minore ha conoscenze sessuali non adeguate alla sua età?
- Venite a conoscenza di un certo video o di una foto che circola online o -ancora- il minore ha ricevuto un contenuto (o filmato), ma c'è imbarazzo e preoccupazione nel raccontarvi di più...
- Il minore si isola totalmente e sembra preso solo da una relazione online?
- Ci sono prese in giro e allusioni sessuali verso un bambino/ragazzo in particolare?

Il nostro Istituto nell'anno 2022/23 attiverà per i ragazzi di terza secondaria primo grado percorsi di Educazione dei rischi della rete focalizzando l'attenzione sull'aspetto dell'affettività, al fine di informare ed accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità; questo per aiutarli ad essere più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri.

Inoltre, all'interno dell'Istituto è attivo lo Sportello di Ascolto, al fine di supportare gli studenti e le studentesse in difficoltà.

---

## **4.7 - 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 bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, **concrete o simulate** o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

**La legge n. 269 del 3 agosto 1998** "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella **legge n.**

**38 del 6 febbraio 2006** "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet", segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, 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 bambini/e ed adolescenti, 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.

**Secondo la Legge 172/2012 - Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.**

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito [www.generazioniconnesse.it](http://www.generazioniconnesse.it) alla sezione "Segnala contenuti illegali" (Hotline).

**Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di [Telefono Azzurro](#) e "STOP-IT" di [Save the Children](#).**

## ***Il nostro piano d'azioni***

IL NOSTRO PIANO D'AZIONI

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023):

- Organizzare incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/le studenti/studentesse, con il coinvolgimento di esperti.

- Organizzare incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Integrare lo svolgimento della didattica con attività che prevedano un utilizzo sicuro e consapevole di Internet e delle tecnologie digitali, assicurando la partecipazione attiva degli studenti/studentesse.
- Sensibilizzazione dei genitori e del personale scolastico promuovendo i servizi di Generazioni Connesse;

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi):

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Organizzare incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/le studenti/studentesse, con il coinvolgimento di esperti.
- Organizzare incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Integrare lo svolgimento della didattica con attività che prevedano un utilizzo sicuro e consapevole di Internet e delle tecnologie digitali, assicurando la partecipazione attiva degli studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.
- Sensibilizzazione i genitori e il personale scolastico promuovendo i servizi di Generazioni Connesse

# Capitolo 5 - Segnalazione e gestione dei casi

---

## 5.1. - Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

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. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).

Nelle procedure:

- sono indicate le **figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso.**
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

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.**

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e

studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

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 la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via 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.

## **5.2. - Come segnalare: quali strumenti e a chi**

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

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due 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.
- 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.

Per tutti i dettagli fate riferimento 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.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto

Generazioni Connesse, al numero gratuito [1.96.96](tel:1.96.96).

## COME SEGNALARE

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, il nostro istituto prevede i seguenti strumenti di segnalazione:

- Box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile.
- Sportello di ascolto con professionisti.
- Docente referente per le segnalazioni.

In relazione al CASO A, è opportuno il coinvolgimento del Referente d'Istituto per il contrasto del bullismo e del cyberbullismo, al fine di valutare le possibili strategie d'intervento. Se si ravvisano gli estremi, viene informato il Dirigente scolastico unitamente al Consiglio di classe.

Uno strumento utile per raccogliere informazioni può essere il diario di bordo (allegato alla presente e-Policy): il docente deve cercare di capire se gli episodi sono circoscritti al gruppo o se interessano l'intero Istituto. Operativamente è fondamentale coinvolgere tutti gli studenti e le studentesse, informandoli sui fenomeni e sulle caratteristiche degli stessi, suggerendo di chiedere aiuto se pensano di vivere situazioni, di subire atti identificabili come bullismo o cyberbullismo.

In relazione al CASO B, il docente deve condividere immediatamente quanto osservato con il Referente per il bullismo e il cyberbullismo, al fine di valutare insieme le possibili strategie di intervento. Si avvisa anche il Dirigente Scolastico che convoca il Consiglio di classe. Se non si ravvisano fattispecie di reato, è opportuno:

- Informare i genitori (o chi esercita la responsabilità genitoriale) degli/delle studenti/studentesse direttamente coinvolti/e (qualsiasi ruolo abbiano avuto), se possibile con la presenza di professionisti dell'aiuto, per strategie condivise e modalità di supporto.
- Creare momenti di confronto costruttivo in classe, con la presenza di figure specialistiche Territoriali.
- Informare i genitori degli/delle studenti/studentesse 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).
- Informare gli/le studenti/studentesse ultra 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).



- Convocare il consiglio di classe.
- Valutare come coinvolgere gli operatori scolastici su quello che sta accadendo.

A seconda della situazione e delle valutazioni effettuate con Referente, Dirigente e genitori, si potrebbe poi segnalare alla Polizia Postale -ove necessario ai sensi di legge:

1. contenuto del materiale online offensivo;
2. modalità di diffusione;
3. fattispecie di reato eventuale.

Se è opportuno, richiedere un sostegno ai servizi e alle associazioni territoriali o ad altre autorità competenti (pensiamo al cyberbullismo, con il suo impatto sulla vita quotidiana della vittima, la quale sa che i contenuti lesivi sono online, diffusi fra molte persone conosciute e non, in un circuito temporale senza fine e senza barriere spaziali).

È bene sempre dialogare con la classe, attraverso interventi educativi specifici, cercando di sensibilizzare studenti e studentesse sulla necessità di non diffondere ulteriormente online i materiali dannosi, ma anzi di segnalarli e bloccarli. Ciò è utile anche per capire il livello di diffusione dell'episodio all'interno dell'Istituto.

---

### 5.3. - *Gli attori sul territorio*

Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Per una mappatura degli indirizzi di tali strutture è possibile consultare il [Vademecum](#) di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

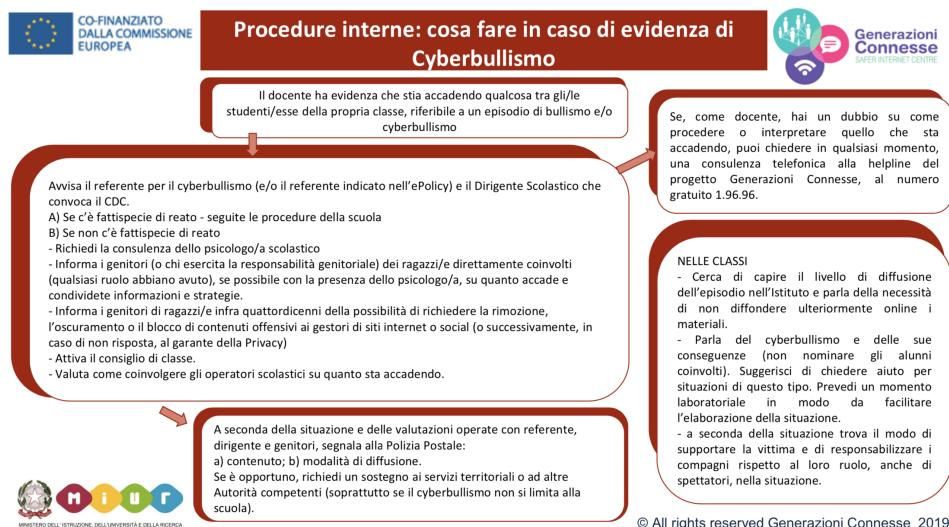
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con

- particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale:** supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
  - **Polizia Postale e delle Comunicazioni:** accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
  - **Aziende Sanitarie Locali:** forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
  - **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico:** segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
  - **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

## 5.4. - Allegati con le procedure

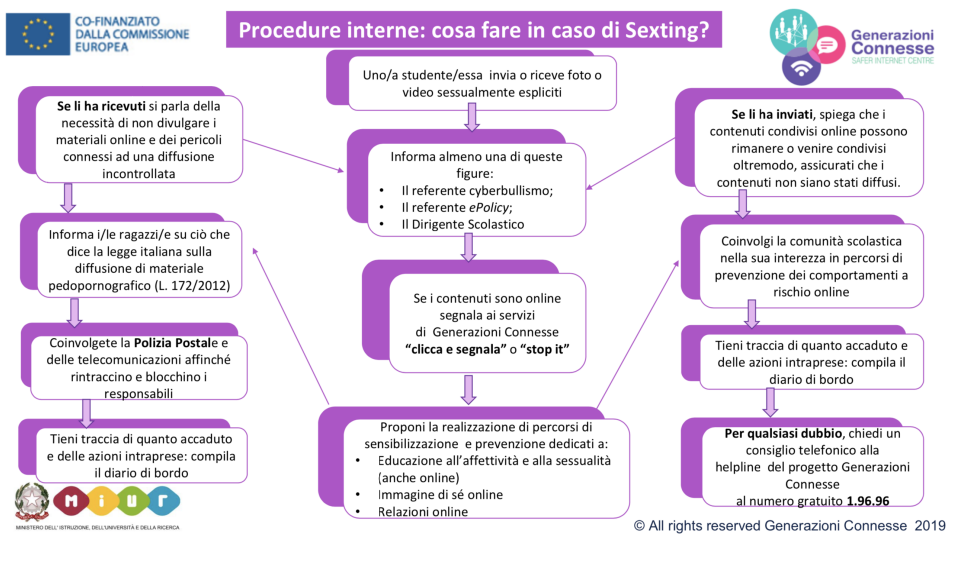
### Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



PDIC84700V - PDIC84700V - REGISTRO PROTOCOLLO - 0005352 - 29/09/2022 - IV.1 - U

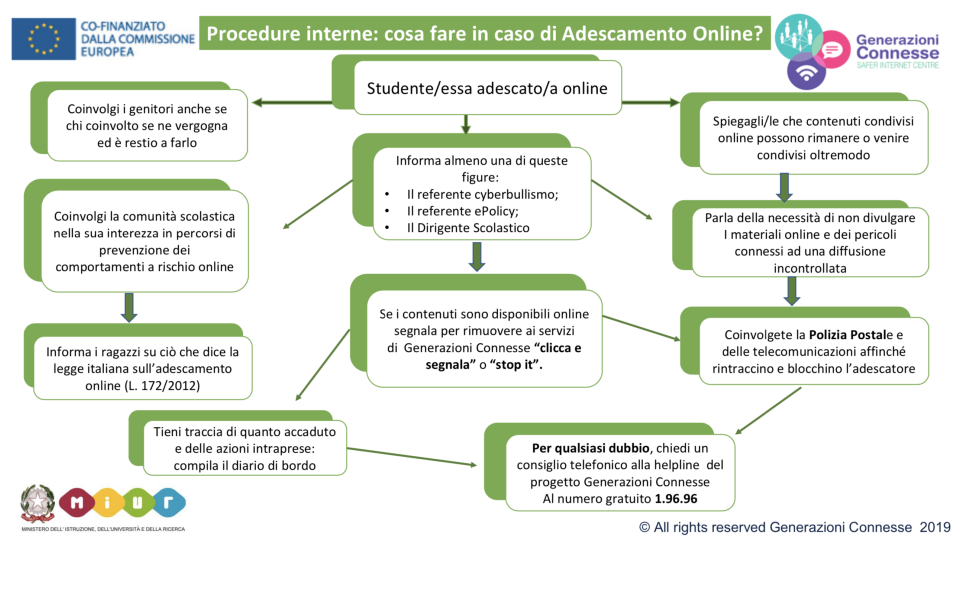


## Procedure interne: cosa fare in caso di sexting?

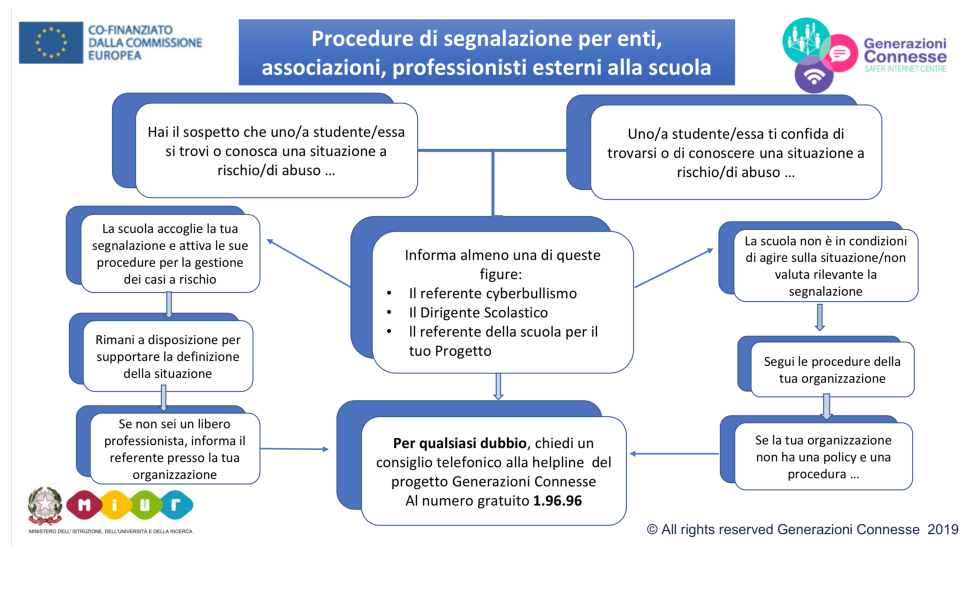


## Procedure interne: cosa fare in caso di adescamento online?

PDIC84700V - PDIC84700V - REGISTRO PROTOCOLLO - 0005352 - 29/09/2022 - IV.1 - U



## Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola



## Altri allegati

- [Scheda di segnalazione](#)
- [Diario di bordo](#)
- [iGloss@ 1.0 l'ABC dei comportamenti devianti online](#)
- [Elenco reati procedibili d'ufficio](#)

## **Il nostro piano d'azioni**

### IL NOSTRO PIANO DI AZIONI

Sulla base delle "Linee guida per l'uso positivo delle tecnologie digitali e della prevenzione dei rischi nelle scuole", vengono assunti i seguenti punti per una collaborazione sinergica tra scuola-famiglia-servizi territoriali, al fine di creare un modello di azioni condivise:

- Coinvolgimento di tutti gli attori della scuola: studenti e studentesse, docenti, genitori e personale ATA, per l'affermazione di un modello di scuola come comunità;
- Interventi educativi ed azioni di supporto, quale prevenzione per eventuali comportamenti a rischio;
- Misure preventive specifiche di tutela anche con l'ausilio di attori territoriali.
- Promozione dell'educazione al rispetto.
- Sviluppo del pensiero critico.
- Promozione dell'Educazione Civica Digitale.

PDIC84700V - PDIC84700V - REGISTRO PROTOCOLLO - 0005352 - 29/09/2022 - IV.1 - U

PDIC84700V - PDIC84700V - REGISTRO PROTOCOLLO - 0005352 - 29/09/2022 - IV.1 - U