



# Documento di ePolicy

---

BAIC82700Q

I.C. "A. ANGIULLI - DE BELLIS"

VIA POERIO 31 - 70013 - CASTELLANA GROTTI - BARLETTA-ANDRIA-TRANI (BA)

Dottor Gerardo Magro

# 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.

### *Il Dirigente Scolastico*

*Il Dirigente Scolastico garantisce, anche online, la sicurezza di tutto il personale della scuola e favorisce la cultura della sicurezza online. Inoltre, in accordo con i referenti dei diversi gradi scolastici alla prevenzione al bullismo e cyber-bullismo, organizza corsi di formazione specifici per un uso consapevole e responsabile delle TIC. Ulteriore compito del Dirigente Scolastico riguarda la gestione attiva di eventuali casi gravi di bullismo e cyber-bullismo.*

### *L'animatore digitale*

*L'animatore digitale offre un supporto al personale scolastico relativo agli aspetti tecnico-informatici, suggerisce modalità di gestione di dati personali nella Rete e informa sui rischi online. Infine si fa promotore della formazione per lo sviluppo delle competenze digitali secondo i bisogni del personale scolastico e verifica l'accesso del personale alla Rete per scopi istituzionali.*

### *Il Referente bullismo e cyber-bullismo*

*Il referente bullismo e cyber-bullismo, nominato sulla base dell'articolo 4 Legge n. 71/2017, coordina e promuove azioni di prevenzione e contrasto al bullismo e cyber-bullismo, anche avvalendosi delle Forze di Polizia, di associazioni ed enti del territorio. Promuove progetti coinvolgendo gruppi di alunni, docenti e genitori.*

### *I docenti*

*I docenti hanno un ruolo fondamentale che afferisce alla formazione di cittadini consapevoli delle opportunità e dei rischi della Rete e quindi devono affiancare nelle attività di didattica digitale gli alunni/e per l'acquisizione di competenze nell'uso della Rete e delle TIC. Inoltre hanno il dovere etico e professionale di segnalare al Dirigente Scolastico o al personale delegato, ogni caso di abuso o violazione che coinvolga i discenti.*

### *Il personale ATA*

*Il personale amministrativo, tecnico ed ausiliario è coinvolto nella responsabilità relativa alla segnalazione di comportamenti non adeguati che potrebbero sfociare in casi di bullismo e cyber-bullismo.*

### *Gli studenti e le studentesse*

*Gli alunni/e devono predisporre all'apprendimento di buone pratiche proposte dalla scuola e dai docenti per un uso corretto e consapevole delle TIC e tutelare la privacy online propria e dei pari. Devono partecipare attivamente alle attività ed eventi proposti dalla scuola e inoltre rendersi*

disponibili nella diffusione di quanto appreso attraverso percorsi di peer education.

#### *I genitori*

*I genitori devono conoscere le buone pratiche relative all'uso consapevole delle TIC e della rete e, in linea con quanto propone l'Istituto, devono promuoverle e avere un ruolo attivo nell'educazione all'uso dei device personali dei propri figli. Essenziale è la collaborazione dei genitori con la scuola e i docenti nella segnalazione di scorrettezze o uso irresponsabile delle tecnologie digitali o Internet non a scopo punitivo, ma esclusivamente educativo.*

#### *Gli Enti educativi esterni e le associazioni*

*Gli Enti educativi esterni e le associazioni hanno il dovere di conoscere e conformarsi alle linee relative all'uso consapevole e responsabile delle tecnologie digitali e della Rete, adottate dalla scuola. Dovere dei professionisti esterni sarà, non solo di fornire la propria competenza professionale, ma anche di assumere e promuovere comportamenti sicuri nel rispetto dei minori garantendo anche la sicurezza online.*

---

## **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).

La scuola a tal fine predispose una informativa per professionisti esterni/Enti esterni che indica:

1. premessa e obiettivi dell'informativa;
2. destinatari;
3. ambito di applicazione;
4. regolamento;
5. procedura per la segnalazione di situazioni a rischio o abusi;
6. provvedimenti per omissione di segnalazione o di violazione del regolamento della scuola.

---

## **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/lle 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.

La nostra scuola intende condividere il Documento di Epolicy con tutta la comunità scolastica attraverso diverse modalità:

1. in maniera ufficiale con la pubblicazione del documento sul sito [www.icangiullidebellis.edu.it](http://www.icangiullidebellis.edu.it) e con la presentazione durante incontri ufficiali ai **genitori**;
2. con la presentazione e la condivisione con gli **organi collegiali scolastici e il personale ATA**;
3. con l'affissione negli ambienti scolastici;
4. con attività di apprendimento-insegnamento rivolte agli **alunni/e**
5. con la produzione da parte di discenti di ordine scolastico superiore di versione child - friendly.

---

## **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.

*La scuola avrà cura di considerare obiettivamente i casi di particolare gravità e valuterà l'intervento e la collaborazione di Forze di polizia postale. **Il fine** ultimo nella gestione delle infrazioni sarà sempre **educativo** e garantirà il giusto supporto psicologico per la persona.*

**Le infrazioni saranno stabilite dopo una attenta analisi della peculiarità dei casi dal gruppo responsabile del contrasto al bullismo e Cyber bullismo.**

---

## **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.

*Tutti i documenti dell'Istituto Comprensivo "Angiulli-De Bellis" sono depositati agli atti e pubblicati sul sito della scuola alla voce Documenti nel box Bullismo e Cyber-bullismo.*

*I documenti sono:*

*Regolamento d'Istituto e Appendice Covid-19;*

*Patto educativo di Corresponsabilità della Scuola dell'Infanzia, della Scuola Primaria e della Scuola Secondaria di Primo Grado.*

---

## **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.

*I due docenti referenti bullismo e cyber dell'Istituto Comprensivo, scelti dal gruppo della Scuola Primaria e della Scuola Secondaria di primo grado, hanno il compito di aggiornare il documento di Epolicy.*

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

---

### **Azioni da svolgere entro un'annualità scolastica:**

- Organizzare un evento che abbia la funzione di presentare il progetto e informare i docenti dell'Istituto della finalità e necessità di diffusione tra alunni del documento dell'ePolicy.
- Organizzare un evento volto a presentare il progetto e il documento ePolicy ai genitori dell'Istituto.
- Organizzare un evento di presentazione del progetto Safer Internet Centre-Generazioni Connesse (SIC) rivolto agli studenti.

### **• Azioni da svolgere nei prossimi 3 anni:**

- Organizzare più eventi volti a informare, presentare il progetto e consultare i docenti dell'Istituto per un monitoraggio sull'uso e sull'efficacia dell'ePolicy.
- Organizzare più incontri per la consultazione degli studenti/studentesse sui temi del bullismo e Cyber-bullismo e presentare attività del progetto Generazioni Connesse e raccogliere eventuali elementi per aggiornare l'ePolicy.
- Organizzare uno o più eventi volti a informare e implementare l'ePolicy e il Progetto di Generazioni Connesse tra genitori.

# 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 competenze digitali e la nostra scuola.**

La nostra scuola rivolge particolare attenzione a tre ambiti delle competenze digitali: tecnologico, cognitivo ed etico-sociale. La padronanza tecnologica deve permettere ai nostri alunni di utilizzare le tecnologie digitali per semplificare il proprio e l'altrui lavoro, per risolvere problemi del quotidiano e per comunicare anche a distanza in tempo reale. L'abilità cognitiva deve puntare all'insegnamento-apprendimento di una ricerca consapevole e critica delle informazioni presenti nella Rete con la finalità di creare materiale personale e innovativo. Inoltre, nella fruizione degli strumenti tecnologici non si può prescindere dalla componente etico-sociale che va implementata nelle nuove generazioni nell'età della formazione affinché diventi accettazione partecipata e responsabile del rispetto della propria ed altrui privacy; del rispetto delle regole di comportamento online (netiquette); della capacità di sapersi difendere da eventuali violazioni sui social network e nella Rete.

La nostra scuola sta avviando l'allestimento di un **blog** affinché si possano raccogliere i bisogni educativi, le curiosità, le esperienze di rete, le riflessioni degli alunni/e e contestualmente effettuare

un intervento mirato e guidato da docenti, teso al raggiungimento di competenze digitali del cittadino dell'era tecnologica.

---

## ***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.

### **La formazione dei docenti nella nostra scuola**

La nostra scuola offre una valida formazione per il raggiungimento di competenze digitali dei propri docenti, con corsi che si avvalgono di professionisti esterni e interni. Inoltre la piena accettazione dell'utilità degli strumenti tecnologici, ha determinato una condivisione tra colleghi delle proprie abilità e competenze digitali. L'uso costante del registro elettronico da parte di tutti i docenti e buona parte dei genitori e alunni, offre una buona opportunità di sperimentazione digitale. Inoltre, la registrazione della nostra scuola alle G Suite for Education nell'anno 2020 sta offrendo nuove possibilità di autoaggiornamento, collaborazione, condivisione e innovazione didattica.

---

## ***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.

**La nostra scuola e la formazione online.**

La nostra scuola offre attraverso il box riservato al "Bullismo e Cyber- Bullismo" presente sul sito ufficiale del nostro Istituto Comprensivo "Angiulli De Bellis", materiale informativo, link di collegamento con la piattaforma Generazioni Connesse per un auto-apprendimento dei docenti. Inoltre aggiorna i docenti sui tempi e le modalità di aggiornamento in presenza e online, offerti da Case Editrici e diverse Aziende di Informatica.

---

## ***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.

L'aggiornamento del Patto Educativo di Corresponsabilità per l'anno scolastico 2020-2021 dà la priorità all'emergenza sanitaria legata alla pandemia da Coronavirus, ma il nostro istituto intende anche progettare un'azione condivisa con organi collegiali in cui sia presente la componente genitoriale per

- condividere regole sull'uso delle tecnologie digitali;
- regolamentare l'uso di comunicazione tra scuola e famiglia per e-mail, whatsApp;
- fornire ai genitori linee guida (presenti sulla Piattaforma di Generazioni Connesse);
- organizzare percorsi di sensibilizzazione e formazione per un uso consapevole della Rete;
- coinvolgere tutte le famiglie.

Dopo tale azione di formazione e condivisione la scuola apporterà ulteriori modifiche e aggiornamenti al Regolamento Scolastico e al Patto educativo di Corresponsabilità con l'obiettivo di costruire una scuola sempre in crescita.

---

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

## **AZIONI da sviluppare nell'arco dell'anno scolastico 2020/2021**

- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per gli studenti incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

## **AZIONI da sviluppare nell'arco dei tre anni scolastici successivi**

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri in modalità blended per alunni/e per l'allestimento di un blog.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

# 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.

### **Protezione dei dati personali a scuola.**

Il nostro Istituto si impegna al rispetto e alla tutela del trattamento dei dati personali di personale scolastico, amministrativo e degli ATA, di genitori e soprattutto alunni/e. Nel particolare la scuola garantisce:

- l'uso di dati utili solo per finalità istituzionali;
- controllo ed eliminazione di dati eccedenti;
- assoluto riserbo di dati sensibili e giudiziari;
- adozione di misure tecniche ed organizzative per garantire la sicurezza;
- controllo del sito istituzionale;
- formazione di docenti sulla normativa relativa alla privacy.

### **Uso delle tecnologie digitali nella nostra scuola.**

L'Istituto Comprensivo "Angiulli-De Bellis" nel plesso della scuola secondaria di primo grado dispone di un'aula 4.0 che offre la possibilità di una rimodulazione continua degli arredi per mettere in atto una didattica per piccoli gruppi, per gruppi classi aperte e verticali. L'aula 4.0 è fornita di dispositivi mobili ( tablet), LIM con monitor interattivo che permette di creare spazi di insegnamento-apprendimento virtuali, aperti e condivisi. L' azione didattica che si intende realizzare in questo ambiente, seppur limitata a piccoli gruppi nel rispetto delle misure di sicurezza sanitarie dell'anno scolastico 2020-21, intende sviluppare nei nostri alunni la creatività attraverso le tecnologie. Infatti strumentazioni quali, macchina fotografica, green scenen (sfondo verde fisico), pannelli riflettenti saranno gli strumenti per poter creare storytelling, foto artistiche ecc.

---

## **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.

### **Diritto di accesso ad internet**

Il nostro Istituto da diversi anni ha espresso la necessità di implementare una didattica digitale, pertanto ha fatto richiesta agli enti territoriali di competenza di attivare in tutti i plessi scolastici la connessione a banda larga che permette l'uso di soluzioni CLOUD. Inoltre tutti gli ambienti scolastici offrono una connessione wireless per i dispositivi del personale scolastico.

La nostra scuola considera l'ambiente online come ambiente fisico e per questo si preoccupa di garantire sicurezza, sia quando gli utenti usano i dispositivi dell'istituto, sia quando usano i propri dispositivi (BYOD). La sicurezza riguarda dunque la parte hardware (fisica) e la parte wireless (rete). La nostra scuola offre anche la possibilità di accesso al Registro Elettronico per un immediato e continuo contatto con i genitori e la possibilità di una didattica digitale con gli alunni/e. Sperimentale è la gestione degli account, rivolta a docenti, assistenti amministrativi e ad un piccolo gruppo di alunni, a cui è stata offerta una registrazione GSuite avente la struttura nome.cognome@icangiullidebellis.edu.it

La nostra scuola per un ottimale fruizione delle tecnologie provvede a:

- periodici interventi di manutenzione anche con supporto di esperti esterni;
- monitoraggio per mezzo di registri di eventuali guasti o anomalie;
- formazione dei docenti e del personale amministrativo.

### **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.

#### **Quali strumenti di comunicazione online usare?**

L'uso degli strumenti di comunicazione online offre grandi opportunità, ma allo stesso tempo potrebbero essere causa di fraintendimenti perchè limita il feedback tangibile e il rapporto empatico. La comunicazione online scolastica può essere di tipo interno ed esterno: la prima tipologia afferisce all'interazione tra docenti, alunni, genitori e personale amministrativo; la seconda invece riguarda la diffusione di informazioni della scuola ai non iscritti, agli enti territoriali e alle associazioni. La comunicazione interna è esplicitata attraverso la fruizione del Registro Elettronico, i social network, le piattaforme di lavoro condivise (Classroom, Drive, Edmodo ecc.) La comunicazione esterna ha l'onere di trasmettere valori, azioni e progetti che la scuola porta avanti, usando come strumenti, il sito della scuola, i profili sui social ( facebook, blog). La nostra scuola si pone l'obiettivo di formare gli alunni/e alla comunicazione e informare gli utenti nel pieno rispetto dell'altro evitando ogni tipo di violazione.

---

### **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.

### **Le nostre regole in linea con le indicazioni del Miur.**

Il Miur in collaborazione con AGID ( Agenzia per il digitale) e il Garante per la Privacy, ha elaborato linee guida per permettere un uso consapevole e responsabile dei propri device a scuola.

La nostra scuola condivide le 10 regole per l'uso dei propri dispositivi a scuola, BYOD ( Bring your own device):

1. Ogni novità determina un cambiamento e quindi un miglioramento;
2. il cambiamento non va rifiutato;
3. la scuola fornisce i servizi necessari per realizzare l'innovazione;
4. il Dirigente Scolastico e i docenti si fanno promotori dell'innovazione digitale;
5. gli strumenti tecnologici sono uno strumento per sviluppare capacità critiche e creative degli alunni/e;
6. l'uso dei dispositivi deve educare all'apprendimento autonomo e permanente;
7. la didattica digitale è gestita dal docente secondo la metodologia e i tempi adeguati ai bisogni educativi del gruppo classe;
8. le tecnologie digitali amplificano gli ambienti di apprendimento perchè consentono una connessione continua con i discenti, pertanto è necessario regolarizzare i tempi e rispettare la sfera pubblica e privata;
9. l'alleanza educativa tra scuola e genitori è una prerogativa per implementare lo sviluppo della didattica digitale;
10. Educare alla cittadinanza digitale è un dovere per la nostra scuola.

**La presente ePolicy, documento programmatico e di indirizzo insieme al Regolamento d'Istituto e al Patto Educativo di Corresponsabilità, viene redatta per consolidare buone pratiche per un corretto uso dei device e per promuovere le competenze di cittadinanza digitale. Si prevede anche un aggiornamento della stessa sulla base di Azioni di diffusione, monitoraggio e condivisione di esperienze digitali.**

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

---

### **Azioni da sviluppare nell'arco dell'anno scolastico 2020/2021.**

- Organizzare un evento online volto a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola: redigere **regolamento uso della tecnologia a scuola.**
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola: **redigere netiquette.**
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti

sull'uso dei dispositivi digitali personali a scuola.

- Organizzare un evento volto a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.

**Azioni da svolgere nel triennio.**

- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity).
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity).

# 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.

## 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).

### **Azioni di prevenzione della scuola**

Gli interventi di sensibilizzazione e prevenzione messi in atto dalla scuola devono essere finalizzati al cambiamento, in particolare è necessario incoraggiare gli alunni ad evitare ogni atteggiamento di silenzio, di osservazione passiva e sottovalutazione delle azioni legate al fenomeno del bullismo e cyber bullismo. La nostra scuola è orientata ad una prevenzione universale per ridurre i rischi e promuovere consapevolezza tra gli alunni/e; prevenzione selettiva per un intervento immediato su una classe che presenta la problematica e prevenzione indicata che riguarda il singolo individuo coinvolto in episodi di bullismo e cyber bullismo. La nostra prevenzione informa, coinvolge e offre soluzioni ai nostri discenti. Come da normativa, nei casi in cui ci si possa trovare di fronte ad una fattispecie di reato (come furto di identità o la persistenza di una condotta persecutoria che mette seriamente a rischio il benessere psico-fisico dell'alunno/a coinvolto/a in qualità di vittima) si farà riferimento agli uffici preposti delle Forze di Polizia per inoltrare la segnalazione o denuncia/querela e permettere alle autorità competenti l'approfondimento della situazione da un punto di vista investigativo. In tal senso è possibile far riferimento a queste tipologie di uffici: Polizia di Stato- Compartimento di Polizia postale e delle Comunicazioni; Questura o Commissariato di Polizia di Stato del territorio di Competenza; Arma dei Carabinieri- Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato- Commissariato on line attraverso il portale

<http://www.commissariatodips.it>

La nostra scuola proporrà ogni anno agli alunni/e la partecipazione ai **concorsi per la Giornata mondiale per la sicurezza in rete (Safer internet day)** presentati dalla Piattaforma Generazioni Connesse per contrastare il fenomeno del bullismo e Cyber bullismo.

---

## ***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.

**Interventi per combattere l'hate speech:**

- condivisione nei Consigli di Classe di percorsi trasversali di Educazione civica tesi alla promozione dei diritti umani con particolare attenzione ad alcuni obiettivi dell'Agenda 2030: ridurre le disuguaglianze, sconfiggere la povertà, parità di genere e istruzione di qualità. Inoltre si intende sviluppare **il diritto alla libertà**, particolarmente tutelato dal Consiglio d'Europa che in collaborazione con il Movimento "No hate Speech Movement" ( sito [www.nohatespeechmovement.org](http://www.nohatespeechmovement.org)) diffonde attività e iniziative per le giovani generazioni.
- Il potenziamento della libertà di parola avverrà anche con il rinnovo del **Progetto Debate** nella Scuola Primaria e Secondaria di Primo Grado.
- Promuovere la riflessione e la redazione di decaloghi condivisi dagli alunni/e che diffondano la pratica dell'uso di un linguaggio non offensivo anche con il supporto dei materiali presenti sulla Piattaforma Generazioni Connesse.

- Strutturare interventi di inclusione.
  - Progettare video o storytelling da diffondere attraverso il sito della scuola.
- 

## ***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?*

Consapevoli dei rischi derivanti dai Disturbi da dipendenza da Internet, il nostro Istituto Comprensivo promuove soprattutto per gli alunni della Scuola Primaria giornate di "Disintossicazione da smatphone" con uscite sul territorio.

Per gli alunni della Scuola Secondaria di Primo Grado si proporranno laboratori teatrali con la finalità di sviluppare le competenze sociali (riconoscere e saper gestire le altrui e proprie emozioni).

Per gli alunni di tutti i gradi scolastici è previsto un Progetto Coding strutturato con metodologie adeguate al target con la finalità di sviluppare un orientamento didattico anche al gioco analogico e digitale.

I suddetti progetti saranno svolti con risorse umane interne e nei tempi in cui sarà superata l'emergenza sanitaria.

---

## ***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 mediali 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.

### **Combattere il sexting con la formazione tra i banchi di scuola.**

La particolare delicatezza dell'argomento rischia di lasciare gli adolescenti all'oscuro da alcuni rischi che sfociano in veri e propri reati perseguiti dalla legge. Nel 2019 è stato introdotto in Italia il reato di Reveng Porn (regolato dalla Legge 19 Luglio 2019 n.69 art. 10) che punisce coloro che a

scopo di vendetta diffondono foto o video sessualmente espliciti di terzi. Il Reveng Porn è un fenomeno che scaturisce dalla fiducia tradita, ma ha il potere di diffondere materiale privato con velocità sorprendente e di far permanere sulla rete tale materiale, finchè non avviene la dovuta segnalazione agli enti preposti. Gli effetti che può subire un adolescente, in seguito alla pubblicazione sui social di materiale intimo ceduto con leggerezza, sono:

- violenza psicosessuale
- umiliazione
- bullismo
- cyber-bullismo
- molestie
- stress emotivo.

Proporre video come " Se mi posti ti cancello" e " La ragazza visibile" presenti sulla Piattaforma Generazioni Connesse possono avviare percorsi di educazione all'affettività da svolgere nelle classi terze della Scuola Secondaria di Primo grado.

---

## **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.

La scuola offre uno sportello d'ascolto di un esperto psicologo con la finalità di intraprendere il dialogo con l'alunno/a vittima di adescamento.

La scuola intende offrire un supporto ai genitori per mettere in atto azioni di controllo e di intervento.

**Seguono consigli di intervento immediato:**

in caso di sospetto di adescamento il genitore deve evitare di sostituirsi al minore per evitare che vengano compromesse le prove;

chiedere l'intervento della Polizia Postale e delle Comunicazioni;

salvare conversazioni con screenshot;

consultare il servizio di neuropsichiatria infantile e consultorio familiare per un supporto alla vittima;

consultare Helpline di Generazioni Connesse al 19696.

---

## **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](#).**

#### Consigli utili:

- evitare di scaricare sul proprio device materiale pedopornografico con l'intento di procurarsi una prova, altrimenti si incorre nel reato di detenzione di materiale pedopornografico;
- non inoltrare il materiale ai centri messi a disposizione da Safer Internet Centre;
- segnalare conversazioni o materiale esclusivamente pubblico e non privato;
- la segnalazione può essere in forma anonima oppure fornendo i propri dati anagrafici, in quest'ultimo caso il CNCPO ( Centro nazionale per il contrasto della pedopornografia su internet) contatterà il segnalatore.

#### Perchè fare una segnalazione se ci si imbatte in materiale pedopornografico?

- La segnalazione è essenziale per identificare il bambino abusato e porre fine all'abuso;
- per la rimozione del video;
- per mettere in atto interventi psicologici adeguati per la vittima;
- per evitare che il reato di pedopornografia sfoci in abuso sessuale agito.

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

---

### **AZIONI da sviluppare nell'arco dell'anno scolastico 2020/2021.**

- Organizzare un'attività di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolto agli alunni/e.
- Organizzare un incontro informativo online per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Promuovere lezioni e laboratori di classe per alunni/e dedicati all' Educazione Civica Digitale.
- Offrire informazioni relative alla formazione deidocenti sulle tematiche del rispetto della diversità; rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza.

**AZIONI da sviluppare nell'arco dei tre anni scolastici successivi.**

- Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli alunni/e.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/le studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.
- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

# 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 minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting:** nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere 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:19696).

## **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.

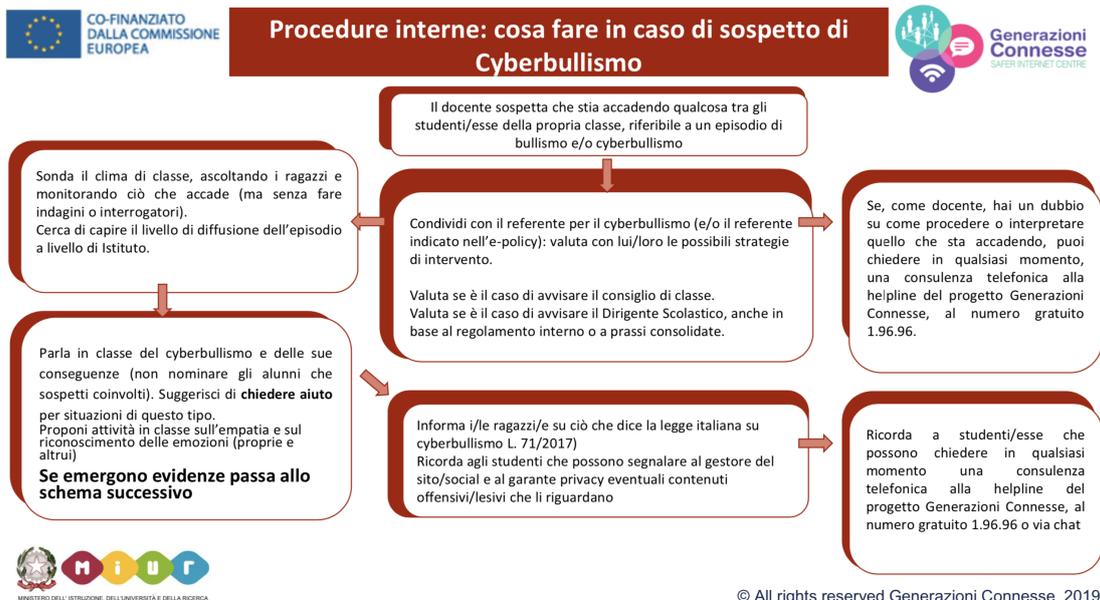
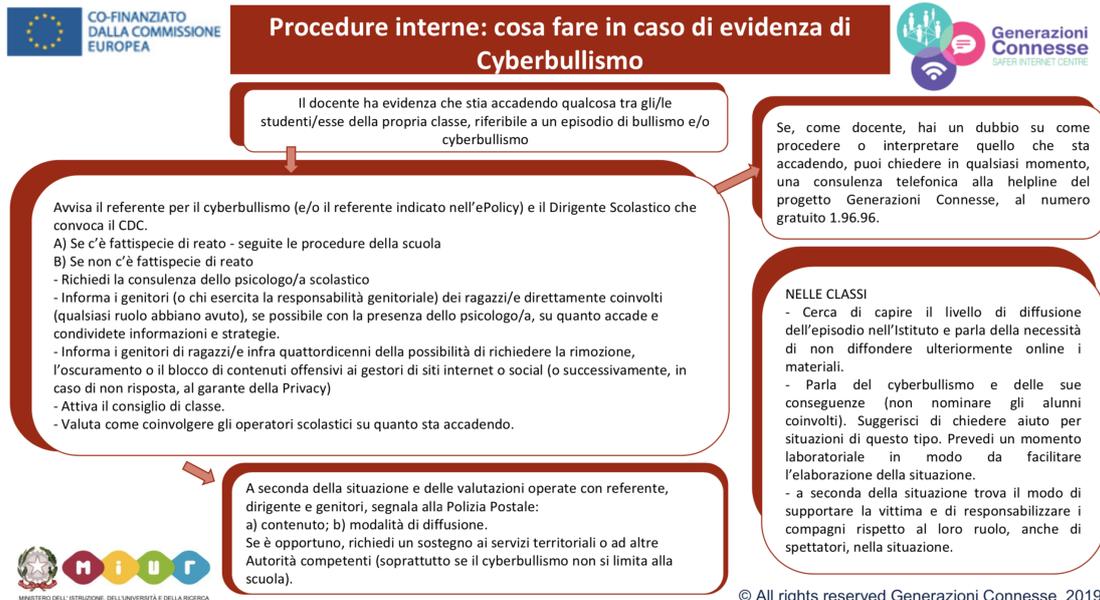
Per una mappatura degli indirizzi di tali strutture è possibile consultare il [Vademecum](#) di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza 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.

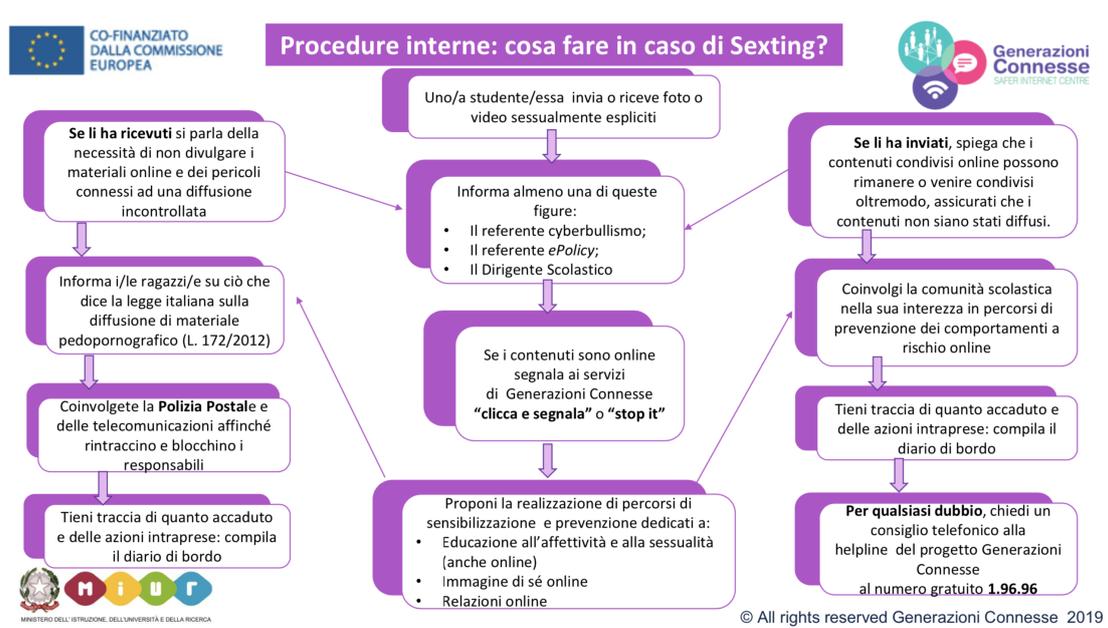
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

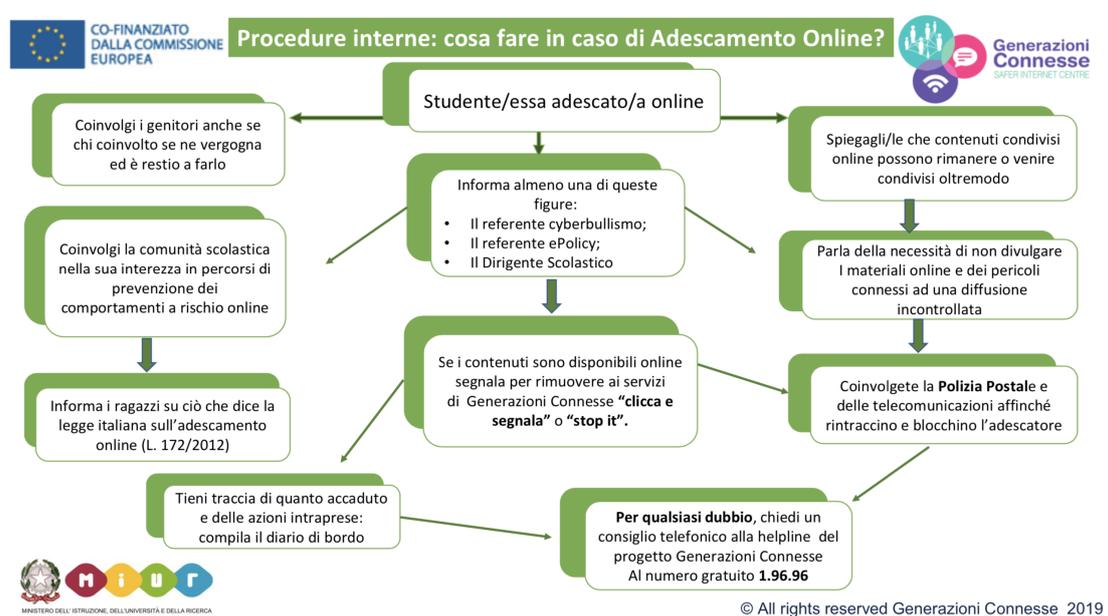
### **Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?**



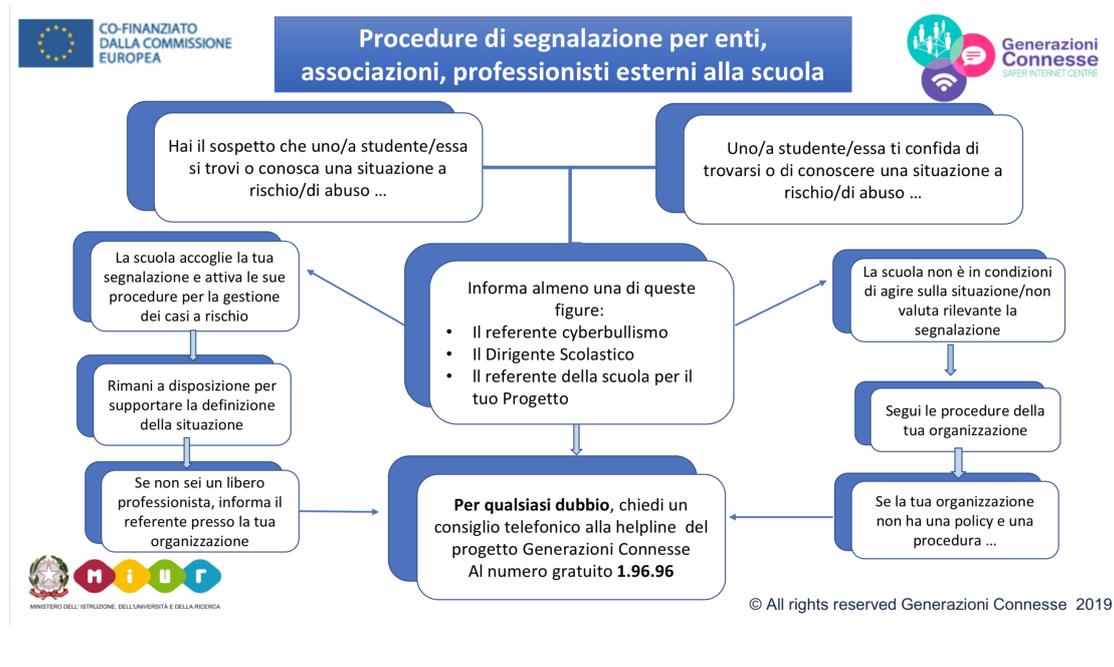
## Procedure interne: cosa fare in caso di sexting?



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



## 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

**Non è prevista nessuna azione.**

