



# Documento di ePolicy

TNIC825003

Istituto Comprensivo di Scuola Primaria e Secondaria di primo grado - LAVIS

Via Carlo Sette 13/A - 38017 - Lavis - PROVINCIA AUTONOMA DI TRENTO (TN)

FRANCESCA LASARACINA

# Capitolo 1 - Introduzione al documento di ePolicy

---

## ***1.1 - Scopo dell'ePolicy***

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.

Le "competenze digitali" sono fra le abilità chiave all'interno del [Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente](#) e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

## Argomenti del Documento

### 1. **Presentazione dell'ePolicy**

1. Scopo dell'ePolicy
2. Ruoli e responsabilità
3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
5. Gestione delle infrazioni alla ePolicy
6. Integrazione dell'ePolicy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

### 2. **Formazione e curriculum**

1. Curriculum sulle competenze digitali per gli studenti
2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
4. Sensibilizzazione delle famiglie e Patto di corresponsabilità

### 3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**

1. Protezione dei dati personali
2. Accesso ad Internet
3. Strumenti di comunicazione online
4. Strumentazione personale

### 4. **Rischi on line: conoscere, prevenire e rilevare**

1. Sensibilizzazione e prevenzione
2. Cyberbullismo: che cos'è e come prevenirlo
3. Hate speech: che cos'è e come prevenirlo
4. Dipendenza da Internet e gioco online
5. Sexting
6. Adescamento online
7. Pedopornografia

### 5. **Segnalazione e gestione dei casi**

1. Cosa segnalare
2. Come segnalare: quali strumenti e a chi
3. Gli attori sul territorio per intervenire
4. Allegati con le procedure

## Perché è importante dotarsi di una E-policy?

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi

all'uso di Internet.

L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

## ***1.2 - Ruoli e responsabilità***

Affinché l'E-policy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, s'impegni nell'attuazione e promozione di essa.

### **Dirigente Scolastico s'impegna a**

- garantire la sicurezza online dei membri della comunità scolastica, anche utilizzando un Internet Service filtrato approvato, conforme ai requisiti di legge vigenti;
- creare le condizioni affinché tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della Comunicazione (TIC);
- creare altresì le condizioni affinché tutto il personale scolastico riceva una formazione adeguata ai regolamenti scolastici;
- attuare le procedure previste dalle norme in caso di reclami e/o segnalazioni o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.
- accogliere le segnalazioni dei casi di presunto cyberbullismo e sovrintendere alla loro gestione, in collaborazione con il referente alla prevenzione e contrasto del Cyberbullismo.

### **Animatori Digitali e Gruppo di Lavoro TIC**

- si occupano della diffusione della ePolicy fra i colleghi, fornendo supporto in caso di difficoltà o dubbi in merito all'attuazione della stessa;
- sono promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della scuola digitale, previa rilevazione dei bisogni didattico - formativi dei docenti.

### **Tecnico-informatico di Istituto**

Su indicazione del Dirigente Scolastico:

- può accedere a tutti i file dell'area Intranet e controllarne i contenuti;
- limita, attraverso un proxy, l'accesso a determinati siti e gestisce il firewall presente in ciascun plesso scolastico;
- cura la manutenzione e la gestione dei laboratori informatici, dei laboratori mobili e di ogni altra apparecchiatura informatica, occupandosi anche dell'installazione di nuovi software.

### **Referente alla prevenzione e contrasto del Cyberbullismo**

- coordina e promuove le azioni di prevenzione e contrasto del cyberbullismo;
- in accordo con il Dirigente Scolastico, accoglie le segnalazioni dei casi di presunto Cyberbullismo e si avvale della collaborazione delle forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio;
- coinvolge studenti, docenti e genitori nella realizzazione di progetti e percorsi formativi;

### **Docenti e educatori**

- diffondono la cultura dell'uso responsabile delle TIC e della Rete, anche integrando parti del curriculum della propria disciplina con approfondimenti ad hoc;
- vigilano attivamente e attentamente gli alunni quando lavorano con le nuove tecnologie e li supportano in caso di difficoltà;
- utilizzano le tecnologie in modo consapevole e professionale in ambito scolastico;
- condividono con il proprio team docenti e/o Consiglio di Classe le situazioni di cui vengono a conoscenza e che considerano rischiose;
- segnalano al Dirigente Scolastico qualunque problematica, violazione o abuso che vede coinvolti studenti e studentesse.
- comunicano ai genitori difficoltà, bisogni o disagi espressi dagli alunni rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo.

### **Personale ATA**

- collabora nel controllo dell'uso delle tecnologie da parte degli studenti segnalando alla dirigenza, attraverso le procedure contenute nella Policy, le situazioni ritenute rischiose e stabilendo con essa eventuali tempi e modalità di azione.

### **Studenti e Studentesse**

- usano al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti e dalla presente ePolicy,
- online, tutelano e rispettano se stessi e i propri compagni;
- vengono coinvolti in progetti ed attività che riguardano l'uso positivo delle TIC

e della Rete;

- conoscono e rispettano i regolamenti scolastici dedicati anche all'attività didattica on-line;
- utilizzano responsabilmente le tecnologie e le immagini, comprendendo che l'utilizzo improprio rappresenta una lesione della privacy altrui e un reato punibile a tutti gli effetti;
- segnalano tempestivamente qualsiasi situazione ritengano rischiosa o riconoscano come abuso;
- in ambiente scolastico e/o nel corso di attività didattiche curricolari ed extracurricolari, utilizzano Internet in maniera responsabile, senza cercare o produrre materiale inappropriato o offensivo.

### **Genitori**

- affiancano l'istituto nel promuovere la sicurezza on-line, anche al di fuori del contesto scolastico;
- si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete;
- segnalano usi scorretti della Rete e comunicano con i docenti circa i problemi rilevati quando i propri figli non usano responsabilmente le tecnologie digitali o Internet;
- condividono la visione educativa-formativa e organizzativa prevista dalla ePolicy d'Istituto.

### **Enti Educativi esterni e Associazioni del territorio che collaborano con l'Istituto**

- si confrontano costruttivamente con la scuola riguardo all'uso consapevole della rete e delle TIC;

- promuovono comportamenti adeguati sulla sicurezza on-line e assicurano la protezione degli studenti e delle studentesse durante le attività che svolgono in collaborazione con l'Istituto;
  - condividono la visione educativa, formativa e organizzativa prevista dalla ePolicy d'Istituto consultabile sul sito.
- 

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

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

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

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

---



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

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/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.

---

## **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.

- Per le infrazioni e relative sanzioni previste dall'istituto si rimanda al Regolamento di Disciplina approvato e pubblicato sul sito della scuola al seguente indirizzo: <https://www.iclavvis.it/documenti/progetto-d-istituto>

## ***1.6 - Integrazione dell'ePolicy con Regolamenti esistenti***

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

---

## ***1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento***

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

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

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

- 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.

L’Istituto, per implementare le competenze digitali degli studenti, adotta le piattaforme didattiche ritenute idonee secondo le modalità specificate nel capitolo 3 del presente documento. Tenendo conto del [Piano Nazionale Scuola Digitale](#) (PNSD), in particolar modo il paragrafo 4.2. su “Competenze e contenuti”, [Sillabo sull’Educazione Civica Digitale](#) (presente sul sito GENERAZIONI CONNESSE), [DigComp 2.1](#) (quadro di riferimento per le competenze digitali dei cittadini, documento europeo per la catalogazione delle competenze digitali di base) e [Raccomandazione del Consiglio europeo](#) relativa alle competenze chiave per l’apprendimento permanente (C189/9, p. 9), considerando il [Piano Provinciale Scuola Digitale](#) e il Piano Digitale di Istituto ["La Rete Accogliente"](#), l’Istituto individua quattro aree di competenza da sviluppare che sono incluse nel curriculum dello studente:

- Area 1: “Alfabetizzazione su informazioni e dati”.

- Area 2: "Comunicazione e collaborazione".
  - Area 3: "Creazione di contenuti digitali".
  - Area 4: "Sicurezza".
- 

## ***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.

Tutto ciò anche alla luce dell'introduzione della **didattica digitale integrata** e della **didattica a distanza**.

Gli insegnanti dovrebbero avere o raggiungere un buon livello di formazione in merito all'utilizzo e l'integrazione delle TIC nella didattica, partendo da compiti semplici per arrivare a compiti più complessi.

Su tali premesse l'Istituto, attraverso il Collegio dei docenti, riconosce e favorisce la partecipazione del personale a diverse iniziative. Le attività possono essere promosse direttamente dalla scuola (ad es. con l'aiuto degli Animatori Digitali), da reti di scuole, dall'amministrazione o liberamente scelte dai docenti (anche online), purché restino coerenti con il piano di formazione.

Risulta ormai indispensabile l'uso delle TIC nella didattica: un loro utilizzo strutturato e integrato non solo può rendere gli apprendimenti motivanti, coinvolgenti ed inclusivi, ma permette al docente di guidare gli studenti ad una corretta fruizione dei contenuti online, ormai modalità naturale di apprendimento al di fuori della scuola. Inoltre le TIC permettono di sviluppare capacità che sono sempre più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza e il confronto fra pari in modalità asincrona.

Per creare una sinergia fra scuola, studenti e famiglie, al fine di promuovere la condivisione di buone pratiche nell'utilizzo consapevole delle TIC, è auspicabile che tutti i docenti dell'Istituto scolastico seguano un percorso formativo che abbia ad

oggetto i rischi legati all'uso responsabile e sicuro della Rete. Formare i docenti sulle tematiche in oggetto vuol dire non pensare esclusivamente all'alfabetizzazione ai media ma anche considerare la sfera emotiva e affettiva degli studenti che usano le nuove tecnologie.

---

## ***2.3 - Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali***

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

La scuola individua come primo strumento di formazione per docenti il sito [Generazioni Connesse](#).

---

## ***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.

Per i genitori degli studenti, la scuola individua, come primo strumento di approfondimento delle tematiche in oggetto, il sito [generazioni.connesse](#). Oggi più che mai è importante rinforzare l'alleanza educativa fra scuola e famiglie. Sarebbe opportuno aggiornare o integrare, oltre che il regolamento scolastico, anche il "Patto di corresponsabilità", con specifici riferimenti alle tecnologie digitali e all'ePolicy, per informare e rendere partecipi le famiglie. A tale proposito è importante rendere partecipi i genitori sulle condotte che si dovranno adottare a scuola e, in generale, offrire loro consigli da mettere in pratica con i propri figli, in riferimento ai rischi connessi ad un uso distorto della Rete da parte degli studenti.

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

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

- Realizzazione di una sezione dedicata alla ePolicy sul sito della scuola.
- Redazione dell'estratto della ePolicy

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

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali (corso obbligatorio).
- Organizzare alcuni incontri formativi all'anno con enti esterni in merito agli obiettivi previsti dal Piano Digitale di Istituto e della Didattica Digitale Integrata;
- Organizzare alcuni incontri formativi all'anno con enti esterni in merito all'uso consapevole e sicuro di Internet e delle tecnologie digitali;





# Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT della e nella scuola

---

## 3.1 - Protezione dei dati personali

*“Le scuole sono chiamate ogni giorno ad affrontare la sfida più difficile, quella di educare le nuove generazioni non solo alla conoscenza di nozioni basilari e alla trasmissione del sapere, ma soprattutto al rispetto dei valori fondanti di una società. Nell'era di Internet e in presenza di nuove forme di comunicazione questo compito diventa ancora più cruciale. È importante riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino”.*

(cfr. <http://www.garanteprivacy.it/scuola>).

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il “corretto trattamento dei dati personali” a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni.

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre.

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare

riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori. A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali.

Per approfondire rimandiamo al [Sito del Garante della Privacy](#) e al seguente vademecum [Social privacy Come tutelarsi nell'era dei social-network](#)

Si rinvia inoltre alla sezione del sito web della scuola dedicata alla Privacy ([www.iclavis.it/privacy](http://www.iclavis.it/privacy)) oppure ai documenti di seguito elencati:

- [Informativa Privacy alunni e genitori](#)
- [Informativa Privacy gestione dati personali sito web](#)
- [Informativa G-Suite Ic Lavis e Richiesta consenso](#)

---

## **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.

Tali obiettivi sono condivisi anche dal [Piano Provinciale Scuola Digitale](#) e dal Piano Digitale d'Istituto "[La Rete Accogliente](#)".

La scuola garantisce al personale scolastico e agli studenti il diritto a internet attraverso un'infrastruttura di rete adeguata alle necessità di ciascun plesso e in grado di supportare il traffico dati generato da un numero elevato di utenti. La connessione è in fibra ed è cablata sulla quasi totalità dell'istituto; è infine dotata di firewall gestiti direttamente dall'amministratore di Rete.

Interventi periodici di manutenzione e verifica sono programmati dalla Dirigenza Scolastica in accordo con il tecnico-informatico della scuola. Altre verifiche possono essere compiute su segnalazione degli Animatori Digitali, dei referenti dei Laboratori Informatici di plesso e delle coordinatrici di plesso.

La segreteria didattica, quella amministrativa, l'ufficio della RAS/FAS e della Dirigenza Scolastica sono connesse a rete LAN dedicata e a server indipendente ubicato in un'aula appositamente predisposta all'interno del plesso scolastico della sede centrale.

### **L'infrastruttura tecnologica dell'Istituto è così costituita:**

#### **SSPG LAVIS:**

RETE WIFI: copre tutto l'edificio principale, altri AP fuori dal controller sono stati collocati nelle aule non raggiunte da un forte segnale.

RETE CABLATA: copre tutto l'edificio, senza eccezione. Tutti i dispositivi che possono essere messi in dominio, sono collegati a questa rete.

FIREWALL: al momento è installato OPENDNS sul server della didattica; in fase di rinnovo della licenza.

**SP LAVIS:**

RETE WIFI: copre tutto l'edificio principale.

RETE CABLATA: copre tutto l'edificio, senza eccezione. Tutti i dispositivi che possono essere messi in dominio, sono collegati a questa rete.

FIREWALL: collegato e attivo, in attesa di rinnovo della licenza

**SP PRESSANO:**

RETE WIFI: copre tutto l'edificio principale, ad eccezione della bidelleria e della mensa al piano terra. Ci sono 2 AP, i quali coprono un piano ciascuno.

RETE CABLATA: copre tutto l'edificio, senza eccezione. Tutti i dispositivi che possono essere messi in dominio, sono collegati a questa rete.

FIREWALL: collegato e attivo, in attesa di rinnovo della licenza.

**SP ZAMBANA:**

RETE WIFI copre tutto l'edificio principale.

RETE CABLATA copre tutto l'edificio, senza eccezione. Tutti i dispositivi che possono essere messi in dominio, sono collegati a questa rete.

FIREWALL: è attivo il servizio firewall, utilizziamo Zyxel.

---

## ***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.

[Il sito web della scuola](#) è lo strumento utilizzato dall'Istituto per raggiungere le seguenti finalità:

- fornire una vetrina che promuova e valorizzi le attività dell'istituto;
- fornire informazioni relative alla propria organizzazione;
- fornire modulistica alle famiglie;
- essere una bacheca informativa per comunicare contenuti importanti alla comunità scolastica ed extrascolastica.

L'Istituto è fornito inoltre di un **Sito Intranet** per gestire e organizzare il flusso delle informazioni per docenti e personale ATA.

L' Istituto utilizza il **REL (registro elettronico)** quale strumento per gestire in modo veloce e efficace una comunicazione capillare tra scuola e famiglia. In particolare le famiglie possono, attraverso di esso, visualizzare molte informazioni utili:

- andamento scolastico (assenze, argomenti lezioni, note disciplinari);
- risultati scolastici (voti, documenti di valutazione);
- udienze (prenotazioni colloqui individuali);
- eventi (agenda eventi);
- circolari e comunicazione varie (comunicazioni di classe, comunicazioni personali).

L'Istituto esclude l'utilizzo dei social media quale strumento utile per qualsivoglia comunicazione scuola/famiglia.

In ambito prettamente didattico, la scuola attualmente adotta per tutto il personale e gli studenti la **Google Workspace for Education**, una piattaforma integrata a marchio Google che consente di comunicare e di gestire contenuti didattico - digitali con grande semplicità e flessibilità. L'utilizzo della Google Suite è ritenuta indispensabile per realizzare le azioni didattiche previste dalla Didattica Digitale Integrata.

Inoltre le Apps di Google garantiscono sicurezza e privacy, connessione e interoperabilità, comunicazione facilitata tra docenti e studenti.

Ciascun utente, attraverso un account personale, ha accesso a una serie di servizi tra i quali i principali sono:

#### **Per gli studenti**

- una casella di posta (**studente.nome.cognome@iclavis.it**), con spazio di archiviazione illimitato, attiva solo per il tempo di permanenza nell'Istituto;
- **Google Drive** che permette di archiviare e condividere online tutti i tipi di file, senza limiti di spazio;
- **Google Classroom**, per poter accedere all'ambiente virtuale di classe nel quale lavorare attivamente in modalità sincrona e asincrona con i propri docenti;
- **Google Meet**, utilizzato per partecipare a video-lezioni in caso di Didattica a Distanza.

### Per i docenti

- una casella di posta personale (**nome.cognome@iclavis.it**), con spazio di archiviazione illimitato;
- una casella di posta personale (**nome.cognome@scuole.provincia.tn.it**), con spazio di archiviazione illimitato;
- **Google Drive**, che permette di archiviare online tutti i tipi di file, senza limiti di spazio;
- **Google Classroom**, app che viene utilizzata per poter creare l'ambiente virtuale di classe nel quale lavorare attivamente con i propri studenti, in modalità sincrona e asincrona;
- **Google Meet**, utilizzato per riunioni collegiali d'Istituto, per gestire video-lezioni con gli studenti in caso di Didattica a Distanza, per riunioni e colloqui individuali con le famiglie.

### Per i genitori

- una casella di posta per ciascun genitore (**genitore.nome.cognome@iclavis.it**), con spazio di archiviazione illimitato, attiva solo per il tempo di permanenza nell'Istituto del proprio figlio; ogni genitore utilizza tale indirizzo di posta elettronica per comunicare con la Segreteria Studenti, con la Segreteria Amministrativa, con il Dirigente Scolastico, con i docenti, con il tecnico-informatico;
- **Google Meet**, utilizzato per partecipare alle video riunioni scuola/famiglia.

Tutti gli utenti sono consapevoli che, dal momento in cui ricevono le credenziali di accesso, tutti i servizi offerti sono dedicati ad un utilizzo esclusivamente scolastico e didattico.

Le famiglie concedono l'autorizzazione alla creazione dell'account e all'utilizzo della Google Suite da parte dei figli compilando apposito form. Parimenti concedono l'autorizzazione all'utilizzo di alcune piattaforme e applicazioni digitali a scopo didattico, disponibili su internet ed esterne alla G-Suite, che potranno essere utilizzate dagli alunni durante lo svolgimento di alcune attività scolastiche.

Dal momento in cui gli account degli studenti vengono creati e attivati, i genitori sono responsabili della vigilanza sull'utilizzo della casella di posta elettronica e delle app ad essa collegate, sia sul dispositivo fisso di casa che sui dispositivi mobili di proprietà degli studenti, avendo sempre cura che le finalità di utilizzo siano esclusivamente didattiche.

Le caselle di posta elettronica degli utenti sono impostate in modo tale da non permettere la registrazione su piattaforme di gioco online e sui social network a uso personale.

I docenti sono tenuti a tenere aggiornati i pc di classe, cancellando con frequenza dati sensibili e documenti superflui e/o archiviando nel proprio Drive personale tutti i file

utilizzati. Parimenti gli insegnanti sono tenuti a non salvare sui pc collocati in aree comuni file personali o contenenti dati personali degli alunni.

Gli aggiornamenti periodici sia del software che del Sistema operativo, così come la manutenzione di tutti i pc e i device, sono gestiti unicamente dal tecnico informatico di Istituto.

La scuola garantisce formazione adeguata a tutto il personale scolastico sulla gestione dei dispositivi elettronici e sulle regole basilari della sicurezza.

---

## **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 dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella delle/gli studentesse/ti e delle/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.

Risulta fondamentale per la comunità scolastica mantenere un dialogo sempre aperto su questa tematica e alimentare la riflessione affinché l'Istituto possa dotarsi e/o

mantenere aggiornata una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

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

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

- Organizzazione di interventi volti a formare e rendere consapevole la comunità scolastica sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity);
- Organizzare Caffè Digitali per il personale docente quali occasioni di formazione, di approfondimento e di confronto sulla gestione dei dispositivi elettronici, della G-Suite e dei principali sistemi di archiviazione online, di varie piattaforme ed app dedicate alla didattica;
- Sostituire dispositivi elettronici obsoleti.

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

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



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

---

## 4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

## 4.2 - Cyberbullismo: che cos'è e come prevenirlo

La legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", nell'art. 1, comma 2, definisce il cyberbullismo:

*"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo".*

La stessa legge e le relative **Linee di orientamento per la prevenzione e il contrasto del cyberbullismo** indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di [cyberbullismo](#) e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
  - Ha il compito di coordinare le iniziative di prevenzione e contrasto del [cyberbullismo](#). A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
  - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

---

## **4.3 - Hate speech: che cos'è e come prevenirlo**

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

**Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:**

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

All'interno della programmazione di **Educazione Civica e alla Cittadinanza** di ogni anno scolastico, è prevista la trattazione di questo argomento declinato nelle varie discipline e adattato, come contenuti, all'età degli alunni coinvolti.

---

## **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 è intenzionato ad organizzare, durante il corso del prossimo triennio, un incontro con esperti esterni, destinato ai genitori, per approfondire tale tematica. Nel caso si presenti la necessità o si manifesti l'interesse dei ragazzi, l'argomento sarà trattato dai docenti in classe.

---

## **4.5 - Sexting**

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

Ogni anno scolastico e in particolar modo in caso di effettiva necessità il nostro Istituto intende promuovere attività curricolari e/o extracurricolari attraverso le quali affrontare le problematiche connesse al fenomeno in questione. Inoltre intende fornire al personale della scuola, agli studenti e alle loro famiglie strumenti finalizzati al riconoscimento e alla prevenzione del fenomeno stesso.

---

## **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.

E' già consolidata un'attività svolta dalla Polizia Postale che tratta questa tematica. In momenti separati, alunni, genitori e docenti, vengono informati e allertati sulla pericolosità del fenomeno attraverso il racconto di fatti realmente avvenuti.

---

## **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'Istituto farà in modo di concordare con la Polizia Postale che nell'incontro con i genitori si affronti la tematica della pedopornografia on line fornendo anche ai genitori i contatti utili per le eventuali segnalazioni.

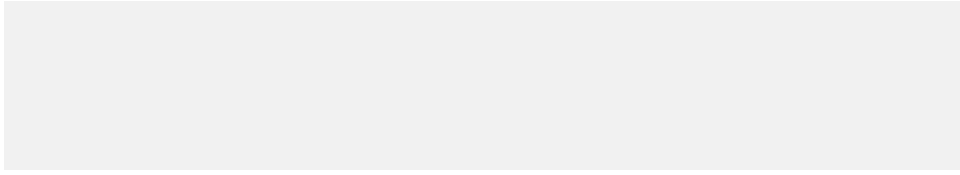
## ***Il nostro piano d'azioni***

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

- 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 e ai docenti, con il coinvolgimento di esperti.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.

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

- Promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.



# 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 condivisione avverrà attraverso assemblee scolastiche, riunioni con i genitori e momenti in classe dedicati all'ECC, in modo da coinvolgere 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.

---

## **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).

E' comunque auspicabile ed opportuno che ciascun studente e studentessa, in primo luogo possa fare riferimento ai propri docenti di classe.

#### **Fasi di segnalazione da parte del docente o del personale scolastico:**

- il docente comunica l'accaduto direttamente alle referenti al contrasto e alla prevenzione del Cyberbullismo e/o al Dirigente Scolastico: se lo reputa necessario, compila il modulo per la segnalazione del presunto caso di cyberbullismo (Allegato1) scaricabile dall'apposita sezione dell'Intranet dell'IC.
- conservare le prove dell'accaduto e riportare eventuali testimonianze alle referenti al contrasto e alla prevenzione del Cyberbullismo e al Dirigente Scolastico, per cercare di comprendere meglio la situazione.
- l'insegnante concorda con le referenti del Cyberbullismo e con il Dirigente Scolastico come intervenire e se coinvolgere eventuali figure esterne.

---

## **5.3. - Gli attori sul territorio**

Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

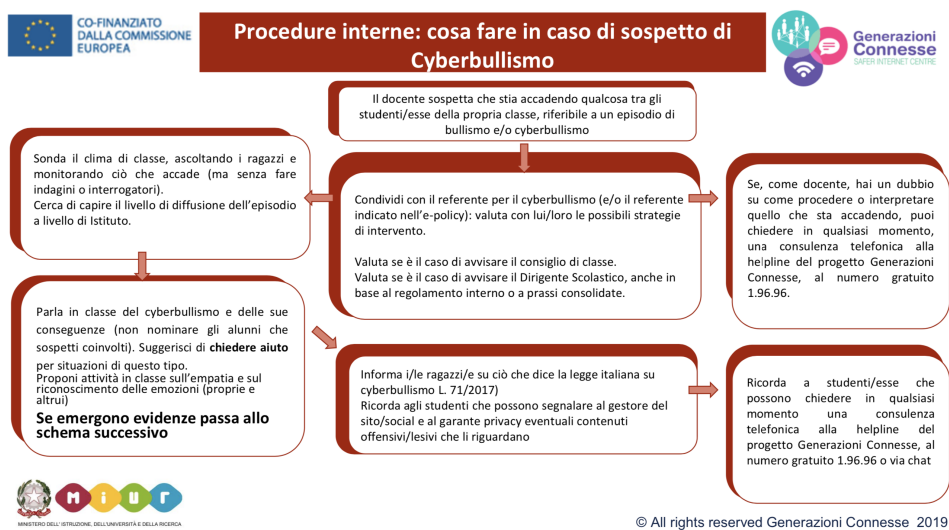
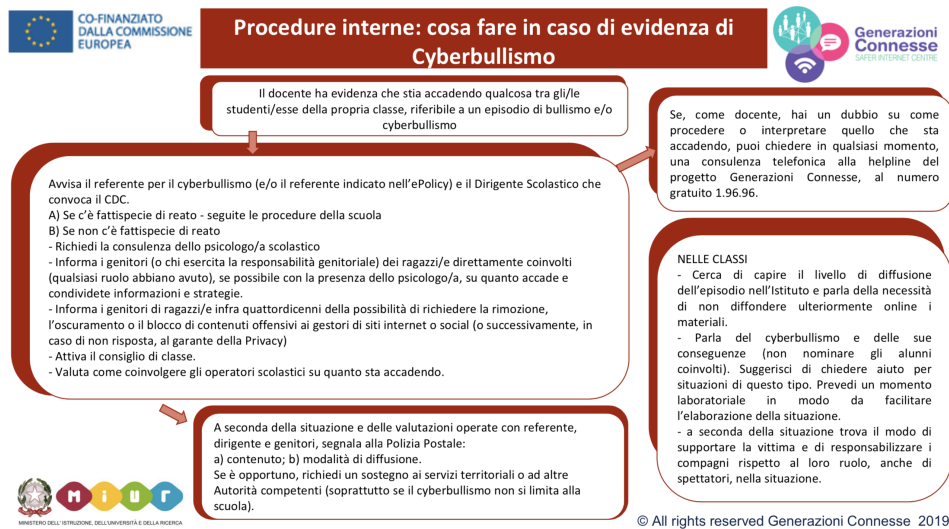
Per una mappatura degli indirizzi di tali strutture è possibile consultare il [Vademecum](#) di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

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

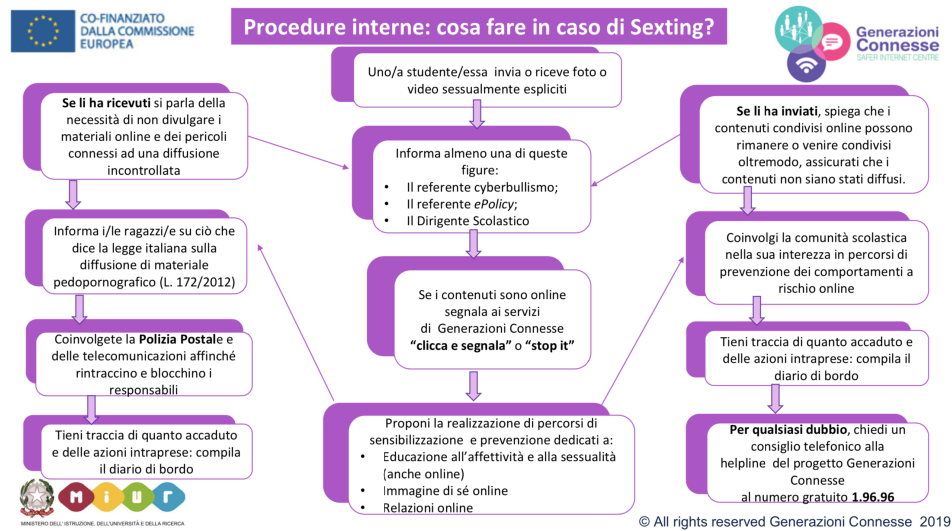
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale:** supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni:** accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali:** forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico:** segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

## 5.4. - Allegati con le procedure

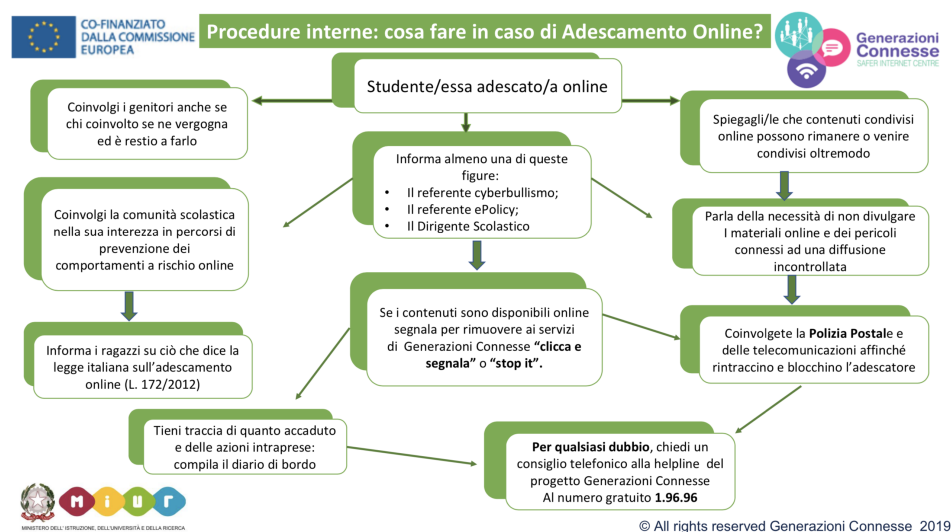
### Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



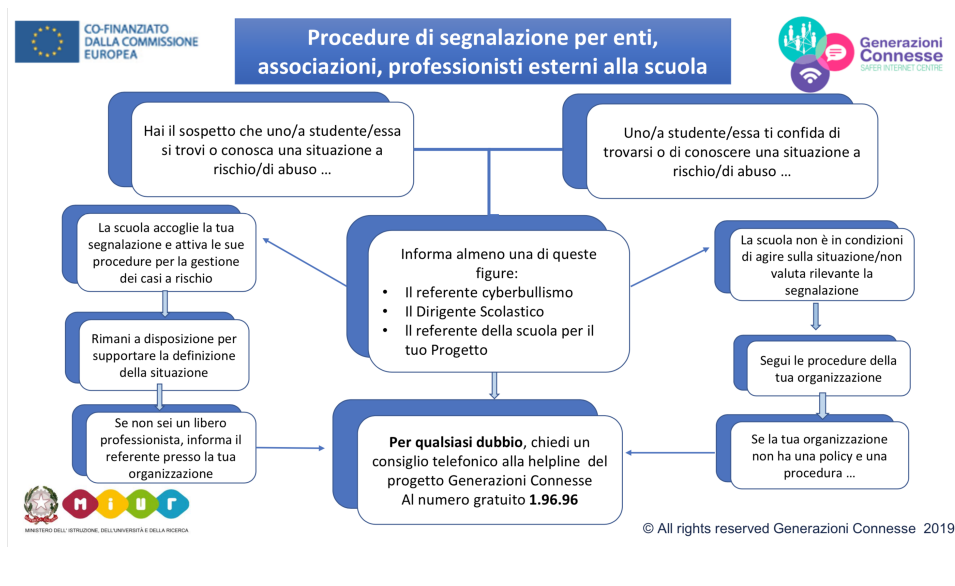
### Procedure interne: cosa fare in caso di sexting?



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



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



## Altri allegati

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

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

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

- Predisporre un indirizzo mail e una scatola/box in ciascun plesso per la raccolta di segnalazioni da inserire in uno spazio accessibile e ben visibile della scuola;
- Affiggere in ciascuna aula Docenti di ciascun plesso le procedure interne per le segnalazioni di cui al punto successivo.

