

ISTITUTO COMPRENSIVO - "REGIO PARCO"-TORINO  
Prot. 0008982 del 29/10/2020  
04-01 (Uscita)



# Documento di ePolicy

---

TOIC87700C

I.C. TORINO - REGIO PARCO

CORSO REGIO PARCO 19 - 10152 - TORINO - TORINO (TO)

Mira Francesca Carello

# 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.

Dirigente Scolastico: responsabile per la sicurezza dei dati e garante dell'applicazione della E-Policy:

- individua attraverso il Collegio dei Docenti un referente del bullismo e cyberbullismo;
- coinvolge nella prevenzione e contrasto al fenomeno del bullismo/cyberbullismo tutte le componenti della comunità scolastica;
- favorisce la discussione all'interno della scuola, attraverso gli organi collegiali, creando i presupposti di regole condivise di comportamento per il contrasto e la prevenzione dei fenomeni del bullismo e del cyberbullismo;
- promuove la cultura della sicurezza online attraverso percorsi di formazione specifici e/o iniziative sul territorio.

Animatore Digitale: insieme agli altri docenti del team digitale:

- supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali;
- é uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica);
- monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e ha il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

Referente Cyberbullismo: promuove attività ed eventi funzionali alla prevenzione delle problematiche inerenti al cyberbullismo in collaborazione con forze dell'ordine, associazioni e centri di aggregazione giovanile del territorio.

Docenti:

- diffondono la cultura dell'uso responsabile delle TIC e della rete internet;
- sono tenuti a segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse;
- sono invitati a partecipare alle attività di formazione proposte dai referenti.

Personale ATA: 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.

Genitori: vengono coinvolti affinché, in continuità con l'Istituto scolastico, siano partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali; si opera affinché si relazionino in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunichino con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet. È estremamente importante che accettino e condividano quanto scritto nell'ePolicy dell'Istituto.

Enti educativi esterni e associazioni: sono tenuti a prendere visione dell'ePolicy d'istituto e conformarsi ad essa.

---

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

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

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

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

---

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

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/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 ePolicy è pubblicata sul sito della scuola dopo essere stata approvata dal Collegio dei Docenti e dal Consiglio d'Istituto.

Ogni anno scolastico i docenti invitano studenti e famiglie a prenderne visione.

---

## ***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.

Nel caso in cui una violazione al regolamento di istituto si configuri come atto di bullismo/cyberbullismo o più in generale come infrazione all'ePolicy d'istituto, colui che ne viene a conoscenza informa tempestivamente il Dirigente Scolastico e il referente per il bullismo/cyberbullismo.

Qualora tali infrazioni dovessero configurarsi come reato, il Dirigente Scolastico farà una tempestiva segnalazione all'autorità competente, fatto obbligo di denuncia.

Verrà valutata la gravità della violazioni in base alla quale saranno attivate azioni educative e, all'occorrenza, allertati i servizi predisposti (Servizi sociali, Polizia postale, Nucleo di prossimità, supporto psicologico).

Si rinvia al Regolamento d'Istituto per i provvedimenti disciplinari previsti e al capitolo 5 del documento di ePolicy per la procedura attivata.

---

## ***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.

---

## ***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.

---

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

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

- Creazione del gruppo di lavoro ePolicy (Azione sviluppabile nel breve periodo)
- Realizzazione di un sistema di monitoraggio delle attività (Azione sviluppabile nell'arco di un anno)
- Realizzazione di un'assemblea per discutere delle attività di progetto (Azione sviluppabile nell'arco di un anno)

# 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.

Nel corso del prossimo triennio l'Istituto promuoverà l'implementazione organica di un curriculum verticale delle competenze digitali, che richiami le quattro dimensioni sulle quali sarà possibile lavorare in classe, in un'ottica che integra la dimensione tecnologica con quella cognitiva, etica e sociale:

- dimensione tecnologica: comprensione e conoscenza sia della struttura hardware di base e della "sintassi" di funzionamento degli strumenti digitali e nozioni di utilizzo dei più diffusi applicativi;
- dimensione cognitiva: capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità;
- dimensione etica: capacità di gestire in modo sicuro i propri dati personali e quelli altrui, e di usare le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri;
- dimensione sociale: sviluppo delle abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui propri doveri nei riguardi di coloro con cui si comunica online.



Il curriculum sarà sviluppato in modo trasversale rispetto alle discipline di studio e si accompagnerà a un approfondimento specifico riguardante le tecnologie, in coerenza con quanto previsto dal Piano Scuola Digitale (PNSD) e dalla Raccomandazione del Consiglio Europeo relativa alle competenze chiave per l'apprendimento permanente. Si seguiranno le linee del DigComp, ovvero il quadro di riferimento per le competenze digitali dei cittadini, che individua otto livelli di padronanza in relazione alle principali aree di competenza.

---

## ***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.

L'Istituto fa parte della rete Riconessioni, promossa dalla Compagnia di San Paolo, realizzata dalla Fondazione per la Scuola, in partnership con Open Fiber, che ha l'obiettivo di creare un modello di innovazione a livello nazionale, partendo dalla città di Torino.

Il progetto, attivo dall'anno scolastico 2017-2018, ha previsto e prevede tuttora la formazione di insegnanti sia in presenza che a cascata, per raggiungere il 60% del corpo docente; la sperimentazione accompagna le scuole primarie e secondarie di primo grado della rete in un processo di innovazione tecnologica, organizzativa e didattica.

L'Istituto, attraverso il collegio dei docenti, riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola, anche con l'aiuto dell'animatore digitale, dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti (anche online), purché coerenti con il piano di formazione.

L'uso delle TIC nella didattica nel primo ciclo, che ha sostituito interamente la scuola in presenza nella fase di Didattica a Distanza, dovrà essere potenziato al fine di rendere l'apprendimento motivante, coinvolgente e inclusivo, su vari aspetti (formazione studenti e docenti, device, connessioni, partecipazione delle famiglie).

Grazie a questi presupposti, i docenti potranno guidare studenti e studentesse rispetto alla fruizione dei contenuti online, ormai la modalità naturale di apprendimento anche al di fuori della scuola. Inoltre, le TIC permettono di sviluppare capacità sempre più importanti in ambito didattico (e lavorativo, in futuro), come il lavoro di gruppo a distanza e il confronto fra pari in modalità sincrona e asincrona.

---

## ***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.

L'Istituto ha da anni un rapporto consolidato con il Nucleo di Prossimità della Polizia Municipale, che si occupa della prevenzione e degli interventi necessari nei casi di bullismo e cyberbullismo, in un'ottica educativa e riparativa, nella costruzione di consapevolezza e responsabilizzazione degli allievi.

I momenti di formazione e aggiornamento verranno implementati a partire sia dall'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica, sia dall'analisi delle richieste che provengono dagli studenti e dalle studentesse: i docenti, una volta formati, potranno a loro volta supportare allieve e allievi nel percorso di formazione sull'utilizzo consapevole delle TIC.

Verrà predisposta un'area specifica sul sito dell'Istituto con materiali formativi per gli insegnanti, con un link e materiali informativi del progetto "Generazioni connesse", dove trovare ulteriori approfondimenti, spunti aggiornamenti e strumenti didattici utili da usare con gli studenti e le studentesse, per ciascun grado di scuola.

---

## ***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.

In tale sezione verrà creato un collegamento al sito di Generazioni Connesse, comprendente un'area riservata ai genitori, e le famiglie saranno invitate a prendere visione dei materiali in esso contenuti.

---

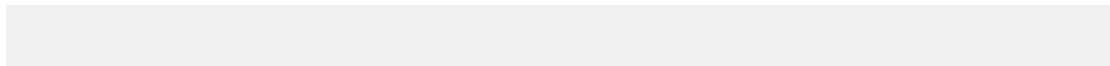
### ***Il nostro piano d'azioni***

#### **AZIONI (da sviluppare nell'arco dell'anno scolastico)**

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

L'Istituto ha adottato le seguenti misure tecniche e organizzative per garantire la sicurezza dei trattamenti:

#### SITO WEB:

- migrazione del sito web dal suffisso ".gov.it" , in quanto non più valido per le istituzioni scolastiche secondo la determina n. 36 del 12 febbraio 2018, al suffisso ".edu.it". Tale migrazione è avvenuta durante l'a.s. 2019;
- utilizzo del protocollo https per la comunicazione su Internet che protegge l'integrità e la riservatezza dei dati scambiati on line;
- progettazione del nuovo sito nel rispetto delle norme previste dal GDPR 679/16;
- sistema di backup.

#### RETE INTRANET:

- presenza di Wi-fi con access point Ubiquiti;
- adozione di firewall Open-Source Dschola come filtro per la navigazione. Il filtro si aggiorna automaticamente con la blacklist gratuita dell'Università di Tolosa UT1 oppure utilizza il filtro Open Dns o entrambi i sistemi. Il Firewall si basa su una solida distribuzione OpenBSD open source. e supporta anche reti di grandi dimensioni (500-1000 PC e oltre) e connessioni internet in fibra ottica (10/100/1000Mbit). E' inoltre compatibile con tutte le reti wireless e diversi sistemi di autenticazione;
- utilizzo di white list / black list per la navigazione (sistemi di filtraggio dei contenuti).

Attualmente l'autenticazione degli utenti sulla rete Wi-Fi dei plessi avviene attraverso l'inserimento delle credenziali da parte del docente responsabile dei laboratori informatici del plesso.

Nelle sedi Giacosa, Lessona, Poli e De Amicis i docenti possono collegarsi, con credenziali personali alla rete Wi-Fi solo per attività didattiche e per ragioni organizzative; gli allievi possono collegarsi alla rete Wi-Fi utilizzando le credenziali della propria classe, solo per attività didattiche e con il consenso dell'insegnante presente in classe. Fa eccezione la scuola Verga, che usa un altro sistema (fornito dalla rete Riconessioni), per cui una volta dato l'accesso al Wi-Fi ci si connette automaticamente. Esiste una modalità guest, per cui si può concedere la connessione per 24 ore.

## FORMAZIONE DEL PERSONALE E INFORMATIVE SUL TRATTAMENTO DEI DATI PERSONALI:

Durante l'anno scolastico 2019-2020 tutti i docenti dell'Istituto Comprensivo sono stati formati sul Regolamento UE 679/2016.

Sul sito dell'IC Regio Parco, tra i regolamenti, è riportata l'informativa sulla privacy: <https://www.icregioparco.edu.it/index.php/informativa-sulla-privacy>

---

## **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.

Il nostro Istituto Comprensivo ha partecipato ai seguenti PON e progetti per l'innovazione digitale:

- Progetto realizzazione/ampliamento rete LanWlan- 10.8.1.A1-FESR PON-PI-2015-148
- Progetto realizzazione ambienti digitali - 10.8.1.A3-FESR PON-PI-2015-22
- Progetto Smart Class 10.8.6A-FESR PON
- Progetto Riconessioni - Fondazione San Paolo,

che hanno consentito di realizzare una rete Wi-Fi in grado di coprire il 100% delle aule scolastiche nelle sedi delle scuole primarie e secondarie e un'aula 3.0 nella sede Lessona, acquistare dispositivi per il comodato d'uso per molti studenti che ne sono privi e in futuro per la realizzazione di classi virtuali.

L'IC Regio Parco, dall'a.s. 2017/2018, partecipa al Progetto Riconessioni, un progetto triennale promosso dalla Compagnia di San Paolo e realizzato dalla Fondazione per la Scuola, che ha l'obiettivo di creare un modello di innovazione culturale per affrontare il cambiamento determinato anche dalla rivoluzione digitale. Il progetto prevede: connessione degli edifici scolastici alla banda ultra larga di Open Fiber - partner del progetto -; formazione di dirigenti ed insegnanti; miglioramento delle infrastrutture.

La rete intranet delle sedi permette l'apertura del registro elettronico alle famiglie nelle scuole del primo ciclo; la compilazione da parte dei docenti avviene per lo più in tempo reale e le famiglie possono consultare immediatamente quanto scritto dai docenti.

L'azione didattica viene realizzata grazie all'ausilio di laboratori (aula di informatica in diversi plessi, aula 3.0 presso la sede Lessona) e all'esistenza di LIM in alcune aule, tuttavia la situazione risulta critica a causa dell'obsolescenza di molte postazioni. Si ritiene necessario aumentare il numero di LIM o anche solo schermi collegabili con il computer dell'aula.

La situazione più critica risulta quella della scuola dell'infanzia (sede Mameli priva di connettività e Ciriè di cablatura).

La carenza di dispositivi di alcune sedi, e in particolare della scuola secondaria Verga, sarà colmata, al termine dell'emergenza epidemiologica, dal rientro dei dispositivi acquisiti dall'Istituto e dati in comodato d'uso agli allievi per favorire l'accesso alla didattica digitale.

Sono inoltre stati acquistati nuovi PC per la Segreteria, ed è stato fatto un investimento sulla formazione del personale di segreteria per la digitalizzazione progressiva.



### **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.

La comunicazione verso l'esterno (famiglie di ragazzi e bambini non ancora iscritti, ma anche verso i nostri iscritti, associazioni, istituzioni) avviene attraverso il **sito web della scuola** (<https://www.icregioparco.edu.it/>), che viene costantemente aggiornato attraverso la pubblicazione di comunicazioni, regolamenti, avvisi, informazioni organizzative. Gli utenti consultano le pagine web del sito e hanno l'opportunità di contattare la segreteria e la Dirigente.

L'Istituto è dotato, per alcune sue sedi, di un **canale YouTube**; si prevede di estendere a ogni plesso la possibilità di condividere materiali digitali creati sia da docenti che da allievi.

Il canale principale di comunicazione verso l'interno dell'istituto è il **registro elettronico**: inizialmente aperto alle famiglie del plesso Giacosa, a partire dalla primavera 2020 è aperto a tutte le famiglie degli alunni della scuola primaria e secondaria di primo grado. Il registro elettronico costituisce il primario riferimento per le comunicazioni scuola-famiglia e per ogni comunicazione interna tra le diverse figure che operano all'interno della scuola: circolari (interne e per i genitori), messaggi di interesse generale per la classe, andamento scolastico (assenze, argomento delle lezioni, compiti assegnati, note disciplinari), risultati scolastici (voti, documento di valutazione), prenotazione di colloqui individuali, eventi.

Il sito dell'IC Regio Parco comprende poi un'**area riservata**, accessibile con login da parte del personale della scuola. Qui è possibile consultare e scaricare la modulistica, i documenti di riferimento, il calendario degli impegni, l'albo sindacale e presentare alcune richieste online. Tutto il personale della scuola viene dotato di credenziali individuali e ogni utenza viene eliminata a scadenza del contratto di lavoro.

Dall'a.s. 2012/2013 è stato introdotto l'utilizzo della **Google Suite For Education**, che ha consentito la creazione di un account individuale per tutto il personale della scuola e per un numero sempre maggiore di alunni di scuola primaria e secondaria di primo grado. L'account viene eliminato al termine della frequenza per gli allievi del nostro istituto, e al termine del contratto di lavoro per il personale della scuola. Sono state create mailing list per rendere la comunicazione più rapida ed efficace tra i vari gruppi di lavoro. Le comunicazioni tra docenti e Dirigente, docenti e allievi all'interno dell'istituto e gli scambi di email con genitori e altri Enti avvengono quindi attraverso una casella email istituzionale.

I docenti utilizzano **Drive** come repository di documenti anche da redigere simultaneamente (Documenti e Fogli Google). Ciò ha permesso di lavorare anche da remoto, senza duplicazione dei documenti originali e senza l'utilizzo di chiavette USB, con conseguente aumento della sicurezza informatica.

L'istituto ha avviato un numero sempre maggiore di classi digitali attraverso diverse piattaforme; a partire dall'a.s. 2020/2021 si adotterà esclusivamente **Classroom** per permettere la didattica non solo a distanza (DAD) ma digitale integrata (DDI): assegnazione, consegna, feedback sui compiti, condivisione di materiali digitali in diversi formati, anche semplificati, comunicazioni con gli allievi sia in gruppo classe che personalizzate. L'istituto ha elaborato un Piano Scolastico per la Didattica Digitale Integrata da allegare al Piano Triennale dell'Offerta Formativa.

Per le videoconferenze vengono utilizzate le piattaforme:

- **Google Meet** per le videoconferenze (videolezioni, incontri degli organi collegiali a numero ristretto, colloqui con i genitori, riunioni organizzative);
- **GoToMeeting** per i collegi docenti (numero di utenti superiore a 100).

---

## 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.

Si riportano, e integrano, brani tratti dal **Regolamento d'Istituto** approvato a settembre 2020.

L'utilizzo per motivi personali dei telefoni all'interno dell'Istituto è consentito ai docenti e agli alunni solo in caso di effettiva necessità.

Gli alunni sono tenuti a non fare uso personale dei cellulari e di altri dispositivi elettronici durante l'orario scolastico; inoltre hanno l'obbligo di rispettare il divieto di utilizzare fotocamere, videocamere, registratori vocali all'interno degli spazi scolastici tutti (palestre, mensa, cortile e

servizi igienici). Per esigenze didattiche e previa indicazione dei docenti, gli alunni possono usare il cellulare o altri dispositivi personali, come previsto dal Decalogo MIUR BYOD (Bring Your Own Device).

Nel tempo scuola, le comunicazioni famiglie-allievi avvengono tramite i numeri di telefono della scuola.

E' vietato anche agli insegnanti l'uso del cellulare in classe per motivi non didattici: fanno eccezione i docenti collaboratori del DS e responsabili di sede che hanno necessità di essere facilmente contattabili dalla scuola, nonché tutti i docenti che si trovino nella necessità di comunicare informazioni importanti in relazione alle regole di sicurezza in senso lato; i cellulari, se in possesso degli allievi durante il tempo scuola e non utilizzati per attività didattiche, devono essere tenuti spenti nello zaino in una tasca chiusa. L'allievo riaccenderà il cellulare solo quando si troverà fuori dalla scuola; tale disposizione mira a garantire la sicurezza degli allievi che devono scendere dalle scale e/o percorrere i corridoi per arrivare all'uscita.

E' consentito ai docenti portare a scuola il proprio dispositivo (tablet o pc, smartphone) e collegarlo alla rete wireless del proprio plesso utilizzando le credenziali personali fornite dall'Istituto, al solo scopo didattico o comunque relativo all'organizzazione delle attività dell'istituto.

Negli ultimi anni si è riscontrato un problema sempre maggiore nell'utilizzo consapevole dei mezzi informatici e soprattutto delle chat tra compagni di classe e tra genitori. Molto spesso il linguaggio usato non è adeguato, come anche la quantità di messaggi scambiata; si rileva la necessità di definire lo scopo dell'interazione tramite tale mezzo social e regole per il suo corretto utilizzo.

Quando i ragazzi si iscrivono alla scuola secondaria di primo grado sono già in buona parte dotati di uno smartphone, e sono iscritti a social network come Whatsapp, SnapChat, TikTok, Facebook, Instagram,... Quasi nessuno è consapevole di non avere ancora raggiunto l'età che ha previsto il legislatore per avere un account su tali piattaforme o servizi di messaggistica.

L'obiettivo principale diventa, quindi, la sensibilizzazione delle famiglie non solo nei confronti di un problema educativo, ma anche legislativo che dovrebbe tutelare il minore ritenuto non ancora in possesso di strumenti e risorse necessarie per fruire in modo corretto e consapevole delle potenzialità del web e delle TIC.

Altri importanti riferimenti per delineare le regole di corretto utilizzo delle tecnologie sono:

- il regolamento all'interno del **Piano Scolastico per la Didattica Digitale Integrata** allegato al Piano Triennale dell'Offerta Formativa;
  - l'**autorizzazione all'utilizzo della GSuite**, che include importanti regole per l'utilizzo corretto della piattaforma da parte degli studenti e delle studentesse.
-

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

---

### **AZIONI (da sviluppare nell'arco dell'anno scolastico):**

- 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

### **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 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).

---

## ***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.

- Promuovere, all'interno della programmazione curricolare, attività e/o laboratori sul tema del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc.
- Promuovere i buoni comportamenti digitali nell'utilizzo dei social.
- Organizzare laboratori in collaborazione con il Nucleo di Prossimità della Polizia Municipale sul tema "I rischi del mondo digitale", rivolti agli studenti della scuola secondaria.

---

## ***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?*

L'Istituto promuove azioni di prevenzione attraverso percorsi di benessere digitale durante le ore curricolari e durante i laboratori organizzati dal Nucleo di Prossimità.

---

## ***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.

---

## 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.

- Promuovere un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.

---

## 4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, **concrete o simulate** o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

**La legge n. 269 del 3 agosto 1998** "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce



nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella **legge n. 38 del 6 febbraio 2006** "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet", segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

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

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

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

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

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

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

**AZIONI (da sviluppare nell'arco dell'anno scolastico in corso).**

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli studenti/studentesse.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.
- Promuovere all'interno della programmazione curricolare attività e/o

laboratori sul tema del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc.

**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 studenti/studentesse, docenti e genitori con l'intervento di esperti.
- 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.
- Organizzare uno o più eventi e/o dibattiti, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse 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 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).

Nello specifico, il nostro istituto, per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, prevede i seguenti strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni; cyberbullismo@regioparco.org ;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti dell'Associazione "Parole in Movimento";
- docenti referenti per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito [1.96.96](tel:19696).

Sono indicate le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso:

- Referenti Bullismo e Cyberbullismo, Dirigente e Animatore digitale (gestione del caso);
- Docenti della classe, referenti di plesso, Psicologa (accoglienza);
- Referenti di plesso e referenti Bullismo e Cyberbullismo (presa in carico).

Inoltre, la scuola individua le figure che costituiranno un team preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti): Referenti Bullismo e cyberbullismo, Dirigente, Psicologa, Animatore digitale.

---

### ***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.

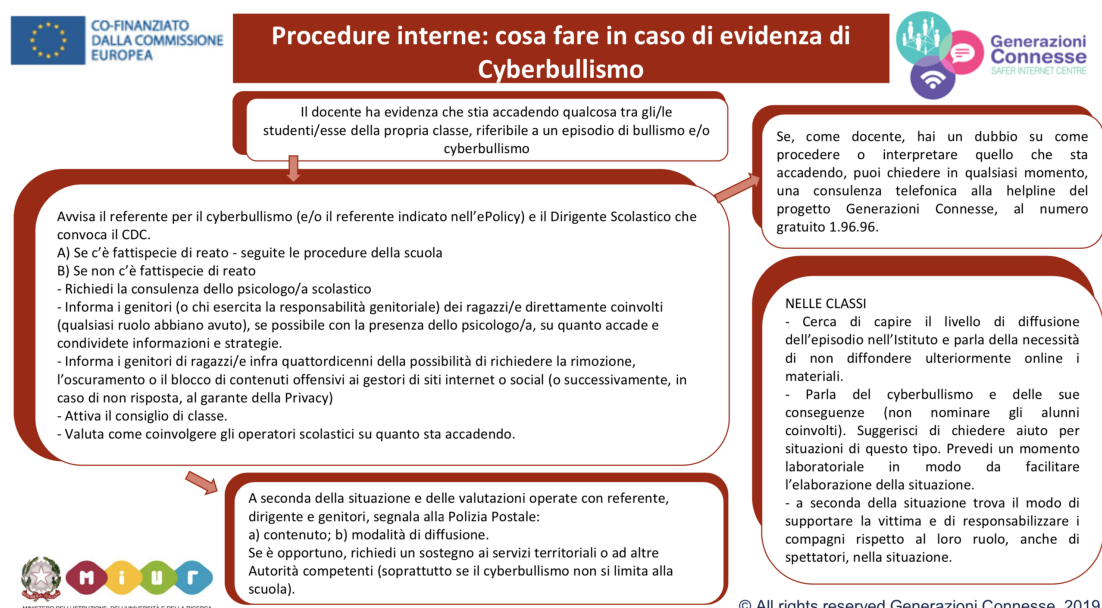
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

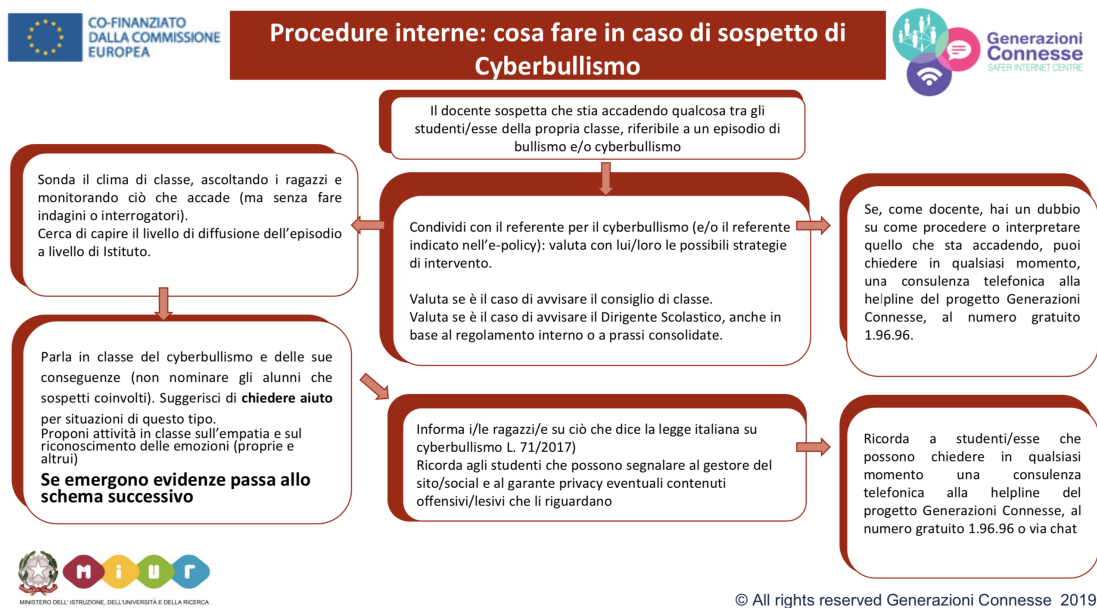
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.

- **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.

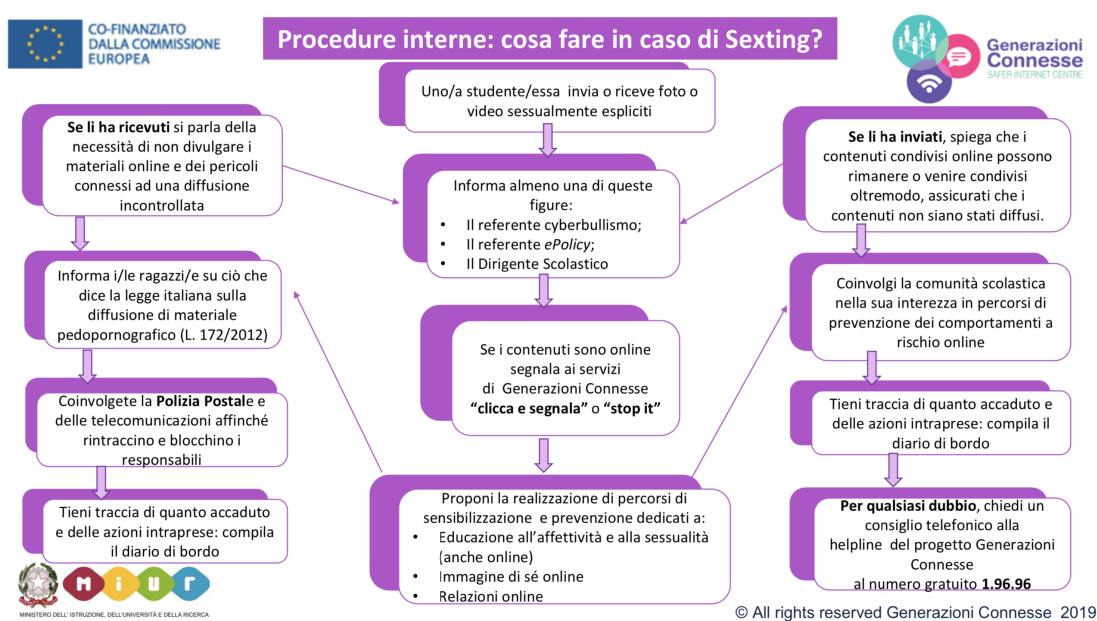
## 5.4. - Allegati con le procedure

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



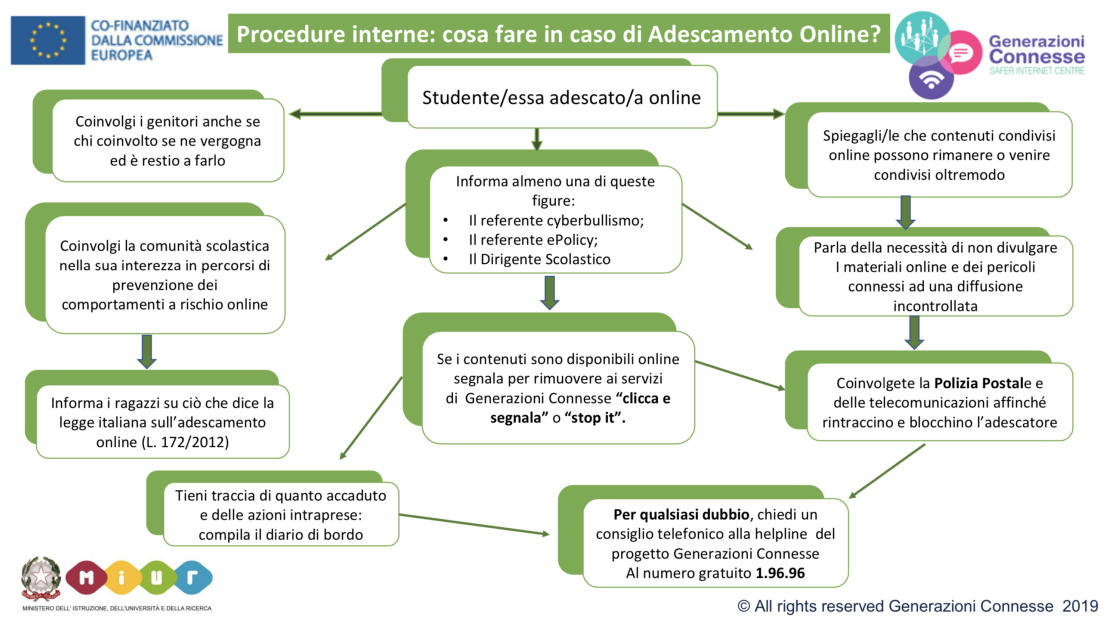


## Procedure interne: cosa fare in caso di sexting?

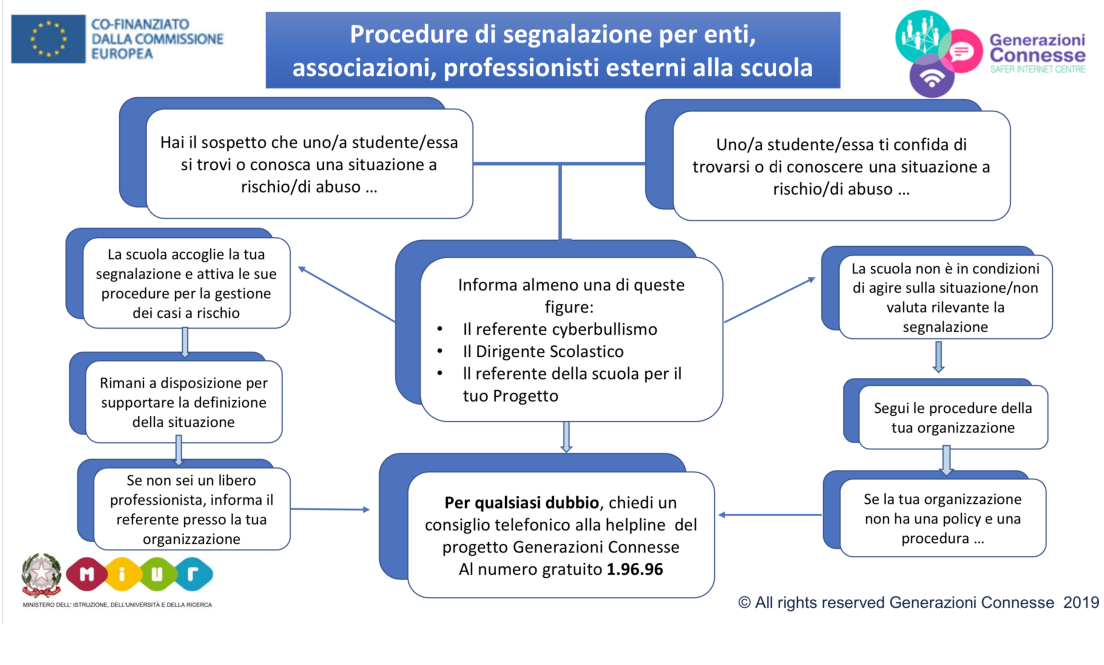


## Procedure interne: cosa fare in caso di adescamento online?





## 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***

- creazione e gestione condivisa casella di posta cyberbullismo@regioparco.org
- creazione sul sito della scuola di una sezione dedicata, di facile accesso, completa di modulistica e materiali per la segnalazione, a disposizione di famiglie e docenti
- diffusione, all'interno dell'Istituto Comprensivo della procedura da seguire per le segnalazioni.

