

# Documento di ePolicy

CRIC803006

IC CASTELVERDE "U.FERRARI"

VIA UBALDO FERRARI 10 - 26022 - CASTELVERDE - CREMONA (CR)

Susanna Rossi

# 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.

**Della presente E-Policy sono parte integrante anche i seguenti Documenti**

**deliberati dagli Organi Collegiali dell'Istituto:**

**- REGOLAMENTO Disciplinare per l'uso corretto dei dispositivi elettronici atto a prevenire e contrastare IL BULLISMO E IL CYBERBULLISMO;**

**- LINEE GUIDA per la promozione di comportamenti adeguati e corrette abitudini con le Tecnologie dell'Informazione e della Comunicazione (TIC);**

**- PATTO EDUCATIVO DI CORRESPONSABILITA';**

**- Procedure "Cosa fare in caso di sospetto/certo caso di bullismo/cyberbullismo"**

---

## ***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'impegno nell'attuazione e promozione di essa.

**L'Istituto, in conformità delle linee generali dell'e-policy, individua i seguenti ruoli e responsabilità:**

**Dirigente Scolastico**

**ha il ruolo di promuovere l'uso a norma delle tecnologie e della Rete assumendosi le seguenti responsabilità:**

**a. garantire che tutti/e gli/le insegnanti ricevano una formazione adeguata per l'utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC);**

**b. garantire che le modalità di utilizzo corretto e sicuro delle TIC e di Internet siano integrate nel curriculum di studio (promozione delle competenze digitali, educazione civica...) e nelle attività didattiche ed educative delle classi;**

**c. garantire la sicurezza digitale offline/online dei membri della Comunità Scolastica;**

#### **Animatore Digitale/Team digitale**

**L'Animatore Digitale, Team Digitale e FFSS Multimedialità hanno i seguenti compiti:**

**a. Progettazione di attività di formazione legate alle competenze digitali dei docenti;**

**b. Implementazione della tecnologia multimediale nella pratica didattica quotidiana;**

**c. PON progettazione e presentazione delle candidature, gestione della GPU;**

**d. Ricerca di materiale didattico multimediale;**

**e. Consulenza informatica ai docenti;**

**f. Supporto ai docenti in caso di attivazione della D.D.I. (Didattica Digitale Integrata)**

**g. Supporto organizzativo alla segreteria;**

**h. Informatizzazione dei registri personale dei docenti e dei documenti di valutazione degli alunni;**

**i. Coordinamento, supervisione e collaudo degli acquisti tecnologici e digitali.**

**Referente educazione civica e gruppo e-policy**

**ha i seguenti compiti:**

**a. Si occupa del documento E-Policy dell'Istituto;**

**b. E' il referente per Generazioni Connesse;**

**c. si occupano della diffusione della Policy fra i colleghi;**

**d. si relaziona con i docenti della scuola, fornendo supporto in caso di difficoltà o dubbi in merito all'attuazione della Policy;**

**e. diffonde la cultura dell'uso responsabile delle TIC e della Rete, costruendo un curriculum digitale integrato con le altre discipline;**

**f. propone o organizza incontri formativi che hanno come tema la sicurezza on-line, i rischi della rete e la necessità di saper riconoscere situazioni potenzialmente pericolose;**

**g. Supporta il personale scolastico anche in riferimento ai rischi online;**

**Referente Bullismo e Cyberbullismo -**

**ha il compito di:**

**a. coordinare e promuovere le iniziative di prevenzione e contrasto del bullismo/cyber bullismo, coinvolgendo, con progetti e percorsi formativi ad hoc, studenti/esse, colleghi/e e genitori. A tal fine, può anche avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio;**

**b. può svolgere il compito di supporto al Dirigente Scolastico per la revisione/stesura di Regolamenti e atti;**

**Referente tecnico d'Istituto**

**Implementa l'uso (in collaborazione con la F.S. Multimedialità), nei PC scolastici, di sistemi di archiviazione (USB, memorie esterne), controlla la presenza di virus o malware.**

**Direttore dei servizi generali e amministrativi e Segreteria**

**hanno i seguenti compiti:**

**a. assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della Scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;**

**b. garantire il funzionamento dei diversi canali di comunicazione dell'Istituto (sportello, circolari, sito web, ecc.) all'interno delle Scuole e fra le Scuole e le famiglie degli/le alunni/e per la notifica di documenti e informazioni nell'ambito dell'utilizzo delle Tecnologie Digitali e della Rete;**

**c. curare la parte amministrativa legata alla elaborazione del Piano Diritto allo Studio e al Piano delle Attività attinente alle TIC.**

## **Coordinatori di classe e team docente**

**hanno i seguenti compiti:**

**- ad inizio anno illustra i documenti relativi alla corresponsabilità e alla sicurezza digitale dell'istituto;**

**- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle Tecnologie Digitali e della Rete e sulla politica di sicurezza adottata dalla Scuola, rispettandone il Regolamento (si veda sezione del sito dell'Istituto Regolamenti);**

**d. assicurare che gli/le alunni/e abbiano una chiara comprensione delle opportunità di ricerca offerte dalle Tecnologie Digitali e dalla Rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;**

**e. garantire che le Comunicazioni Digitali dei/le docenti con alunni/e e genitori siano svolte tramite le funzionalità del Registro Elettronico, di Gsuite o altre modalità stabilite dai docenti stessi nel rispetto del codice di comportamento professionale;**

**f. assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;**

**g. controllare l'uso delle Tecnologie Digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli/le alunni/e durante le lezioni e ogni altra attività scolastica (ove consentito);**

**h. nelle lezioni in cui è programmato l'utilizzo della Rete, guidare gli/le alunni/e a siti controllati e verificati, e controllare che nelle ricerche sulla Rete siano trovati e trattati solo materiali idonei;**

**i. segnalare qualsiasi problema/abuso o proposta di carattere tecnico organizzativo al Referente tecnico d'Istituto, all'Animatore Digitale, al Team Digitale, ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella Scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;**

**j. monitorare gli/le alunni/le per riconoscerne eventuali abusi, difficoltà o disagi rilevati a Scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo attraverso l'attivazione dei protocolli;**

**k. comunicare ai genitori tempestivamente difficoltà, bisogni o disagi espressi dagli/le alunni/e rilevati a scuola e connessi all'utilizzo delle TIC;**

**l. segnalare tempestivamente al Dirigente scolastico e ai genitori qualsiasi**

**abuso rilevato a scuola nei confronti degli/le alunni/e in relazione all'utilizzo delle tecnologie digitali o di Internet, per l'adozione delle procedure previste dalle norme;**

**- gestire in collaborazione con il/la referente bullismo e cyberbullismo la procedura in caso di sospetto/certo cyberbullismo;**

#### **Alunni**

**hanno il compito di:**

**a. essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle Tecnologie Digitali;**

**b. avere una adeguata comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;**

**c. comprendere l'importanza di adottare buone pratiche di sicurezza online quando si utilizzano le Tecnologie Digitali per non correre rischi;**

**d. adottare condotte rispettose degli altri anche e soprattutto quando si comunica in Rete, rispettando le norme della Privacy;**

**e. esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle TIC o della Rete ai docenti e ai genitori.**

#### **Genitori**

**il ruolo dei genitori degli/le alunni/e include i seguenti compiti:**

**a. sostenere la linea di condotta della Scuola adottata nei confronti dell'utilizzo delle Tecnologie dell'Informazione e delle Comunicazioni nella didattica;**

**c. relazionarsi in modo costruttivo per concordare con i/le docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle Tecnologie Digitali o della Rete;**

**d. fissare delle regole per l'utilizzo dei Dispositivi Digitali, farne un accorto monitoraggio, tenendo di conto dell'età e tenendo sotto controllo i comportamenti che i/le figli/e hanno soprattutto nella Rete e del cellulare;**

**e. accettare e condividere quanto scritto nell'e-policy dell'Istituto;**

**f. si daranno indicazioni sull'uso sicuro anche a casa (in riferimento ai siti sicuri per lo studio e l'approfondimento nonché attenzione ai sistemi di filtraggio).**

**gli Enti esterni e le Associazioni devono:**

**a. conformarsi alla politica della scuola riguardo l'uso consapevole delle TIC, della Rete e a quanto contenuto nel documento e-policy.**

---

### ***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).

**Le organizzazioni/associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve o/e lungo periodo, dovranno attenersi a quanto stilato nell' E-policy dell'Istituto.**

---

### ***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.

La scuola, nei momenti di confronto collegiale e istituzionale con i diversi attori della comunità educante condividerà il documento e-policy e tutti gli altri regolamenti che normano l'uso delle TIC e della Rete.

---

## ***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.

**L'Istituto sta elaborando un regolamento che coinvolge tutti gli ordini di scuola.**

---

## ***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.

**Pertanto specifici riferimenti alla E-policy, entro la fine dell'anno scolastico dovranno essere fatti nei seguenti documenti:**

- regolamento della Didattica Digitale Integrata

- regolamento uso di Gsuite

**Inoltre si ravvisa la necessità di integrare, il prima possibile, il Regolamento di Istituto con i seguenti Documenti:**

- **REGOLAMENTO Disciplinare per l'uso corretto dei dispositivi elettronici atto a prevenire e contrastare IL BULLISMO E IL CYBERBULLISMO;**

- **Manuale delle Procedure Privacy (Mdp) e Regolamento per l'utilizzo di Internet e della Posta Elettronica, per il suo completo superamento.**

**Inoltre ogni laboratorio di informatica dispone di uno Regolamento.**

---

## ***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 monitoraggio dell'E-Policy e del suo eventuale aggiornamento, attivato dal gruppo e-policy, è annuale.**

---

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

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

- 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
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- 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
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy 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.

Il nostro Istituto da anni ha elaborato un Curriculum verticale che comprende anche una parte dedicata all'alfabetizzazione informatica e alla cittadinanza digitale.

Il referente di educazione civica ha elaborato con il gruppo di riferimento un curriculum di cittadinanza.

---

## ***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'animatore digitale, il team digitale e le FFSS Multimedialità supportano i docenti nella formazione e autoformazione proponendo momenti in presenza/online per approfondire l'uso delle nuove tecnologie e delle piattaforme utilizzate nell'Istituto.

Si è provveduto anche ad organizzare corsi di formazione con enti esterni sulla didattica a distanza.

---

### ***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 Comprensivo si avvale della figura dell'Animatore digitale che, con il**

**Dirigente Scolastico e il D.S.G.A., collabora per raggiungere gli obiettivi di innovazione del PNSD nella scuola. Inoltre è attiva la figura del Referente d'Istituto per le attività di prevenzione e contrasto al bullismo e al cyberbullismo. La formazione sull'utilizzo consapevole e sicuro delle TIC è stata estesa ad altre figure.**

**Si rende, comunque, necessaria la formazione di tutti i docenti sull'uso**

**consapevole e sicuro di Internet e sui rischi della rete.**

Attenzione è stata anche data alla sicurezza informatica e alla privacy.

---

## ***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.

**Scuola** e famiglia sono chiamate a collaborare per garantire la crescita formativa di ciascun alunno, perciò stipulano, ad integrazione della E-safety Policy e del Regolamento disciplinare, all'inizio dell'anno scolastico, e a cui sono tenuti ad adeguarsi, il PATTO EDUCATIVO DI CORRESPONSABILITA', presentato durante le elezioni dei rappresentanti dei genitori ad ottobre.

---

### ***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 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.

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

**Scegliere almeno 1 di queste azioni**

- 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.

# 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.

**Il personale scolastico è "incaricato del trattamento" dei dati personali (degli/le alunni/e, dei genitori, ecc.) ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione).**

Viene fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli/le alunni/e eccedenti i trattamenti istituzionali obbligatori tramite apposito modulo.

**In merito alla protezione dei dati personali, si fa riferimento a quanto previsto dal Decreto Legislativo del 30 giugno 2003, n.196 (cosiddetto Codice della Privacy), integrato dal D. Lgs. 10 agosto 2018, n. 101, e dal GDPR (General Data Protection Regulation) n. 679 del 2016.**

**All'atto dell'iscrizione viene fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori, come per l'utilizzo di fotografie, video o altri materiali audiovisivi contenenti l'immagine e/o il nome del proprio figlio/a all'interno di attività educative e didattiche per scopi documentativi, formativi e informativi, durante gli anni di frequenza della scuola.**

In caso di partecipazioni a concorsi o manifestazioni l'Istituto richiede apposita autorizzazione, chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato all'interno di modulistica o sul proprio sito web istituzionale. La formula utilizzata per chiedere il consenso è, in ogni caso, comprensibile, semplice e chiara. Pertanto, in ottemperanza al GDPR (General Data Protection Regulation) e al D. Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre, la scuola non si impegna solo a tutelare la privacy degli/le studenti/esse e delle loro famiglie, ma anche ad informare e soprattutto rendere consapevoli gli/le studenti/esse di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri.

**Si veda il sito del Miur : <https://www.miur.gov.it/privacy-tra-i-banchi-di-scuola>**

**e quello del Garante della Privacy: <https://www.garanteprivacy.it/scuola>**

---

## ***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.

Tutti i plessi sono dotati di accesso a internet, rete cablata e wifi, utilizzata per la didattica.

L'amministrazione opera su rete separata e dedicata, adeguatamente protetta.

Le impostazioni dei dispositivi dei laboratori e delle aule sono definite e messe in opera dai referenti TIC di plesso e dal referente tecnico d'Istituto.

Gli alunni e gli studenti utilizzano i dispositivi e accedono a internet solo in presenza e con il controllo degli insegnanti, responsabili del loro comportamento, delle macchine e dei software in uso.

La modifica di installazioni, impostazioni e aggiornamenti dei software deve essere autorizzata dai referenti TIC, dall'animatore digitale o dal dirigente.

---

### ***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.

L'accesso ai laboratori multimediali dei plessi è regolato da orario settimanale per garantire un tempo minimo dedicato ad ogni classe.

L'accesso in orari diversi è su prenotazione per attività specifiche programmate.

L'uso di laboratori mobili viene definito secondo la progettazione delle classi o gruppi.

Ogni aula è dotata di connessione a internet e postazione docente destinate alla didattica d'aula.

I profili utente per la didattica sono ad accesso libero, i profili docente sono protetti da password.

L'utilizzo di strumenti personali connessi alle reti di Istituto dovrà essere autorizzato previo riconoscimento e registrazione.

Strumenti e supporti di memoria esterni devono essere protetti da sistemi di controllo dell'accesso e dei dati.

L'Istituto fornisce a tutto il personale interno un account e un indirizzo di posta elettronica per le comunicazioni professionali e, per i docenti, per l'uso della piattaforma didattica on line.

Analogo profilo è fornito agli alunni, finalizzato all'accesso e utilizzo della piattaforma didattica on line.

L'Istituto utilizza un sito web proprio, gestito attraverso piattaforma esterna per le comunicazioni generali all'utenza, come repository ad accesso libero o in aree riservate per modelli e documenti generali.

Per le comunicazioni scuola-famiglia si utilizzano il registro elettronico e la piattaforma didattica.

---

## **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.

I docenti possono utilizzare, per la didattica e la comunicazione professionale, dispositivi personali previo riconoscimento e accredito del dispositivo se connesso alle reti dell'Istituto.

Dispositivi personali degli studenti possono essere utilizzati esclusivamente per l'attività didattica, previo progetto e autorizzazione e sotto il controllo del docente e accredito del dispositivo.

---

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

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

**Scegliere almeno 1 di queste azioni:**

- **Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti / operatori scolastici**
- **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 il personale adulto 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:**

- **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)**

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

---

## 4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

- Nel caso della **sensibilizzazione** si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.
- Nel caso della **prevenzione** si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.

**L'Istituto Comprensivo adopera le seguenti azioni di prevenzione:**

- **informare e formare docenti, personale ATA e allievi sui rischi di un utilizzo non sicuro delle Nuove Tecnologie della Comunicazione con l'ausilio del Team Digitale, condividendoli successivamente con il personale della scuola;**

- **favorire il coinvolgimento dei genitori nel percorso del proprio figlio, quindi, nelle attività di formazione legate ad un uso corretto delle Nuove Tecnologie Digitali;**
  - **avvalersi della figura del referente che ha il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo.**
- 

## **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).

Per prevenire il Bullismo/Cyberbullismo i docenti, dopo aver individuato vittime e prepotenti, intervengono sul gruppo classe, attivando percorsi individualizzati, finalizzati ad accrescere i comportamenti cooperativi tra gli studenti.

Si sta lavorando alla stesura di un documento indicante le procedure di intervento in eventi/problema riconosciuti.

---

## ***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.

L'Istituto Comprensivo, per prevenire l'uso scorretto ed ostile del linguaggio, usato contro gruppi, persone, minoranze intende costruire progetti di continuità verticale, ispirandosi alle finalità ed agli obiettivi del Manifesto della comunicazione non ostile facilmente reperibile in rete e che rende disponibili documenti e linee guida per

attività ed interventi da proporre sulle classi. Il Manifesto è raggiungibile al seguente link:

<https://paroleostili.it/manifesto/>

---

## **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 Comprensivo partecipa alla rete di scopo regionale "Io non gioco più" che ha, tra i progetti proposti, la formazione e interventi per la prevenzione dalla dipendenza dal gioco d'azzardo. La stessa ATS e la rete delle Scuole che promuovono salute, a cui aderisce il nostro Istituto, forniscono supporto anche in accordo con la Prefettura di Cremona con cui ancora sussiste il Protocollo "Scuola spazio di legalità".

---

## **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.

Spesso tali immagini o video, anche se inviate ad una stretta cerchia di persone, si diffondono in modo incontrollabile, perché facilmente modificabili, scaricabili e condivisibili, e possono creare seri problemi, sia personali che legali, alla persona ritratta. L'invio di foto che riguardano minorenni in pose sessualmente esplicite configura, infatti, il reato di distribuzione di materiale pedopornografico.

Per prevenire tali problematiche, l'Istituto Comprensivo promuove percorsi di educazione all'affettività e alla sessualità e, anche nell'ambito dei percorsi di Cittadinanza e Costituzione, intende attivare percorsi finalizzati alla consapevolezza dei rischi collegati alla diffusione in rete.

---

## 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.

Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad esempio, all'adescatore. È importante che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove.

Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video...).

L'adescamento, inoltre, può essere una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di

Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.

Nei casi più estremi in cui l'adescamento porta ad un incontro fisico e ad un abuso sessuale un sostegno psicologico esperto per il minore è da considerarsi prioritario e urgente.

Le azioni specifiche verranno definite all'interno del protocollo di intervento sulle situazioni/problema.

Per consigli e per un supporto è possibile rivolgersi alla Helpline di Generazioni Connesse (19696).

---

## 4.7 - Pedopornografia

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

**La legge n. 269 del 3 agosto 1998** *“Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù”*, introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella **legge n. 38 del 6 febbraio 2006** *“Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet”*, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di *“pornografia minorile virtuale”* (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

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

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

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

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

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

L'esposizione o il coinvolgimento dei minori afferenti all'Istituto a situazioni di pedopornografia è da considerare evento particolarmente grave per gli aspetti educativi e psicosociali necessariamente delicati.

Qualora il personale dell'Istituto riceva notizia di un possibile evento di pedopornografia, dopo una semplice verifica dell'attendibilità dell'informazione, si provvederà a

- verificare le condizioni di sicurezza delle reti e dei supporti
- coinvolgere le autorità competenti per le opportune indagini e per la rimozione dei contenuti
- coinvolgere le figure professionali interne e territoriali per una valutazione dell'opportunità di supporti psicologici
- coinvolgere le strutture specializzate, per gli interventi di supporto psicologico/educativo specifico

## ***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 informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai docenti**

**con gli strumenti messi a disposizione dalla piattaforma ed eventualmente con l'intervento di esperti su problematiche specifiche.**

- 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,**

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

**Scegliere almeno 1 di queste azioni:**

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti 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.**
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori, con il coinvolgimento di esperti.**
- 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.**

# 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/lle 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.

**La scuola attraverso le figure dei docenti si è sempre impegnata a segnalare fatti ed eventi in qualche modo lesivi della dignità personale e attualmente le procedure sono in via di formalizzazione.**

---

## **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).

Conosciuto l'evento, il docente lo segnala ai colleghi del Consiglio di Classe o di Interclasse; all'interno del Consiglio si decidono quali azioni intraprendere, e, in base alla gravità, si coinvolgono:

- solo i genitori
- il referente del bullismo
- il Dirigente scolastico
- le forze dell'ordine.

Nel caso si riscontrino delle violazioni o degli eventi di tipo negativo che avvengono con strumenti digitali si provvederà a salvarne documentazione.

In caso di fatti accertati si strutturano attività da svolgere all'interno delle classi coinvolte allo scopo di sensibilizzare gli alunni alla necessità di rispettare l'identità altrui e all'uso consapevole degli strumenti digitali, sottolineando che lo spazio online è da ritenersi reale.

---

### **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.

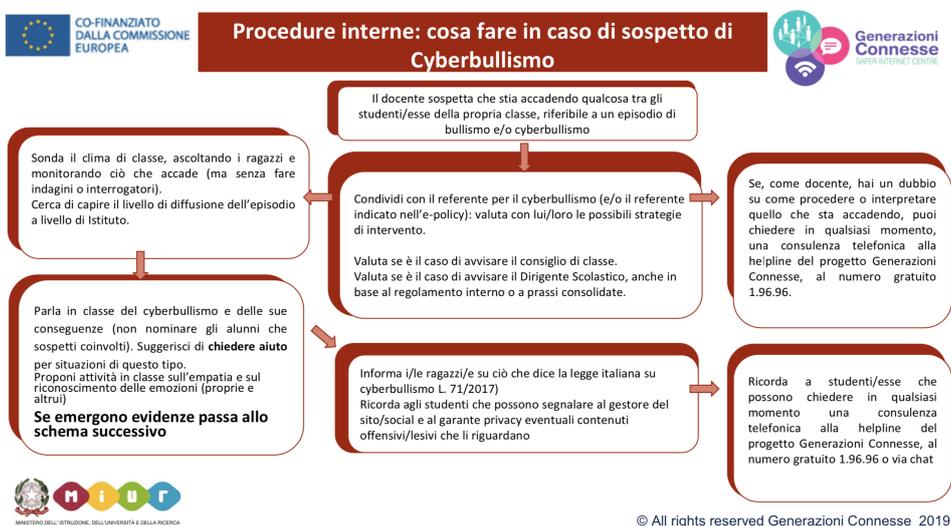
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

L'Istituto, oltre agli Enti e Servizi nazionali presenti sul territorio, si può avvalere del supporto della Prefettura di Cremona, con cui è in essere un protocollo firmato da tutti gli istituti scolastici della Provincia di Cremona, e con associazioni che agiscono nel campo giovanile.

---

## ***5.4. - Allegati con le procedure***

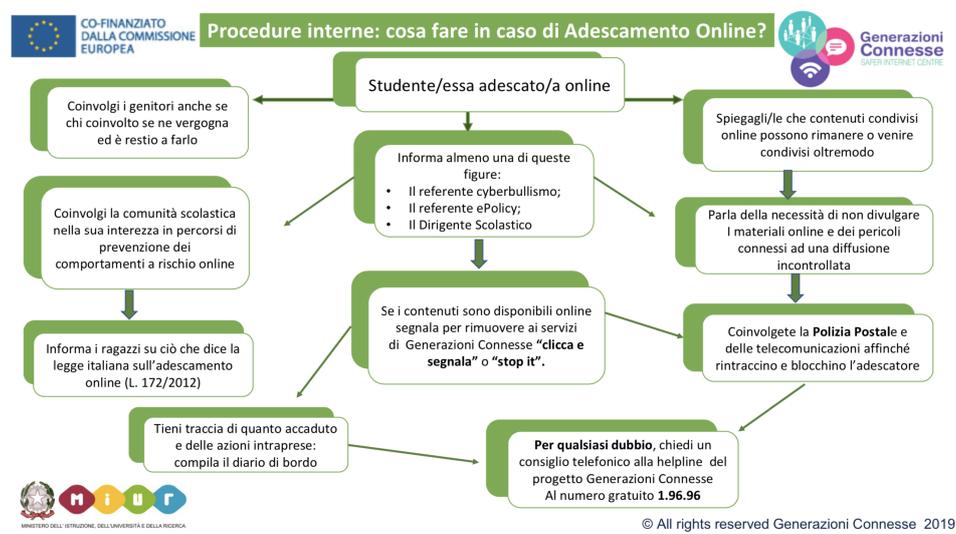
### **Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?**



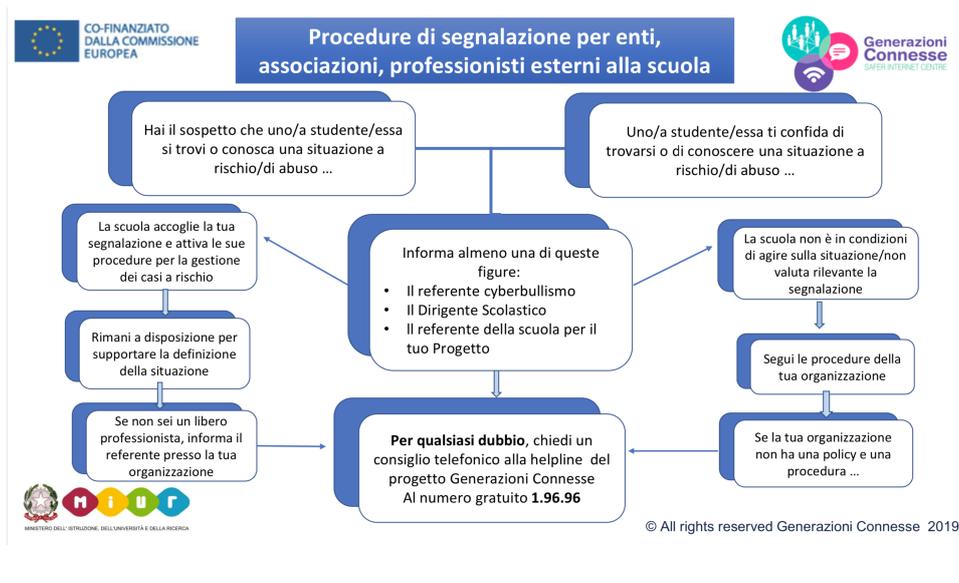
## Procedure interne: cosa fare in caso di sexting?



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



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



## Altri allegati

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

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

**Non è prevista nessuna azione.**

