



# Documento di ePolicy

MIIC88200X

IC A. BENEDETTI MICHELANGELI

VIA DANTE10 - 20084 - LACCHIARELLA - MILANO (MI)

Andrea Ventura

# 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**

- **elabora in collaborazione con il referente del bullismo e cyberbullismo un regolamento condiviso per i fenomeni di bullismo e cyberbullismo**
- **è il garante della sicurezza anche online in collaborazione con l'amministratore di sistema, e le figure incaricate dell'Istituto**
- **promuove la cultura della sicurezza, organizzando corsi di formazione specifici sull'utilizzo responsabile delle TIC per tutte le figure scolastiche**
- **garantisce la tutela degli aspetti legali riguardanti la privacy in collaborazione con il DPO**
- **coordina la gestione degli episodi di bullismo e cyberbullismo in collaborazione con i docenti e il referente del bullismo e del cyberbullismo**

### **ANIMATORE DIGITALE**

- **supporta il personale scolastico sia dal punto di vista tecnico informatico, sia riguardo i rischi online e la protezione dei dati personali**
- **promuove percorsi di formazione interna all'istituto negli ambiti di**

### **sviluppo della "scuola digitale"**

- **monitora e rileva eventuali problematiche connesse all'uso delle TIC a scuola**

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

- **coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e cyberbullismo**
- **collabora con le realtà di rete extrascolastiche per la promozione di iniziative di formazione**
- **predispone il protocollo di istituto per il contrasto ai fenomeni di bullismo in collaborazione con il DS**
- **collabora con il DS e con i docenti nella gestione degli episodi di bullismo, cyberbullismo e uso improprio delle tecnologie digitali**
- **coordina il team antibullismo e per le emergenze**

### **I DOCENTI**

- **diffondono la cultura dell'utilizzo responsabile delle TIC e della rete e partecipano alle attività di formazione**
- **promuovono l'uso di tecnologie digitali nella didattica delle proprie discipline, supportando e riportano gli alunni nell'utilizzo consapevole delle TIC per scopi didattici**
- **assicurano la vigilanza degli alunni a loro affidati e promuovono la cultura dell'accoglienza e del rispetto nei confronti di tutti**
- **riconoscono eventuali episodi di bullismo e cyberbullismo e collaborano con il DS e con il referente nella gestione di essi**
- **segnalano al Dirigente problematiche, violazioni e abusi, anche online, che coinvolgono i loro studenti**

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

- **i collaboratori scolastici svolgono un ruolo di vigilanza attiva sugli alunni negli spazi loro assegnati (con particolare attenzione a tutti gli spazi comuni)**
- **il personale di segreteria svolge funzioni amministrative e contabili**
- **il personale ATA segnala al DS e al referente eventuali episodi di bullismo e cyberbullismo e collabora nella gestione di essi**

#### **GLI STUDENTI E LE STUDENTESSE**

- **partecipano alle attività di prevenzione organizzate dalla scuola**
- **adottano comportamenti responsabili in osservanza del Regolamento di Istituto, anche con riferimento all'utilizzo dei dispositivi digitali**
- **prendono le distanze, denunciano, segnalano tutti i comportamenti di bullismo e cyberbullismo di cui si trovano ad essere spettatori**
- **leggono, comprendono e accettano il documento il Regolamento di Istituto e dell'E-Safety Policy**

#### **GENITORI**

- **sono partecipi dell'educazione sull'uso consapevole delle TIC e della Rete**
- **sono responsabili dell'uso dei device personali dei propri figli e sono consapevoli delle potenziali implicazioni penali e civili per il minore e per la famiglia come conseguenza di atti di bullismo e cyberbullismo**
- **si relazionano in modo costruttivo con i docenti in un rapporto di sinergia e collaborazione**
- **partecipano attivamente alle attività promosse dall'istituto sull'utilizzo responsabile delle TIC**
- **accettano e condividono il documento eE-Safety Policy e firmano e il patto di Corresponsabilità Scuola-Famiglia**

## ENTI ED ASSOCIAZIONI ESTERNE

- **i professionisti che realizzano progetti nella scuola promuovono comportamenti sicuri e assicurano la protezione degli studenti e studentesse durante le attività**
  - **collaborano con la scuola per la realizzazione di percorsi di prevenzione e gestione del fenomeno del bullismo e del cyberbullismo**
- 

### ***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 erogano attività educative all'interno dell'Istituto prendono visione, accettano e condividono quanto è contenuto nella E-Policy. Adegua il loro comportamento al Codice di Comportamento dei dipendenti pubblici nel rispetto del Regolamento interno di Istituto.**

**L'istituto condivide le procedure di segnalazione con tutte le figure che operano con gli studenti; tali figure devono rispettare il protocollo di emergenza nel caso vengano a conoscenza uso non consapevole o abuso delle tecnologie digitali. Assicurano la collaborazione nella gestione dei casi di bullismo e cyberbullismo**

---

## ***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.

**Il documento E-Safety-Policy viene condiviso con l'intera comunità scolastica.**

**Nello specifico:**

- **con gli studenti, come base di partenza per un uso consapevole e maturo dei dispositivi e della tecnologia informatica. In particolare il capitolo 4 (che definisce e descrive il cyberbullismo e i rischi online) sarà oggetto di riflessione nell'ambito delle attività di educazione civica ed educazione alla cittadinanza digitale. I docenti si faranno promotori del documento.**

- **con i docenti, attraverso la pubblicazione dell'E-Safety-Policy sul sito istituzionale della scuola e attraverso la presentazione del documento stesso agli organi collegiali**
  - **con il personale ATA, attraverso la pubblicazione dell'E-Safety-Policy sul sito istituzionale della scuola**
  - **con i genitori, attraverso la pubblicazione dell'E-Safety-Policy sul sito istituzionale della scuola. La scuola ritiene fondamentale lavorare in sinergia con le famiglie, pertanto verranno organizzati momenti specifici di incontro con le famiglie finalizzati ad illustrare il documento**
  - **Con il Consiglio di Istituto (organo deputato alla approvazione del Regolamento interno)**
- 

## ***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.

**Gli usi errati e poco consapevoli delle tecnologie digitali a scuola da parte degli studenti:**

- **utilizzo del smartphone personale durante le ore di lezione**
- **scatti di immagini o registrazione di video di compagni/e e del personale scolastico senza il loro consenso**
- **scatti di immagini o registrazione di video di compagni/e e del personale scolastico senza il loro consenso che li ritraggano in pose offensive**
- **condivisione di dati personali**

- **condivisione di video e/o immagini finalizzati all'offesa, all'umiliazione e all'esclusione.**
- **utilizzo della rete per scopi ludici o interessi privati che esulano dalla didattica**
- **collegamenti a siti non adeguati e non indicati dai docenti**

#### **Le sanzioni:**

- **Hanno finalità educativa e sono ispirate al principio di responsabilizzazione personale e al ripristino di corretti rapporti all'interno della comunità scolastica.**
- **Sono sempre temporanee proporzionate all'età, alla gravità dei comportamenti e delle conseguenze da essi derivanti, alla situazione personale dell'alunno .**
- **Vanno comminate dopo aver effettuato la ricostruzione dell'accaduto e dopo aver invitato l'alunno ad esporre le proprie ragioni.**
- **La responsabilità disciplinare è personale**
- **L'applicazione di una sanzione non esclude la responsabilità dell'alunno in merito al risarcimento degli eventuali danni arrecati.**
- **Nessuna sanzione può influire sulla valutazione del profitto.**

#### **Tipologia delle sanzioni.**

- **Richiamo verbale da parte dei docenti e/o da parte del Dirigente Scolastico.**
- **Richiamo scritto da parte dei docenti con annotazione sul diario e, a seconda della gravità, anche sul registro di classe.**
- **Consegna da svolgere in classe o a casa.**
- **Sospensione dell'intervallo per l'alunno o per la classe per un periodo adeguato alla mancanza disciplinare.**
- **Sospensione dalle visite d'istruzione e/o attività didattiche esterne**

- **Sospensione dell'attività didattica con allontanamento dello studente per un periodo inferiore a 15 giorni, deliberata dal Consiglio di Classe ed eventuale attivazione di un percorso di riflessione per gli alunni e le famiglie in collaborazione con il servizio di Psicologia Scolastica .**
- **Sospensione dell'attività didattica con allontanamento dello studente per un periodo superiore a 15 giorni Deliberata dal Consiglio di Istituto su proposta del Consiglio di Classe convocato anche in seduta straordinaria. (art. 4 comma 6 D.P.R. 249/98) ed attivazione di un percorso di riflessione per gli alunni e le famiglie in collaborazione con il servizio di Psicologia Scolastica.**
- **Quando si è in presenza di fatti di rilevanza penale o vi sia pericolo per l'incolumità delle persone, la sanzione potrà comportare l'esclusione dallo scrutinio finale o la non ammissione all'esame (D.P.R. 249/98 e successivo D.P.R. 235/07).**
- **Nei casi di danneggiamento, sarà obbligo dei responsabili provvedere al risarcimento monetario del danno procurato.**
- **Attività di volontariato extrascolastiche previste dai protocolli territoriali attivi: a) "Protocollo di prevenzione e contrasto dei fenomeni di bullismo, cyber-bullismo e delle condotte antisociali, siglato da Comune di Lacchiarella, dall'Istituto Comprensivo e dalla Parrocchia Santa Maria Assunta"; b) Protocollo di prevenzione e contrasto dei fenomeni di bullismo, cyber-bullismo e delle condotte antisociali, siglato da Comune di Zibido San Giacomo, dall'Istituto Comprensivo e dalla Parrocchia**

**Previa la condivisione di questa scelta da parte dei genitori, viene predisposto un percorso educativo con finalità pro-sociali da svolgersi in orario extrascolastico.**

#### **Sostituzione delle sanzioni**

**Il Consiglio di classe (anche con riferimento alla normativa di contrasto al bullismo/cyberbullismo) può offrire allo studente la possibilità di sostituire le sanzioni deliberate con altri provvedimenti e incombenze .**

**Previa verifica da parte della scuola delle condizioni di realizzazione e la condivisione di questa scelta da parte dei genitori, questi compiti possono essere previste attività di:**

- a) **produzione di elaborati che inducano lo studente ad uno sforzo di riflessione e di rielaborazione critica degli episodi verificatisi;**
  - b) **collaborazione con il personale ausiliario;**
  - c) **volontariato nell'ambito della comunità scolastica;**
  - d) **operazioni di pulizia e ripristino degli arredi e /o dei locali scolastici;**
  - e) **la partecipazione ad attività di recupero e sensibilizzazione appositamente organizzate, anche insieme alla famiglia, ed in collaborazione con il Servizio di Psicologia Scolastica.**
- 

## ***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.

**Vengono aggiornati e strettamente correlati ai contenuti dell'E-Policy i documenti di Istituto, quali in primo luogo il Regolamento d'Istituto e il Protocollo di Gestione dei casi di Bullismo e Cyberbullismo**

---

## ***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.

**Ogni anno il gruppo di lavoro di docenti che si è occupato della redazione dell'E-Policy (coordinato dal Dirigente, dal Referente per il Cyberbullismo e l'animatore Digitale) , provvederà all'aggiornamento e alla verifica del documento stesso.**

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

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

- Presentare e condividere il documento e-Policy con gli alunni durante le lezioni di ed. civica (ed. digitale) a cura del gruppo di lavoro dell'e-policy.
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

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

- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori

# Capitolo 2 - Formazione e curriculum

---

## ***2.1. Curriculum sulle competenze digitali per gli studenti***

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

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

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

Lo studente al termine del primo ciclo, attraverso gli apprendimenti sviluppati a scuola, lo studio personale, le esperienze educative vissute in famiglia e nella comunità, è in grado di iniziare ad affrontare in autonomia e con responsabilità, le situazioni di vita tipiche della propria età, riflettendo ed esprimendo la propria personalità in tutte le sue dimensioni.

Ha buone competenze digitali, usa con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo

---

## ***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.

Sono previsti corsi di formazione per l'uso di piattaforme per l'insegnamento a distanza nei confronti di tutti i docenti dell'istituto in modo da permettere a tutti i docenti di effettuare didattica a distanza con gli studenti.

Sono inoltre previsti corsi di formazione per l'utilizzo base degli strumenti informatici in uso nell'istituto (PC, LIM...)

Tutti i docenti sono tenuti alla formazione in materia di privacy tramite corso con il DPO.

---

## ***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.

Nei corsi di formazione tenuti dall'animatore digitale si pone grande attenzione all'uso

di Internet in modo sicuro e quindi alle competenze sulla sicurezza digitale.

---

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

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

Il "Patto di corresponsabilità" prevede specifici riferimenti all'uso delle tecnologie digitali e all'ePolicy ed è fondamentale, quindi, per informare e rendere partecipi le famiglie sul percorso che si vuole intraprendere con il documento e il piano d'azione.

I genitori sono informati sulle condotte che si adotteranno a scuola e, in generale, si danno consigli da mettere in pratica con i propri figli. Alle famiglie sono fornite indicazioni su come

- **elaborare regole sull'uso delle tecnologie digitali** nelle comunicazioni con la scuola e con i docenti (es. mail, gruppo whatsapp, sito della scuola etc.) e sono informati adeguatamente anche riguardo alle regole per gli studenti e le studentesse;
  - **fornire linee guida sull'uso delle tecnologie digitali nella comunicazione** con i figli e in generale in famiglia
  - **organizzare percorsi di sensibilizzazione e formazione dei genitori** su un uso responsabile e costruttivo della Rete in famiglia e a scuola.
  - **prevedere azioni e strategie per il coinvolgimento delle famiglie** in tali percorsi di sensibilizzazione, ad esempio, mediante l'organizzazione di iniziative in cui anche gli studenti e le studentesse siano protagonisti.
-

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

---

### **AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022)**

#### **Scegliere almeno 1 di queste azioni**

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

#### **Scegliere almeno 1 di queste azioni**

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

# 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.

**In termini di dati personali il nostro istituto si è impegnato a:**

- Redigere e mantenere un registro dei trattamenti dei dati: sia per il titolare che per il responsabile dei trattamenti.
- Fare una valutazione dei rischi sulla privacy: (definita nel regolamento Data Protection Impact Assessment o PIA) relativamente ad alcune tipologie di trattamento dei dati sensibili come ad esempio dati relativi alle origini razziali per favorire l'integrazione degli/le alunni/e, dati relativi alle convinzioni religiose, al fine di garantire la libertà di culto, e dati relativi alla salute per adottare misure di sostegno degli/le alunni/e, come i dati vaccinali con le Asl.
- Fare un'analisi di processo sulla raccolta/gestione del consenso all'interno della modulistica e sul sito web istituzionale.
- adottare idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti:
- fare un'analisi del sito web istituzionale di riferimento con proposte volte a migliorare la sicurezza e la protezione dei dati trattati

a) il sito è migrato da suffissi gov.it (non più validi per le istituzioni scolastiche secondo la determina n. 36 del 12 febbraio 2018) al suffisso edu.it;

b) il sito è stato progettato secondo i concetti di privacy by default e by design

c) il sito utilizza il protocollo HTTPS (l'Hypertext Transfer Protocol Secure per proteggere l'integrità e la riservatezza dei dati scambiati online;

d) c'è un sistema di backup (sistema che permette di salvare regolarmente i dati; ripristinare eventuali file modificati o rimossi per errore dalla rete; garantire la presenza di una copia di sicurezza di tutti i file importanti);

- la intranet scolastica ha messo i seguenti dispositivi di sicurezza

a) sulle reti Wi-fi installate;

b) utilizzo di un proxy (un server che, ad esempio, si interpone nel flusso di comunicazione fra un computer e un sito Internet, eliminando il collegamento diretto fra il client e il server di destinazione. Permette di fornire un maggiore anonimato durante la navigazione in Rete, funziona da antivirus e memorizza una copia locale degli elementi web).

c) uso di un firewall hardware (componente [hardware](#) che, utilizzando un certo insieme di regole predefinite, permette di filtrare ed eventualmente bloccare tutto il

traffico da e verso una qualsiasi [rete di computer](#), lasciando passare solo tutto ciò che rispetta determinate regole);

Inoltre sono istituiti corsi di formazione destinati ai responsabili, agli incaricati ed eventualmente ai sub-incaricati del trattamento.

---

## **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.

**Nel regolamento scolastico è inserita una parte dedicata all'uso di Internet in cui gli studenti si impegnano a:**

- *utilizzare la rete nel modo corretto*
- *rispettare le consegne dei docenti*
- *non scaricare materiali e software senza autorizzazione*
- *non utilizzare unità removibili personali senza autorizzazione*
- *tenere spento lo smartphone durante lo svolgimento delle attività didattiche*
- *durante eventuali attività che prevedano l'utilizzo dello smartphone, utilizzarlo esclusivamente per svolgere le attività didattiche previste*
- *segnalare immediatamente materiali inadeguati ai propri insegnanti.*

**I docenti si impegnano a:**

- *utilizzare la rete nel modo corretto*
- *non utilizzare device personali se non per uso didattico*
- *formare gli studenti all'uso della rete*
- *dare consegne chiare e definire gli obiettivi delle attività*
- *monitorare l'uso che gli studenti fanno delle tecnologie a scuola.*

*Inoltre è stato anche predisposto un regolamento per la DAD sia per i docenti che per gli alunni e per i genitori.*

---

### **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.

Le piattaforme digitali istituzionali in dotazione all'Istituto sono:

- **Axios Registro Elettronico** che consente di gestire a 360° tutto il lavoro del Docente: valutazioni, assenze, note didattiche, argomenti di lezione e molto altro ancora.
- **Google Suite for Education (o GSuite)**, fornita gratuitamente da Google a tutti gli istituti scolastici con la

possibilità di gestire fino a 10.000 account utente. La GSuite in dotazione all'Istituto è associata al dominio della scuola e comprende un insieme di applicazioni sviluppate direttamente da Google, quali Gmail, Drive, Calendar, Documenti, Fogli, Presentazioni, Moduli, Hangouts Meet, Classroom.

---

### **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.

1. **La nostra scuola attraverso l'animatore digitale promuove le condizioni strutturali per l'uso delle tecnologie digitali.** Fornisce, per quanto possibile, i necessari servizi e l'indispensabile connettività, favorendo un uso responsabile dei dispositivi personali (BYOD). Le tecnologie digitali sono uno dei modi per sostenere il rinnovamento della scuola.
2. **La nostra scuola attraverso l'animatore digitale accoglie e promuove lo sviluppo del digitale nella didattica.** La presenza delle tecnologie digitali costituisce una sfida e un'opportunità per la didattica e per la cultura scolastica. Occorre coinvolgere l'intera comunità scolastica anche attraverso la formazione e lo sviluppo professionale.
3. **Il digitale nella didattica è una scelta che la nostra scuola attraverso l'animatore digitale sta percorrendo.** L'uso dei dispositivi in aula, siano essi analogici o digitali, è promosso da alcuni docenti, nei modi e nei tempi che ritengono più opportuni.

4. **Il digitale trasforma gli ambienti di apprendimento.** Le possibilità di apprendere sono ampliate, sia per la frequentazione di ambienti digitali e condivisi, sia per l'accesso alle informazioni, e grazie alla connessione continua con la classe.
5. **La nostra scuola tende a rafforzare la comunità scolastica e l'alleanza educativa con le famiglie.** È necessario che l'alleanza educativa tra scuola e famiglia si estenda alle questioni relative all'uso dei dispositivi personali. Le tecnologie digitali devono essere funzionali a questa collaborazione. Lo scopo condiviso è promuovere la crescita di cittadini autonomi e responsabili.
6. **La nostra scuola attraverso l'animatore digitale educa alla cittadinanza digitale.** Formare i futuri cittadini della società della conoscenza significa educare alla partecipazione responsabile, all'uso critico delle tecnologie, alla consapevolezza e alla costruzione delle proprie competenze in un mondo sempre più connesso.

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

---

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

**Scegliere almeno 1 di queste azioni:**

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- 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)

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

##### **Scegliere almeno 1 di queste azioni:**

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli
  - studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- 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.

**Il nostro Istituto lavora sulle competenze sociali degli alunni, in un progetto verticale di prevenzione universale (cioè rivolto a tutti, partendo dal**

**presupposto che tutti gli studenti possano essere potenzialmente a rischio). E' importante che tutti siano consapevoli del fatto che la prevaricazione esiste e, qualora un ragazzo ne sia spettatore, deve saper individuarla e opporsi.**

**Partendo dalla gestione dei litigi alla scuola dell'infanzia e primaria, si riflette sullo scherzo-scherno-prevaricazione.**

**Gli interventi di prevenzione selettiva vengono effettuati nei gruppi classe in cui si sono verificati episodi rilevanti di conflitto tra gli alunni. Vengono gestiti dallo psicologo/pedagogo, in alcuni casi è prevista anche la riflessione con i genitori.**

**Se invece l'intervento è specifico, su un alunno o su un gruppo di alunni che ha messo in atto comportamenti riconducibili al bullismo o al cyberbullismo o che ne è stato vittima, si parla di prevenzione indicata. E' sempre coinvolta la famiglia dei ragazzi, viene informata la dirigenza e il consiglio di classe. A seconda della gravità vengono intrapresi percorsi differenti che possono coinvolgere anche le forze dell'ordine, psicologi e medici. Agli alunni che hanno messo in atto episodi di bullismo si chiede di riconoscere e comprendere la sofferenza che le loro azioni possono aver causato nella vittima e si prevede un percorso di riparazione che porti alla consapevolezza dell'accaduto.**

---

## ***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).

**Il nostro Istituto ha sensibilizzato alunni e famiglie con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale attraverso interventi di esperti esterni nelle classi e serate dedicate al tema per i genitori.**

---

## ***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.

**Il nostro istituto organizza:**

- **incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, con la partecipazione attiva degli alunni;**
- **dibattiti in momenti scolastici, sui temi della diversità e sull'inclusione rivolti agli alunni;**
- **incontri con esperti esterni (psicologo/pedagogista) di educazione alla sessualità e all'affettività, rivolti agli alunni.**

---

## ***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?*

**Il nostro Istituto promuove interventi laboratoriali e di dibattito per alunni**

**dedicati all' Educazione Civica Digitale.**

---

## **4.5 - Sexting**

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti medialmente sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

La nostra scuola combatte il fenomeno dei sexting ponendo l'attenzione sulla necessità della prevenzione: i più giovani devono acquisire quelle competenze in grado di orientarli e guidarli nelle loro scelte anche online; per questo motivo, l'educazione, compresa l'educazione all'affettività, riveste un ruolo fondamentale su cui i nostri docenti sono molto attivi.

---

## **4.6 - Adescamento online**

Il **grooming** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenzialmente 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.

Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità e la nostra scuola è attiva su questo punto sia con tutto il corpo docente sia con l'ausilio di un supporto psicologico. Ciò aiuta a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori, docenti e psicologo devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e della sessualità.

---

## **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](#).**

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. Non è utile 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.

La nostra scuola è quindi molto attenta su questi punti.

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

**AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022).**

**Scegliere almeno 1 di queste azioni:**

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

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

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.

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.

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

##### **Scegliere almeno 1 di queste azioni:**

Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

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

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 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.

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 in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

# Capitolo 5 - Segnalazione e gestione dei casi

---

## 5.1. - Cosa segnalare

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

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire).

Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).

Nelle procedure:

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

Inoltre, la scuola **individua le figure che costituiranno un team** preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la **collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio** (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

**Tali procedure sono comunicate e condivise con l'intera comunità scolastica.**

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

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

La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

A seguire, le problematiche a cui fanno riferimento le procedure allegate:

- **Cyberbullismo:** è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/le studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online:** se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenni 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.

**Il personale del nostro istituto che venga a conoscenza di episodi cyberbullismo o situazioni rischiose in rete segnala al coordinatore di classe, che avvisa dirigenza e, eventualmente, il responsabile per il contrasto ai fenomeni di bullismo e cyberbullismo (si veda protocollo d'istituto).**

**Devono essere segnalati contenuti con specifici riferimenti a condotte di cyberbullismo, video, immagini e messaggi lesivi della dignità della persona, in cui siano contenuti dati personali, in cui vi siano elementi sessualmente espliciti e/o di incitamento all'odio.**

**Tali contenuti vengono denunciati alla polizia postale**

---

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

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

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

Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

- CASO A (SOSPETTO) - Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
- CASO B (EVIDENZA) - Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

Per tutti i dettagli fate riferimento agli allegati con le procedure.

---

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

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno

vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

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

Il nostro Istituto non prevede l'utilizzo della segnalazione anonima di episodi di cybullismo tramite box/ cassetta.

---

### ***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.

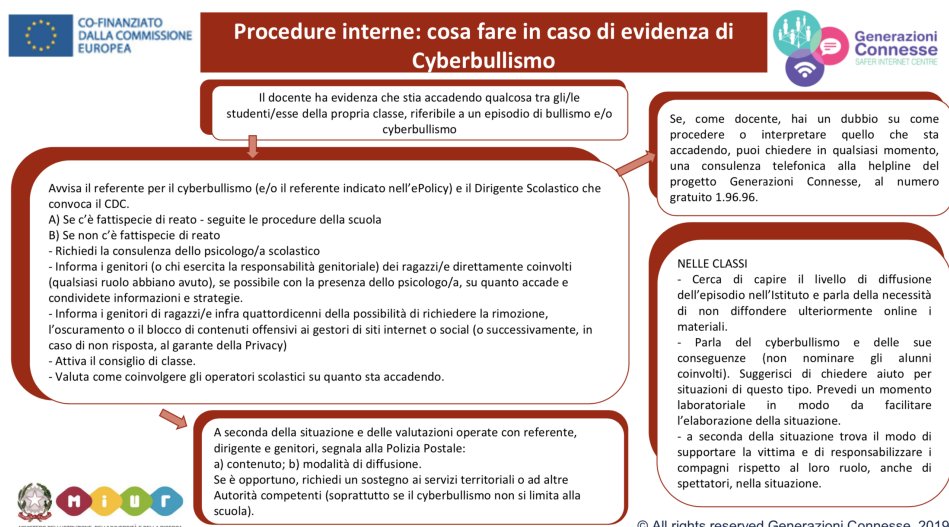
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di

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; raccolgono 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.

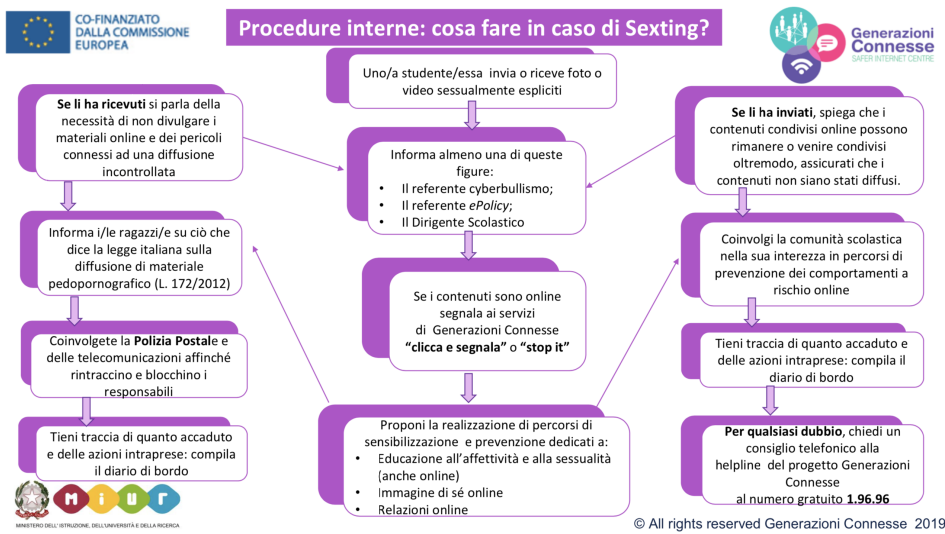
## 5.4. - Allegati con le procedure

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

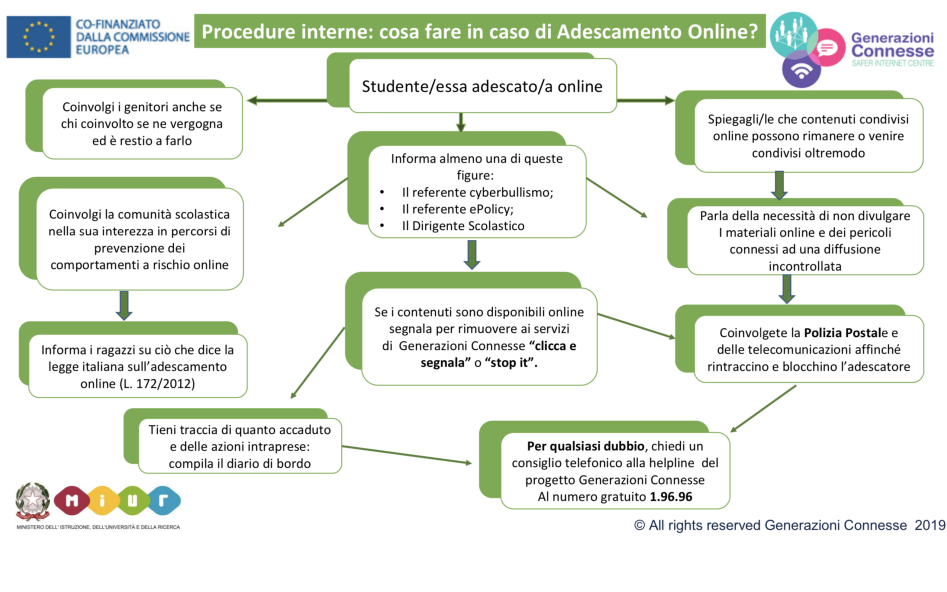




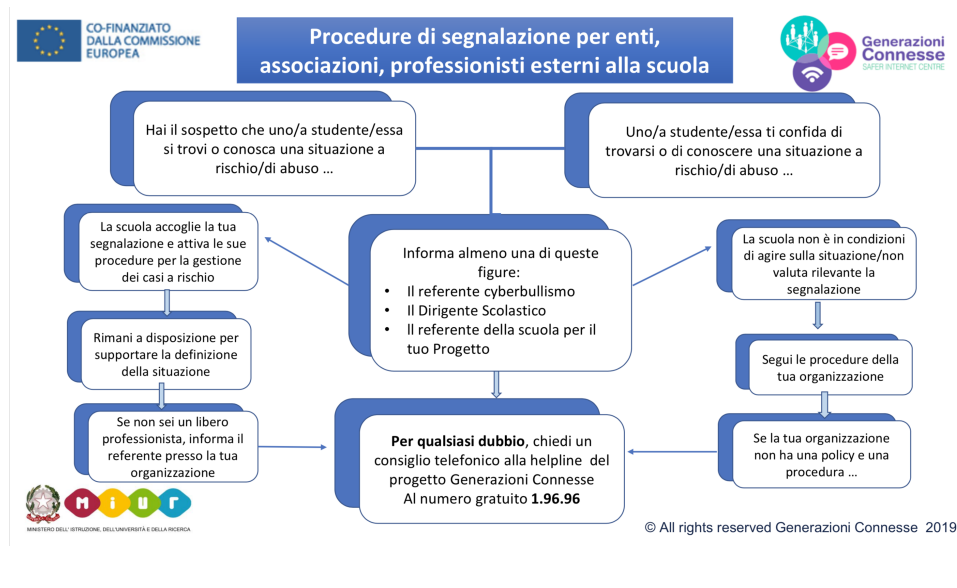
## Procedure interne: cosa fare in caso di sexting?



## 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***

**-Condividere con il personale docente le procedure di segnalazione.**

