



# Documento di ePolicy

LIIC81000C

"G.MARCONI"

VIA DELLA FIERA - 57021 - CAMPIGLIA MARITTIMA - LIVORNO (LI)

MARIA ELENA FRONGILLO

# 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**

Garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica. Promuove la cultura della sicurezza online insieme al docente referente sulle tematiche del bullismo/cyberbullismo, con il quale organizza corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC. Il Dirigente Scolastico ha inoltre la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

### **L'Animatore digitale**

Supporta il personale scolastico da un punto di vista tecnico-informatico, in riferimento ai rischi online, alla protezione e gestione dei dati personali. E' uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" .

### **Il Referente bullismo e cyberbullismo**

Coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, si avvale della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio.

### **I Docenti**

Hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete: integrano parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica. I docenti supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori prevedendo l'uso della LIM; hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

### **Il personale Amministrativo, Tecnico e Ausiliario (ATA)**

Svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il dirigente scolastico e con il personale

docente tutto. Esiste, pertanto, un concreto coinvolgimento del personale ATA nell'applicazione della [legge 107/15 \("La Buona Scuola"\)](#) che concerne non solo il tempo scuola e il potenziamento dell'offerta formativa, ma anche le attività di formazione e autoformazione in tema di bullismo e cyberbullismo. Il personale ATA è coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

## **Gli Studenti e le Studentesse**

In relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzano al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola imparano a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le; partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete. Si fanno promotori di quanto appreso anche attraverso possibili percorsi di peer education.

## **I Genitori**

In continuità con l'Istituto scolastico, partecipano attivamente alle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali. Si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicano con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet.

---

## ***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).

I soggetti esterni che svolgono attività educative nell'Istituto sottoscrivono un'informativa sul trattamento dei dati che potrebbe veder implementata la parte relativa all'e-policy.

---

## ***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.

Nello specifico la nostra scuola intende:

1. condividere e comunicare il documento agli studenti e alle studentesse al fine di:
  - dare loro una base di partenza per un uso consapevole e maturo dei dispositivi e della tecnologia informatica;
  - dare loro regole condivise di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici;
  - dare loro elementi per poter riconoscere e quindi prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e.

Saranno i docenti a prevedere momenti di informazione e di riflessione sul documento ufficiale, in

modo da favorire un confronto nel gruppo classe e semplificare la comprensione. E' prevista inoltre la creazione di un documento child friendly del documento per la comunicazione e la sensibilizzazione ai/lle bambini/e e ai/lle ragazzi/e.

2. condividere e comunicare il documento al personale scolastico in modo da poter orientare tutte le figure sui temi in oggetto, a partire da un uso corretto dei dispositivi e della Rete in linea anche con il codice di comportamento dei pubblici dipendenti.

Sono previsti uno o più incontri informativi nel corso dell' anno scolastico tenuti dal referente del cyberbullismo.

3. condividere e comunicare il documento ai genitori sul sito istituzionale della scuola, tramite momenti di formazione specifici e durante gli incontri scuola-famiglia.

---

## ***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.

Talune condotte, in relazione all'uso improprio delle TIC e della Rete a scuola da parte degli studenti e delle studentesse (ad esempio la condivisione online di immagini o video di compagni/e senza il loro consenso o che li ritraggono in pose offensive e denigratorie oppure la condivisione di scatti intimi e a sfondo sessuale, la condivisione di dati personali, l'invio di immagini o video volti all'esclusione di compagni/e) sono sanzionabili.

A seconda dell'età dello studente o della studentessa e dell'entità del fatto avvenuto, l'intervento avverrà su tutto il contesto classe con attività specifiche educative e di sensibilizzazione, allo scopo di promuovere una maggior consapevolezza circa l'utilizzo delle TIC e di Internet.

Allorchè abbia a verificarsi un fatto grave, sarà **considerata la possibilità di denunciare l'episodio** (con il coinvolgimento ad es. della Polizia Postale) e di garantire, se necessario, immediato supporto psicologico allo/la studente/ssa attraverso i servizi predisposti.

I docenti che utilizzano impropriamente i device o la Rete, o qualora non intervengano nella segnalazione di condotte improprie dei/lle propri/ie studenti/studentesse potranno essere sanzionati come dalla normativa vigente.

---

## ***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 scuola, quale luogo educativo e formativo, di inclusione e accoglienza, si impegna ad attivare azioni di "prevenzione del bullismo e del cyberbullismo per un utilizzo critico e consapevole dei social network e dei media" (art.1, c.7 e lett.I, legge 107/15) e strategie atte ad arginare comportamenti a rischio, in molti casi, derivanti da condizioni di disagio sociale non ascrivibili solo al contesto educativo scolastico. Se è innegabile che il mondo digitale e virtuale rappresenti un'enorme opportunità di sviluppo e crescita culturale e sociale, non va tuttavia sottovalutato che esso contiene una serie di insidie e pericoli su cui è indispensabile misurarsi. L'Istituto Comprensivo "Marconi", dinanzi al dilagare di nuove forme di devianza che coinvolgono anche gli adolescenti, intende attivare sinergie con le famiglie e le altre istituzioni, con l'obiettivo di accrescere il senso della legalità, il benessere ed educare gli studenti ad un uso consapevole del web. La scuola, nell'ambito dell'educazione alla legalità e all'uso consapevole di internet, si impegna a prevenire, individuare e combattere il bullismo e il cyberbullismo in tutte le sue forme. L'allegato n.7 del Regolamento di Istituto approfondisce le interrelazioni fra l'assetto regolamentare della scuola e la normativa vigente.

---

## ***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.

Le modifiche del documento dovrebbero essere discusse con tutti i membri del personale docente. Il monitoraggio del documento dovrebbe prevedere anche una valutazione della sua efficacia a partire dagli obiettivi specifici che lo stesso si pone (promozione delle competenze digitali e dell'uso delle TIC nei percorsi educativi e didattici, prevenzione e gestione dei rischi online etc...). Un docente nominato dal Dirigente Scolastico potrebbe, fra i suoi compiti, fungere da referente per la revisione e/o l'aggiornamento dell'ePolicy.



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

---

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

- Pubblicazione del documento di E policy sul sito dell'Istituto e condivisione con la comunità scolastica
- Miglioramento del sistema di gestione delle infrazioni

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

- Azione 1 Implementazione dell'informativa per i soggetti esterni che erogano attività educative nell'Istituto.
- Azione 2 Maggiore integrazione dell'ePolicy con Regolamenti esistenti.
- Azione 3 Realizzazione di un sistema di monitoraggio delle attività.

# 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.

Il nostro Istituto ha recentemente inserito un Curriculum verticale delle competenze digitali all'interno della programmazione dell'Educazione Civica: le conoscenze e le abilità, direttamente collegabili agli obiettivi prefissati, accompagnano i ragazzi in un percorso organizzato nei tre anni della scuola secondaria di primo grado, toccando temi propri di ciascuna disciplina.

La scuola si interessa già dal 2015 di educare i giovani all'uso responsabile delle nuove tecnologie e della rete internet, che portano alla società contemporanea innegabili vantaggi, ma anche numerose insidie dovute all'utilizzo indiscriminato che, soprattutto i più giovani, sono inclini a farne.

La sala SEFI di Venturina Terme è stata teatro di numerosi incontri dedicati agli studenti delle classi prime della scuola Secondaria di I° grado G. Carducci dell'Istituto G. Marconi di Campiglia Marittima. Gli eventi, proposti dal LIONS Club di Piombino, hanno avuto come tema "La sicurezza su Internet" ed hanno visto la partecipazione di esperti del settore e delle autorità cittadine. che ha saputo catturare l'attenzione degli studenti e dei genitori presenti con una presentazione interattiva.

---

## ***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 nostro Istituto realizza da anni i Caffè digitale tenuti dall'Animatore digitale e dalle Funzioni strumentali. Negli ultimi incontri sono state presentate alcune app utili per la didattica come Prezi, Popplet, Geogebra, Pro-Bot, Google Play Libri, "Hubcampus" Mondadori.

---

## ***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.

Dall'Anno Scolastico 2017/2018 l'Istituto Comprensivo "G.Marconi" sostiene la campagna contro il bullismo e il cyberbullismo programmando più incontri con esperti in materia (EbiCo, Cooperativa Sociale-ONLUS riconosciuta come Spin-Off Accademico dell'Università di Firenze) sui rischi della Rete, a cui sono invitati a partecipare sia gli insegnanti che i genitori. Con la prima iscrizione al Progetto Generazioni connesse il referente dell'Istituto ha organizzato più incontri rivolti ai docenti della scuola per informare e condividere il documento ePolicy, come era previsto tra le azioni da realizzare. Nell'anno in corso è previsto un incontro con la Polizia Postale rivolto a docenti e genitori.

## ***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.

Le famiglie giocano un ruolo educativo fondamentale: è per questo che i genitori vengono chiamati a partecipare agli incontri di sensibilizzazione sul tema del bullismo e cyberbullismo organizzati ogni anno dall'Istituto a fianco dei docenti.

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

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020)

- 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 su un campione di studenti e studentesse in relazione alle competenze digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.

# 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.

1) La nostra scuola redige e mantiene un registro dei trattamenti dei dati, sia per il titolare che per il responsabile dei trattamenti. Il registro dei trattamenti è in continuo aggiornamento grazie al contributo e alla consulenza del DPO.

2) In merito alla valutazione dei rischi sulla privacy (definita nel regolamento Data Protection Impact Assessment o PIA) relativamente ad alcune tipologie di trattamento dei dati sensibili, l'Istituto si avvale della consulenza del DPO. Quest'ultimo, su richiesta del titolare del trattamento, sottopone a valutazione di rischio il trattamento dei dati operato per lo svolgimento delle attività istituzionali. Come dovuto, vengono sottoposti a regime di particolare riservatezza, dati sensibili, come ad esempio quelli relativi alle origini razziali per favorire l'integrazione degli/le alunni/e, quelli relativi alle convinzioni religiose, al fine di garantire la libertà di culto, e quelli relativi alla salute per adottare misure di sostegno degli/le alunni/e, come i dati vaccinali con le Asl.

3) In merito all'Analisi di processo sulla raccolta/gestione del consenso: la richiesta di consenso è chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), nella modulistica dedicata.

4) In merito alle misure tecniche e organizzative per garantire la sicurezza dei trattamenti sul sito:

- il sito dell'Istituto è in fase di aggiornamento per adeguarsi ai protocolli ministeriali.
- E' utilizzato un sistema di cifratura e pseudonimizzazione quando il trattamento di dati lo richiede. Il sistema non si fonda sull'uso di algoritmi, ma sul ricorso alle sole iniziali del nome e del cognome degli interessati;
- Esiste un sistema di backup che permette di salvare regolarmente i dati, ripristinare eventuali file modificati o rimossi per errore dalla rete e garantire la presenza di una copia di sicurezza di tutti i file importanti.

---

## **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.

L'infrastruttura hardware dell'Istituto è stata potenziata nel corso degli ultimi anni: in ogni classe di ciascun plesso è presente una LIM, mentre i plessi Amici, Carducci e Muratori hanno un laboratorio d'informatica con 20 dispositivi.

In ciascun plesso, di ogni ordine e grado, è garantito l'accesso ad Internet agli utenti. L'infrastruttura di rete è stata recentemente aggiornata con la fibra ottica, permettendo un accesso diffuso in ogni aula, laboratorio, corridoio e spazio comune. Tale adeguamento si è reso necessario anche nell'ottica di un utilizzo sistematico di strumenti come il registro elettronico per semplificare la comunicazione e lo scambio di informazioni tra dirigente, docenti e famiglie.

L'accesso alla Rete, per Studenti, Insegnanti e personale amministrativo è garantito con modalità differenziata. Inoltre, pur utilizzando la stessa rete, didattica e segreteria sono separate, in modo tale da garantire maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le due reti grazie al firewall.

Software e sistema operativo vengono aggiornati periodicamente garantendo la protezione dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo.

Periodicamente vengono **programmati dei backup**, cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi.

**E' Predisposta la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo:** se non è previsto uno stand-by, il dispositivo resta accessibile nel caso in cui qualcuno

dimentichi di spegnerlo, con il rischio potenziale di accesso da parte di persone non autorizzate.

In allegato, il Regolamento d'Istituto, comprensivo delle sezioni relative all'uso delle Tic ed alla prevenzione di condotte riconducibili al cyberbullismo.

**Nei laboratori d'informatica esiste inoltre un sistema di blocco che impedisce di scaricare determinati programmi agli studenti.**

---

### ***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.

Fra gli strumenti di comunicazione esterna dell'Istituto troviamo in primis il sito web della scuola: [www.istituto-marconi.it](http://www.istituto-marconi.it). Tale strumento è utilizzato in primis per fornire informazioni di servizio rivolte a studenti o genitori. E' stata creata nel corrente anno scolastico una pagina Facebook del nostro Istituto, in cui è possibile visualizzare eventi e comunicazioni relative all'attività della scuola.

Fra gli strumenti di comunicazione interna, invece, troviamo il registro elettronico, nello specifico SCUOLANEXT con tutte le sue funzionalità. 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).

La scuola utilizza anche la classica e-mail, sia per la comunicazione con i docenti che con le famiglie, oltre ad ulteriori applicativi e piattaforme di lavoro condiviso e collaborativo (come moodle, padlet, [google doc](#), [classroom](#),...) per facilitare e rendere più partecipata la didattica e la comunicazione a scuola.

Per quanto riguarda l'uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne, viene seguito il "diritto alla disconnessione". L'art. 22 (Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola) del CCNL 2016/2018, infatti, fa riferimento ai criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione fra vita lavorativa e vita familiare.



---

## 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.

Il Regolamento di Istituto disciplina l'utilizzo dei dispositivi personali, distinguendo fra l'impiego didattico degli stessi (BYOD) e l'uso non appropriato alla sede scolastica.

---

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

#### **AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).**

- Garantire formazione adeguata allo staff, incluso il corpo docenti: la formazione deve riguardare la gestione dei dispositivi, la conoscenza delle regole basilari sulla sicurezza.
- Testare regolarmente le possibili vulnerabilità.
- Preparare piani di azione in risposta ai problemi più seri: è importante non dover improvvisare nel momento in cui si verifica un problema serio, ma avere un protocollo di azione.
- Impostare il browser per l'eliminazione dei cookies alla chiusura: in questo modo si evita che qualcuno possa avere accesso ad account altrui senza autorizzazione.
- 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
- Adeguare il sito alle linee guida ministeriali e potenziarne l'utilizzo
- 

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

- 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.

L'I.C. Marconi ha fin da subito sostenuto interventi e attività che ruotavano attorno al tema Bullismo e Cyberbullismo. Dal 2018 il nostro istituto, in collaborazione con la Ludoteca Comunale, ha aderito alle iniziative sul tema promosse dalla Cooperativa Sociale Onlus EbiCo (spin-off accademico del Dipartimento di Psicologia dell'Università di Firenze), attivando interventi di sensibilizzazione e prevenzione al Bullismo e Cyberbullismo rivolti agli alunni della scuola secondaria di primo grado (progetto NoTrap), ai genitori, ai docenti e al referente tutor (partecipazione al progetto provinciale Cyberlivorno 2016/2017 e al progetto regionale S.T.A.R. 2 (Scuole Toscane Antibullismo in Rete 2). Gli alunni delle classi della scuola secondaria di primo grado hanno partecipato inoltre ai progetti /interventi di :

- Educazione all'affettività e alla sessualità, promossi dall'ASL d zona;
- Educazione alla Legalità, promossi dall'Arme dei Carabinieri e dalla Guardia di Finanza;
- Sicurezza in Internet, promossi dalla Polizia Postale.

La responsabilità dell'azione preventiva ed educativa chiama in campo, infatti, molteplici agenzie educative oltre alla scuola in supporto alla famiglia, come istituzioni, enti locali, associazioni, ciascuna con un proprio compito nei confronti di bambini e bambine e di adolescenti. Tali agenzie sono chiamate a collaborare ad un progetto comune, nell'ambito di funzioni educative condivise. La necessità di questa collaborazione nasce dal riconoscimento sia da parte dei genitori che da parte degli insegnanti della difficoltà, ciascuno per il ruolo ricoperto, a svolgere da soli la propria funzione formativa ed educativa.

---

## 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).

In seguito alla pubblicazione della L. 71/2017 il nostro Istituto si è mosso fin da subito per rispondere in modo adeguato a quanto previsto dalla normativa. E' sta individuato tra i docenti un referente che ha partecipato alla formazione provinciale (Cyberlivorno 2016/2017) che ha successivamente trasmesso agli altri docenti i contenuti secondo il modello peer to peer. Nell'anno scolastico 2018/2019 le classi seconde della scuola secondaria di primo grado hanno seguito il progetto NoTrap, proposto dalla Società Cooperativa Onlus EbiCo, in collaborazione con la Ludoteca Comunale, che prevede, tra i fondamenti del progetto, il ruolo attivo degli studenti in attività di peer education. Quando è stato rilevato un sospetto caso di bullismo/cyberbullismo tra gli studenti è stata elaborata una serie di interventi sia sul contesto classe che in un'ottica di sostegno verso i minori coinvolti. Il Regolamento di Istituto fa espressamente riferimento a condotte di cyberbullismo e a sanzioni disciplinari commisurate alla gravità degli atti compiuti, contemplando non solo azioni sanzionatorie, ma anche preventive ed educative.

---

## ***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.

Si suggerisce la visione di video pubblicati nella piattaforma Generazioni Connesse; in particolare, della mini-serie Super Errori, in cui il tema dei rischi online in senso lato, è affrontato in modo ironico, ma allo stesso tempo approfondito. I video possono essere usati con i ragazzi delle scuole secondarie di I grado (e con le classi V della primaria). Tali argomenti possono essere trattati trasversalmente in tutti gli ambiti disciplinari, rimandando ai docenti una sensibilizzazione al tema.

---

## ***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?*

La tecnologia ha modificato gli ambienti in cui viviamo e ha un impatto sulla qualità della vita. Gli elementi che contribuiscono al benessere digitale sono:

- la ricerca di equilibrio nelle relazioni anche online
- l'uso degli strumenti digitali per il raggiungimento di obiettivi personali
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile
- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche)

Si tratta di un argomento trasversale, collegato al tema della cittadinanza digitale, del cyberbullismo, di uso integrativo e non sostitutivo dei dispositivi e della Rete, oppure di un contenuto a parte, a cui riservare un momento di riflessione specifica con studenti e studentesse.

La scuola può insegnare molto da questo punto di vista se integra la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online.

Allo stesso modo quando parliamo di videogiochi, dobbiamo pensarli non in termini negativi, ma di benessere digitale. Sono parte del mondo di studenti e studentesse. Tuttavia gli studi recenti dimostrano il progressivo aumentare di questo fenomeno, tanto che la dipendenza dal gioco online è stata inserita nel DSM-5 (Manuale diagnostico e statistico dei disturbi mentali) soprattutto perché associata a gravi conseguenze per la salute psicofisica della persona. Per questo motivo, il nostro Istituto nel corrente anno scolastico, ha previsto un'intervento di sensibilizzazione e prevenzione con il SERD dell'ASL di zona, prevedendo incontri sia con gli alunni che con i genitori.

---

## 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.

Si tratta di un argomento trasversale, collegato all'uso consapevole del digitale, della cittadinanza attiva, dell'educazione emotiva e sessuale oppure di un contenuto a parte, a cui riservare un momento di riflessione specifica con studenti e studentesse.

---

## 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 problematica dell'adescamento online (come quella del sexting), si inquadra in uno scenario più ampio di scarsa educazione emotiva, sessuale e di assenza di competenza digitale, in riferimento al modo in cui i/le ragazzi/e vivono la propria sessualità e la propria immagine online, al loro desiderio

di esprimersi e affermare se stessi. Risulta essere fondamentale continuare a portare avanti quei percorsi che da anni sostiene il nostro Istituto, legati all'educazione all'affettività e alla sessualità, avvalendosi di personale esperto. Fra questi si segnala, in particolare, uno sportello psico-pedagogico, al quale possono rivolgersi alunni e genitori

Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore ( per esempio nel rispondere all'adescatore). E' importante che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove. Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video).

Per consigli e per un supporto è possibile rivolgersi alla [Helpline di Generazioni Connesse \(19696\)](#): operatori esperti e preparati sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che dei bambini, degli adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti l'utilizzo dei nuovi media.

---

## 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 tema della pedopornografia è estremamente delicato e, in termini di prevenzione, occorre parlarne sempre in considerazione della maturità e della fascia d'età degli utenti, selezionando il tipo di informazioni che si possono condividere (ad esempio, non è opportuno diffondere tra i bambini e le bambine più piccoli/e l'uso di servizi come le hotline, sia perché in caso di visione accidentale di materiale pedopornografico è opportuno che bambini/e e ragazzi/e possano parlarne con gli adulti di riferimento per la migliore risposta possibile, sia perché si potrebbe incentivare la ricerca proattiva, che comunque è vietata dalla legge italiana, per minori e per adulti).

A questo proposito, risulta fondamentale l'attività educativa sull'affettività e le relazioni, da portare avanti con il supporto costante degli adulti.

L'I.C. Marconi abbraccia ogni anno progetti sul tema che vengono proposti dalla ASL territoriale, riservandoli ai ragazzi delle classi terze della scuola secondaria di primo grado.

Tale tematica è affrontata negli incontri sui rischi della Rete, organizzati ogni anno dal nostro Istituto, promossi da esperti in materia (EbiCO, Polizia Postale, Carabinieri) e rivolti a studenti e genitori.

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

### **Piano di azioni**

**AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).**

- Organizzare un incontro di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Organizzare un incontro informativo per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/le studenti/studentesse, con il coinvolgimento di esperti.

**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 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.
- Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori e personale della 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 analogha 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.

Si ritiene opportuno segnalare episodi o situazioni direttamente collegabili a bullismo e/o cyberbullismo, sexting o adescamento on line, sia nel caso in cui si abbia il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, sia nel caso in cui ci si trovi in presenza di un evento conclamato.

---

## **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).

La persona adulta (docente, personale ATA, genitore, esperto esterno...) che abbia effettivamente

riscontrato qualcosa o che sia venuto a conoscenza di un episodio o di una situazione di disagio afferibile alle tipologie sopra descritte dovrà informare sia il Referente per il bullismo e cyberbullismo sia il Dirigente Scolastico, che valuterà il caso e le strategie di intervento (preventive, educative o sanzionatorie) da attuare. Successivamente il Referente provvederà a compilare la scheda di segnalazione (allegato).

---

### **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.

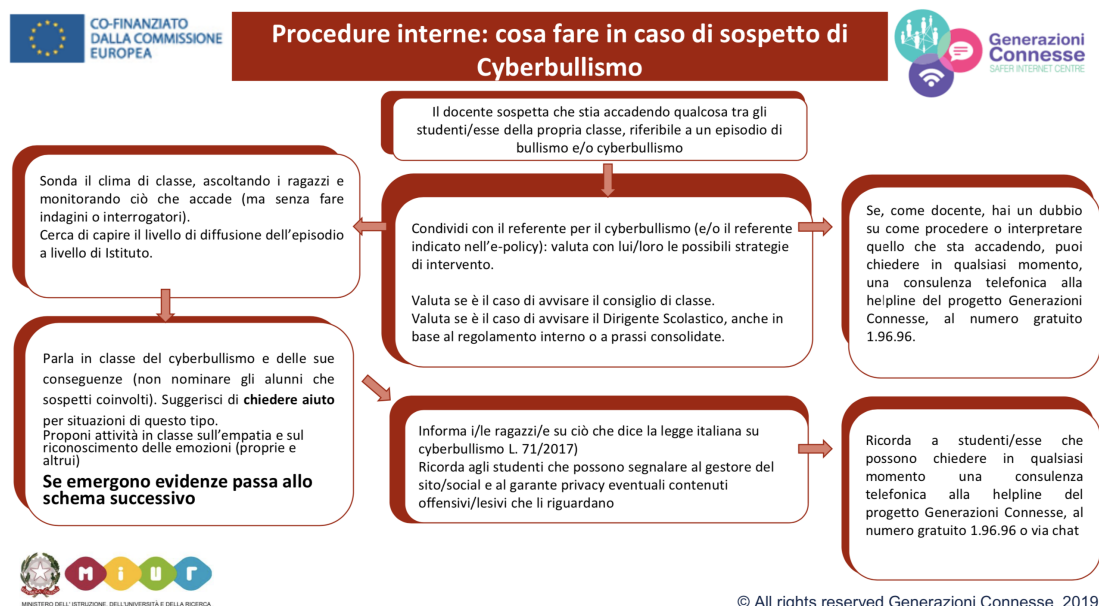
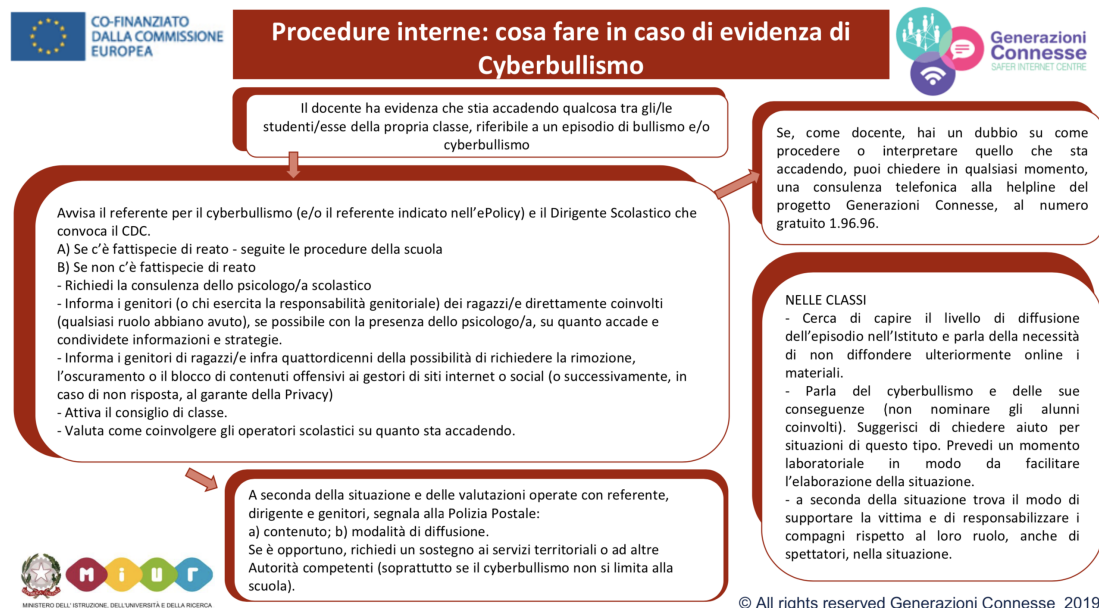
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **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

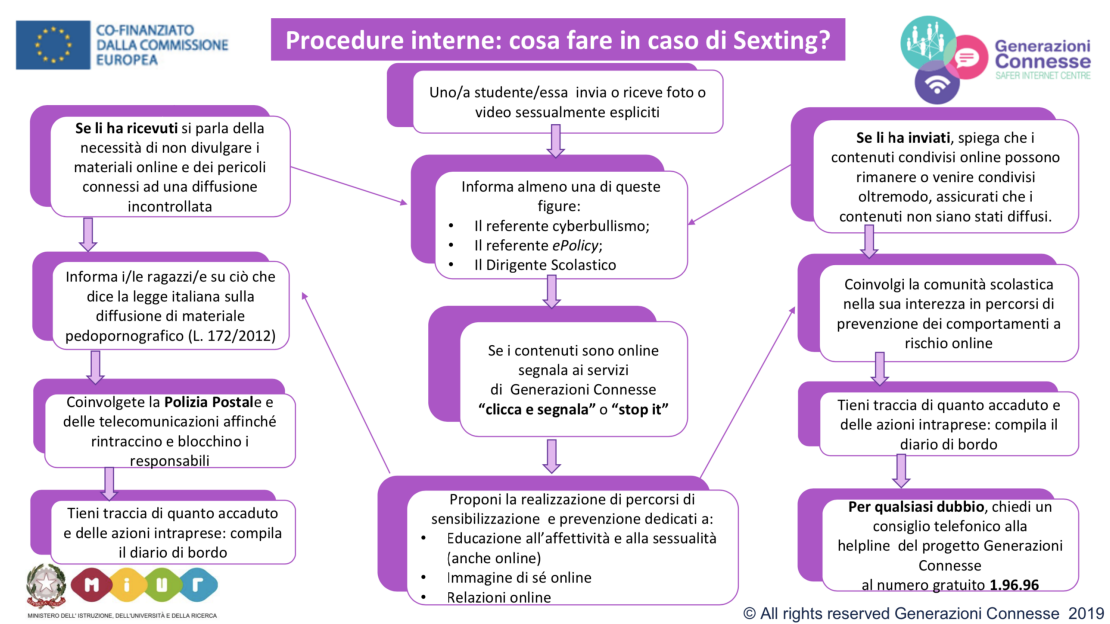
educative, tutela e assistenza in riferimento ai minori.

## 5.4. - Allegati con le procedure

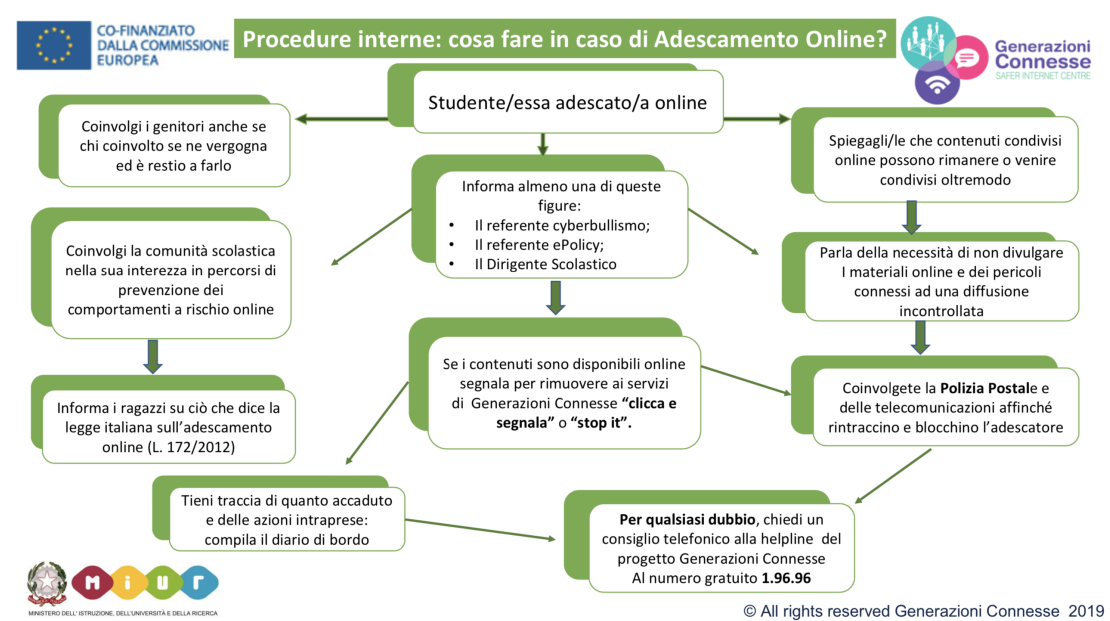
### Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



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

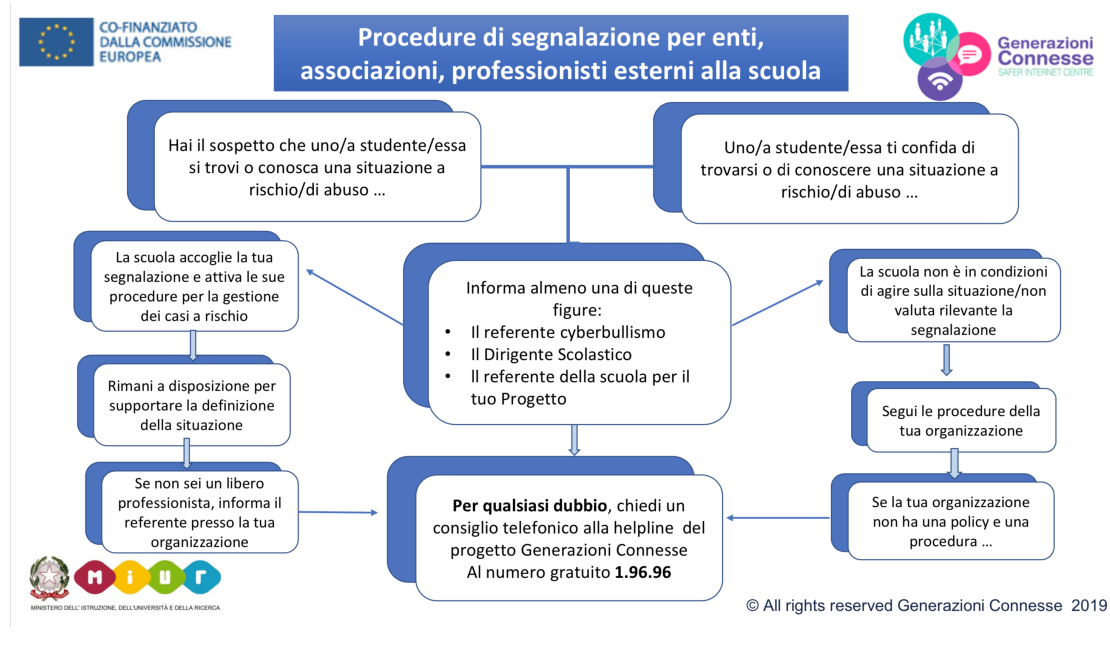


## Procedure interne: cosa fare in caso di adescamento online?





## 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.**

