



# Documento di ePolicy

BAEE15700E

1 C.D. "G . BOVIO"

LARGO DI VAGNO 13 - 70037 - RUVO DI PUGLIA - BARLETTA-ANDRIA-TRANI (BA)

Giuseppe Quatela

# 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.

Il presente documento integra il Regolamento d'Istituto per quanto sopra specificato.

---

## 1.2 - Ruoli e responsabilità

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

Il **Dirigente Scolastico** garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica.

Il Dirigente Scolastico ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

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

Il **Referente bullismo e cyberbullismo** ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Il suo ruolo si svolge non solo in ambito scolastico ma anche in quello extrascolastico, in quanto (ove possibile) può coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori per un approfondimento maggiore sui ruoli relativi alle problematiche del bullismo e del cyber bullismo.

I **Docenti** hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Possono, innanzitutto, integrare parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo anche l'uso delle tecnologie digitali nella didattica. I docenti accompagnano e supportano gli alunni e le alunne nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete; hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti bambini e bambine.

Il **personale ATA**, all'interno dei singoli regolamenti d'Istituto, è coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure; raccoglie, verifica e valuta le informazioni inerenti possibili casi di bullismo/cyberbullismo.

Gli **Alunni e le Alunne**, in relazione al proprio grado di maturità e consapevolezza raggiunta, devono utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola devono imparare a tutelarsi online, tutelare i/le propri/e compagni/e e

rispettarli/le; devono partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete.

I **Genitori**, in continuità con l'Istituto scolastico, devono essere partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali.

Gli **Enti educativi esterni e le associazioni** che entrano in relazione con la scuola devono conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC; devono, inoltre, promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli alunni e delle alunne durante le attività che si svolgono insieme.

---

## ***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).

La scuola nel presente documento prevede un insieme di regole o norme di comportamento da condividere con le organizzazioni/associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve e/o lungo periodo.

L'Istituto si propone di dotarsi di un'informativa sintetica sull'ePolicy comprensiva delle procedure di segnalazione da condividere con tutte le figure che operano con alunni e alunne,

Tale documento dovrà chiarire il sistema di azioni e le procedure di segnalazione da seguire valide anche per i professionisti e le organizzazioni esterne, finalizzate a rilevare e gestire le problematiche

connesse ad un uso non consapevole delle tecnologie digitali.

Tale documento, inoltre, permette di tutelare ragazzi e ragazze da comportamenti potenzialmente rischiosi messi in atto da soggetti esterni alla scuola e che si trovano ad operare all'interno dell'Istituto.

L'informativa deve essere condivisa e sottoscritta nella stipula di eventuali contratti con personale e associazioni esterne: le figure professionali e le organizzazioni coinvolte in progetti, laboratori e attività devono prendere visione di tutti i documenti proposti dall'Istituto e sottoscriverli preliminarmente all'avvio dei programmi con gli alunni e le alunne, in classe o fuori.

L'Istituto può anche richiedere agli attori esterni, eventualmente, il casellario giudiziale come fattore ulteriormente protettivo verso i minori.

L'utilizzo dei dispositivi in dotazione della scuola ed, eventualmente, quelli personali (smartphone, tablet, pc, etc.), deve essere finalizzato allo svolgimento di attività didattiche, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli alunni e le alunne. E' obbligatorio rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

---

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

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

L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

Il documento di ePolicy viene condiviso con tutta la comunità educante, attraverso la pubblicazione

sul sito istituzionale della scuola. La scuola, inoltre, mette in atto delle azioni per la condivisione e comunicazione dell'ePolicy ai diversi membri della comunità scolastica.

1. Alunni e alunne: condivide e comunica il documento nell'ambito di percorsi didattici per un uso consapevole e maturo dei dispositivi e della tecnologia informatica; dà loro regole condivise di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici; fornisce loro elementi per poter riconoscere e quindi prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e.

2. Personale scolastico: condivide e comunica il documento attraverso riunioni informative estese a tutta la comunità scolastica, in modo da poter orientare tutte le figure sui temi in oggetto, a partire da un uso corretto dei dispositivi e della Rete in linea anche con il codice di comportamento dei pubblici dipendenti;

3. Genitori: condivide e comunica il documento tramite un incontro di formazione specifico

E' fondamentale che ciascun attore scolastico (dai docenti agli/lle alunni/e), una volta informato, si faccia a sua volta promotore del documento.

---

## ***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.

La scuola prevede possibili condotte sanzionabili, in relazione all'uso improprio delle TIC e della Rete a scuola da parte degli alunni e delle alunne:

- la condivisione online di immagini o video di compagni/e senza il loro consenso o che li ritraggono in pose offensive e denigratorie;
- la condivisione online di immagini o video del personale scolastico senza il loro consenso o che li ritraggono in pose offensive e denigratorie;
- la condivisione online di messaggi scritti o audio di compagni/e senza il loro consenso, a scopo offensivo e/o di esclusione;
- la condivisione di dati personali; l'invio di immagini o video volti all'esclusione di compagni/e.
- collegamento a siti web non attinenti l'attività didattica in corso

Il personale scolastico è tenuto ad un utilizzo corretto dei device e della Rete, onde evitare di commettere infrazioni, nonché a vigilare sugli alunni e a valutare la natura e la gravità di eventuali episodi di scorrettezza, al fine di considerare la necessità di denunciare l'accaduto (con il coinvolgimento ad es. della Polizia Postale)

---

## ***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.

Il documento di E-policy, infatti, è parte integrante del Regolamento d'Istituto.

---

## ***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 documento andrà revisionato periodicamente, ogni qualvolta ci saranno situazioni o normative nuove e in seguito ad eventuali criticità emerse dal monitoraggio di fine anno scolastico per la comunità scolastica.

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

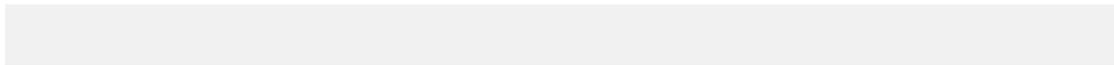
---

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

- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti

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

- Organizzare uno o più eventi o attività volti a presentare ai rappresentanti dei genitori dell'Istituto il documento finale dell'ePolicy.
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti delle classi quinte.
- 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.

La progettazione del curriculum digitale è continuativa e trasversale alle varie discipline e, naturalmente, il curriculum è progettato ad hoc rispetto al target di riferimento. Le competenze digitali richiamano diverse dimensioni:

1. dimensione tecnologica
2. dimensione cognitiva
3. dimensione etica e sociale

I documenti più importanti presi a riferimento per progettare e implementare un buon curriculum sulle competenze digitali sono:

Piano Scuola Digitale (PNSD), [Sillabo sull'Educazione Civica Digitale](#); DigComp 2.1; Raccomandazione del Consiglio europeo relativa alle competenze chiave per l'apprendimento permanente (C189/9, p. 9).

Le aree di competenza individuate, come dal Digcomp, sono:

Area 1: "Alfabetizzazione e dati"

Area 2: "Comunicazione e collaborazione"

Area 3: "Creazione di contenuti digitali"

Area 4: "Sicurezza"

Nel curriculum si tengono presente i descrittori e i livelli di padronanza, nonché alcune modalità valutative, come suggerito nel documento suddetto.

---

## ***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.

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

Fondamentale, infatti, che vi sia attenzione all'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 studenti e studentesse rispetto alla fruizione dei contenuti online, ormai la modalità naturale di apprendimento al di fuori della scuola.

Gli insegnanti, dunque, devono essere pronti a cogliere tale sfida, anche grazie alla possibilità di formazione permanente offerta loro in primis dall'Istituto scolastico, in modo da rispondere ai diversi bisogni formativi della classe.

---

## ***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.

Nell'ottica di creare ulteriore sinergia fra scuola, studenti/studentesse e famiglie, di promuovere la condivisione di buone pratiche nell'utilizzo consapevole delle TIC e di prevenire e contrastare ogni forma di discriminazione, offesa, denigrazione e lesione della dignità dell'altro, nonché fenomeni di bullismo e cyberbullismo, i docenti tutti dell'Istituto scolastico seguiranno un percorso formativo specifico ed adeguato che abbia ad oggetto non solo l'uso responsabile e sicuro della Rete ma anche i rischi legati a quest'ultime.

Per tali ragioni, l'Istituto prevede specifici momenti di formazione permanente per gli insegnanti che mettano al centro i temi in oggetto, considerando anche percorsi di autoaggiornamento personali o collettivi, iniziative seminariali con professionisti/esperti interni (l'Animatore digitale) ed esterni alla scuola, giornate/settimane di approfondimento in accordo con la rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), le amministrazioni comunali, i servizi socio-educativi e le associazioni/enti presenti. Tali azioni programmatiche sono inserite nel Piano triennale dell'offerta formativa.

I momenti di formazione e aggiornamento saranno pensati e creati a partire dall'analisi del fabbisogno comune formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.

Si penserà ad un cronoprogramma che consideri il triennio scolastico, in un'ottica di vera e propria programmazione, con azioni specifiche. Per esempio:

- Analizzare il fabbisogno formativo degli insegnanti sull'uso sicuro della Rete;
- Promuovere la partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse";
- Monitorare le azioni svolte per mezzo di specifici momenti di valutazione;
- Organizzare incontri con professionisti della scuola o con esperti esterni, enti/associazioni, etc.

---

## ***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.

La scuola ritiene di fondamentale importanza il coinvolgimento delle famiglie nell'educazione digitale degli studenti e delle studentesse, con percorsi da mettere in pratica insieme per sensibilizzare i genitori sulle tematiche relative alle TIC.

Un primo passo in tal senso è stato quello di aggiornare o integrare, oltre che il regolamento scolastico, anche il "Patto di corresponsabilità", con specifici riferimenti alle tecnologie digitali e all'ePolicy.

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

A tale proposito è importante informare i genitori sulle condotte che si dovranno adottare a scuola e, in generale, offrire loro consigli da mettere in pratica con i propri figli.

Una particolare attenzione sarà dedicata a consigli, indicazioni e informazioni su iniziative e azioni della scuola, in riferimento ai rischi connessi ad un uso distorto della Rete da parte degli studenti e delle studentesse.

Ciò in continuità anche con l'art. 5 (comma 2) della legge 29 maggio 2017, n.71 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" che prevede l'integrazione, oltre che del regolamento scolastico, anche del "Patto di Corresponsabilità", con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti, al fine di meglio regolamentare l'insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione al fenomeno.

---

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

---

## **AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021)**

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

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

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

# 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.

## **CONSENSO/LIBERATORIA AL TRATTAMENTO DEI DATI PERSONALI S.2020/21**

I sottoscritti genitori / tutori legali esercenti la potestà genitoriale

(madre) ( cognome e nome in stampatello) \_\_\_\_\_

(padre) ( cognome e nome in stampatello ) \_\_\_\_\_

dell'alunno/a

frequentante la classe\_                      sez.\_                      del plesso

### **RIPRESE FOTOGRAFICHE E VIDEO**

1. Esprimono il proprio consenso per riprese e registrazioni video, audio e fotografiche del/la proprio/a figlio/a effettuato nell'ambito delle attività scolastiche in luoghi interni alla scuola o esterni, anche in occasione di viaggi, visite d'istruzione e partecipazione ad eventi connessi all'attività didattica, da solo/a, o con i compagni, con insegnanti e operatori scolastici ed extrascolastici, per ogni esperienza collegata al P.T.O.F. d'Istituto, ai fini di:

formazione, ricerca e documentazione dell'attività didattica e delle esperienze di apprendimento (opuscoli, altre produzioni cartacee, cartelloni e pannelli espositivi all'interno della scuola e anche in luoghi esterni, in occasione di Open-Day, esposizioni, seminari, convegni, mostre, concorsi, ecc.);

partecipazione a iniziative di sensibilizzazione alle problematiche sociali e di cittadinanza presso la sede scolastica o sedi esterne o anche tramite invio della documentazione via Internet sui siti collegati alle iniziative;

divulgazione di attività ed esperienze didattiche effettuate in ambienti scolastici ed extrascolastici, mediante prodotti realizzati con modalità cartacee o tramite strumenti tecnologici, attraverso

- pubblicazione di articoli a mezzo stampa su giornalini scolastici o su giornali locali o su testate giornalistiche del territorio

- pubblicazione di articoli a mezzo stampa o di riprese fotografiche e video ( con voci, commenti, comunicazioni, ecc.) su Internet ( sito web scolastico, siti web locali, siti web o piattaforme digitali appartenenti ad Enti o Soggetti o Associazioni con cui la Scuola collabora nelle attività didattiche )

- trasmissione di produzioni ed elaborati degli alunni ( cartacei o DVD, o elaborati digitali, ecc. ) presso sedi esterne in occasione di partecipazione a concorsi o manifestazioni o iniziative connesse alle attività didattiche e progettuali.

Apporre una x sulla voce scelta

- |               |               |
|---------------|---------------|
| Madre         | Padre         |
| • Consenso    | • Consenso    |
| • NonConsenso | • NonConsenso |

Il consenso al conferimento dei dati suindicati è facoltativo. Il mancato conferimento comporta l'esclusione dalle riprese video o dalle riprese fotografiche.

USO DI PIATTAFORME TELEMATICHE PER FINI DIDATTICI

- Esprimono il proprio consenso per l'iscrizione del/la proprio/a figlio/a su piattaforme telematiche da utilizzare, in orario scolastico ed extrascolastico, per partecipazione ad attività ed esperienze connesse all'attività didattica, per ogni iniziativa formativa collegata al P.T.O.F. d'Istituto

Apporre una x sulla voce scelta

- |               |               |
|---------------|---------------|
| Madre         | Padre         |
| • Consenso    | • Consenso    |
| • NonConsenso | • NonConsenso |

.....

Il presente consenso/liberatoria/autorizzazione al trattamento dei dati (a titolo gratuito, anche ai sensi degli artt. 96 e 97 legge 22.4.1941, n. 633, Legge sul diritto d'autore), vale per tutti gli anni di frequenza delle scuole appartenenti a questo Istituto e potrà essere revocata in ogni momento con comunicazione scritta da inviare tramite e-mail a questo Istituto.

.....

Il/I sottoscritto/I dichiara/no di non aver nulla a pretendere in ragione di quanto sopra indicato e di rinunciare irrevocabilmente ad ogni diritto, azione o pretesa derivante da quanto sopra autorizzato.

Annotazioni ( in caso di firma di un solo genitore ).....

Data \_\_\_\_\_ Firma Madre ( o Tutore legale ) \_\_\_\_\_

Data \_\_\_\_\_ Firma Padre ( o Tutore legale ) \_\_\_\_\_

---

## 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.

E' importante conoscere il più possibile l'infrastruttura tecnologica dell'Istituto, in modo da poterla sfruttare e potenziare in modo coerente con le necessità dei docenti e la visione che la scuola ha rispetto all'uso delle ICT.

Tale adeguamento è necessario anche in ottica di un potenziamento degli strumenti didattici e laboratoriali necessari a migliorare la formazione e i processi di innovazione delle istituzioni scolastiche e all'adozione di strumenti organizzativi e tecnologici che permettano un'amministrazione trasparente, la condivisione di dati e la dematerializzazione degli atti, oltre al

fondamentale scambio di informazioni tra dirigenti, docenti, famiglie e studenti/esse, permesso, ad esempio, dal registro elettronico.

La scuola deve dunque considerare l'ambiente online alla stregua dell'ambiente fisico e valutarne tutti gli aspetti legati alla sicurezza nel momento in cui permette a studenti/esse e docenti l'accesso alla rete tramite i dispositivi della scuola, tramite la rete scolastica o tramite i dispositivi personali nel caso del BYOD (Bring your own device).

E' necessario dotarsi di un regolamento d'Istituto sull'uso delle TIC.

Il regolamento, dunque, deve prevedere una parte dedicata all'uso di Internet in cui gli studenti si impegnano a:

- utilizzare la rete nel modo corretto
- rispettare le consegne dei docenti
- non scaricare materiali e software senza autorizzazione
- non utilizzare unità removibili personali senza autorizzazione
- tenere spento lo smartphone al di fuori delle attività didattiche che ne prevedano l'utilizzo
- segnalare immediatamente materiali inadeguati ai propri insegnanti.

I docenti si impegnano a:

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

La scuola dovrebbe informare che si farà carico di tutte le precauzioni necessarie per garantire agli/le studenti/esse l'accesso a materiale appropriato, ma che allo stesso tempo non può essere responsabile per l'accesso autonomo da parte degli/le studenti/esse a materiali inadeguati e potenzialmente dannosi trovati online.

Oggi è anche fondamentale dotare gli/le studenti/esse delle competenze necessarie ad affrontare la complessità del mondo dell'informazione, che ormai richiede di essere in grado di destreggiarsi tra notizie e fake news, discussioni online e discorsi d'odio (hate speech). Anche il personale scolastico avrà una copia del regolamento e dovrà sottoscriverla, consapevole che l'uso di Internet verrà monitorato e segnalato, e tutto il personale scolastico sarà coinvolto nello sviluppo delle linee guida del regolamento stesso. Saranno, inoltre, responsabili dell'applicazione delle istruzioni sull'uso sicuro di Internet.

Se l'accesso a Internet è un diritto, esso deve anche essere adeguato all'età degli utenti.

Per questo la scuola deve prendere tutte le necessarie precauzioni per evitare l'accesso online da parte di studenti e studentesse, a materiali non adatti a loro all'interno della scuola.

L'obiettivo principale resta quello di arricchire ed ampliare le attività didattiche, secondo quanto prevede il curriculum scolastico, l'età e la maturità degli/le studenti/esse.

### Checklist per la cybersecurity

- Mantenere separate le reti didattica e segreteria: importante per garantire maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le due reti grazie al firewall.
  - Aggiornare periodicamente software e Sistema operativo: garantire che il sistema sia aggiornato lo protegge dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo.
  - Definire la programmazione di backup periodici: cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi (possibilmente anche una copia offline).
  - Garantire formazione adeguata allo staff, incluso il corpo docenti: la formazione deve riguardare la gestione dei dispositivi, la conoscenza delle regole basilari sulla sicurezza.
  - Testare regolarmente le possibili vulnerabilità.
  - Preparare piani di azione in risposta ai problemi più seri: è importante non dover improvvisare nel momento in cui si verifica un problema serio, ma avere un protocollo di azione.
  - Predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo: se non è previsto uno stand-by, il dispositivo resta accessibile nel caso in cui qualcuno dimentichi di spegnerlo, con il rischio potenziale di accesso da parte di persone non autorizzate.
  - Impostare il browser per l'eliminazione dei cookies alla chiusura: in questo modo si evita che qualcuno possa avere accesso ad account altrui senza autorizzazione.
  - Definire una policy sulle password: le password devono essere forti:
    1. Richiedere password complesse con almeno 8 caratteri con numeri, maiuscole e minuscole e caratteri speciali.
    2. Sensibilizzare rispetto al non uso di password facilmente identificabili (nomi dei figli, compleanni, etc.).
    3. Non memorizzare le password nei dispositivi scolastici.
    4. Non condividere le password con nessuno.
  - Minimizzare i privilegi amministrativi: solo poche persone autorizzate dovrebbero avere privilegi amministrativi. Studenti e la maggior parte dei docenti possono accedere con account con permessi limitati.
  - Sviluppare il regolamento sull'uso delle tecnologie a scuola (policy di uso accettabile): deve riguardare chiunque abbia accesso alla Rete, studenti/esse, docenti, amministrazione e segreteria, includere i dispositivi della scuola e quelli personali, anche in caso di BYOD.
- 

## ***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.

Quando ci relazioniamo attraverso l'uso di strumenti di comunicazione online, mettiamo in atto una modalità comunicativa che ha caratteristiche e logiche proprie.

La comunicazione che viaggia online, generalmente, si avvale di messaggi scritti che possono essere memorizzati, diffusi e permangono nel tempo.

D'altro canto, grazie agli strumenti di comunicazione online, come già in parte sottolineato, possiamo usufruire dell'interattività del mezzo, superare le barriere spazio-temporali, usare un linguaggio multimediale, ipertestuale e accattivante, promuovere la partecipazione e il coinvolgimento dei diversi attori in gioco nel processo educativo (dai ragazzi ai genitori).

Diversi strumenti di comunicazione online possono essere utilizzati dalla scuola, sia per raggiungere target esterni sia per far circolare all'interno della scuola informazioni di servizio o contenuti importanti fra i diversi attori scolastici (docenti, studenti, genitori, collaboratori scolastici etc.).

Fra gli strumenti di comunicazione esterna del nostro Istituto troviamo in primis il sito web della scuola, che può essere utilizzato anche per fornire informazioni di servizio rivolte a studenti o genitori.

Fra gli strumenti di comunicazione interna, invece, troviamo il registro elettronico (Argo) con tutte le sue funzionalità, la classica e-mail, gli strumenti di messaggistica istantanea, che però hanno sempre più funzionalità tipiche anche dei social network, whatsapp, [classroom](#), che possono essere ampiamente utilizzati anche per facilitare e rendere più partecipata la didattica e la comunicazione a scuola.

Per quanto riguarda le chat informali fra colleghi, o fra docenti e genitori, non esiste una vera e propria regolamentazione, e per tale ragione è fondamentale, a partire dal buon senso e da una riflessione sulle peculiarità del mezzo, che si elaborino regole condivise sull'uso delle stesse.

Fra queste, ad esempio:

- Mettere in chiaro fin dall'inizio, comprendere e rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità;
- Usare sempre un linguaggio adeguato e il più possibile chiaro e preciso (come già sottolineato la comunicazione online si presta spesso a non pochi fraintendimenti);
- Evitare di affrontare in chat argomenti troppo complessi e controversi (la comunicazione online in una chat di gruppo non è adatta per la gestione di problematiche di questo tipo, che certamente è più opportuno affrontare in presenza o in un Consiglio di classe);
- Evitare discussioni di questioni che coinvolgono due o pochi interlocutori, onde evitare di annoiare e disturbare gli altri componenti del gruppo;
- Non condividere file multimediali troppo pesanti;

- Evitare il più possibile di condividere foto di studenti in chat;
- Indirizzare solo domande precise e chiare, a cui si possano dare risposte altrettanto brevi e precise;
- Evitare messaggi troppo spezzettati, cercando il più possibile di essere brevi ed esauritivi allo stesso tempo.

Altro strumento ormai centrale a disposizione delle scuole per la gestione di assenze, presenze, valutazioni, prenotazioni di incontri e comunicazioni con le famiglie è il registro elettronico.

---

## ***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.

Nel nostro Istituto gli alunni non dispongono e non sono autorizzati ad utilizzare i propri dispositivi personali per la didattica.

---

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

#### **AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021).**

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- 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).**

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare 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.

Gli **interventi o campagne di sensibilizzazione** devono essere mirati a piccoli gruppi, con l'obiettivo di coinvolgere un gruppo ristretto di persone affinché agiscano insieme in favore di una causa in cui credono.

Per far sì che un intervento di sensibilizzazione sia efficace, è importante fornire ai beneficiari informazioni chiare su quali sono le caratteristiche del fenomeno e i dati rappresentativi.

In questo modo gli utenti avranno tutte le informazioni necessarie per avere una fotografia chiara del contenuto che stiamo trattando e del perché è necessario impegnarsi verso un cambiamento (motivazione al cambiamento).

Un'attività di sensibilizzazione dovrebbe quindi fornire non solo le informazioni necessarie, ma anche illustrare le possibili soluzioni o comportamenti da adottare.

Per la **prevenzione** in ambito digitale si deve prevedere 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.

Come sappiamo, le dimensioni che il fenomeno coinvolge sono molteplici e non puramente tecniche e si rifanno alla capacità dei più giovani di gestire situazioni complesse che richiedono: la capacità di gestire la relazione con l'altro/a diverso/a da sé, le dimensioni dell'affettività e della sessualità, il riconoscimento di un limite, anche, ma non solo, legato ad una dimensione di legalità, l'utilizzo sicuro e consapevole delle tecnologie digitali.

Per questo motivo la scuola risponde anche a questi bisogni attraverso strumenti e misure specifiche. Allo stesso modo, quando un evento problematico connesso ai rischi online coinvolge il contesto scolastico, la scuola deve dare una risposta il più possibile integrata, che trovi la sua espressione di indirizzo in procedure chiare esplicitate in appositi regolamenti e che includano la collaborazione (prevedendo accordi specifici) con la rete dei servizi locali (in primis le ASL e la Polizia Postale).

Inoltre, la responsabilità dell'azione preventiva ed educativa chiama in campo diverse agenzie educative oltre alla scuola, come la famiglia, ma non solo (istituzioni, associazioni, società civile, etc.), ciascuna con un proprio compito nei confronti di bambini e bambine e di adolescenti. Tali agenzie sono chiamate a collaborare ad un progetto comune, nell'ambito di funzioni educative condivise. La necessità di questa collaborazione nasce, più o meno consapevolmente, dal riconoscimento sia da parte dei genitori che da parte degli insegnanti della rispettiva difficoltà a svolgere da soli la propria funzione formativa ed educativa. E questo, anche a causa della sproporzione tra le competenze sempre crescenti che le tecnologie digitali richiedono loro e quelle che si avvertono di possedere. La necessità di supportare un uso positivo e consapevole delle TIC da parte dei più giovani, sia in un'ottica di tutela dai rischi potenziali che nella valorizzazione delle opportunità esistenti, pone la scuola e i genitori di fronte alla sfida di riconsiderare la propria identità, il proprio ruolo educativo e le proprie risorse, oltre allo stato dei rapporti reciproci per un patto educativo da rinnovare costantemente.

---

## ***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).

È molto importante sottolineare come il cyberbullismo non sia una problematica che riguarda unicamente vittima e cyberbullo. È un fenomeno sociale e di gruppo. Infatti, centrale è il ruolo delle agenzie educative e di socializzazione (formali e informali) più importanti per gli adolescenti: la famiglia, la scuola, i media, le tecnologie digitali e il gruppo dei pari.

Nella consapevolezza che le azioni efficaci siano quelle che ricorrono agli strumenti educativi, rieducativi e di mediazione del conflitto, esistono tuttavia responsabilità da conoscere, la possibilità di commettere reati o danni civili e specifici dispositivi giuridici.

Nei casi più gravi, basta la denuncia ad un organo di polizia o all’autorità giudiziaria per attivare un procedimento penale (per es. lesioni gravi, minaccia grave, molestie); negli altri casi, la denuncia deve contenere la richiesta che si proceda penalmente contro l’autore di reato (querela).

Le responsabilità per atti di bullismo e cyberbullismo compiute dal minorenne possono ricadere anche su:

- i genitori, perché devono educare adeguatamente e vigilare, in maniera adeguata all’età del figlio, cercando di correggerne comportamenti devianti. Questa responsabilità generale persiste anche per gli atti compiuti nei tempi di affidamento alla scuola (culpa in educando).
- gli insegnanti e la scuola: perché nei periodi in cui il minore viene affidato all’Istituzione

scolastica il docente è responsabile della vigilanza sulle sue azioni e ha il dovere di impedire comportamenti dannosi verso gli altri/e ragazzi/e, insegnanti e personale scolastico o verso le strutture della scuola stessa.

Esiste poi una culpa in organizzando, che si ha quando la scuola non mette in atto le azioni previste per la prevenzione del fenomeno o per affrontarlo.

Le modalità d'intervento previste dall'Istituto, in ottemperanza a quanto previsto dalla normativa vigente, riguardano:

- 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);
- 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;
- nomina del Referente per le iniziative di prevenzione e contrasto.

Le strutture a cui rivolgersi sono:

- i servizi socio-sanitari del territorio di appartenenza
- Helpline di Telefono Azzurro per Generazioni Connesse

---

## ***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.

- Adesione al Progetto "SCUOLA AMICA"
- Elaborazione di un Progetto di Inclusione per gli alunni con Bisogni Educativi Speciali (BES)

---

## ***4.4 - Dipendenza da Internet e gioco online***

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

*L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale?*

La dipendenza da Internet, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica che deve attenzionare il fenomeno e fornire gli strumenti agli studenti e alle studentesse affinché questi siano consapevoli dei rischi che comporta l'iperconnessione. Spesso il trascorrere del tempo online, in termini disfunzionali, è scandito dal gioco virtuale che può anche assumere forme di Dipendenza dal gioco online (Net gaming addiction o Internet Gaming Addiction) inserito all'interno del Manuale Diagnostico Statistico dei Disturbi Mentali (DSM 5).

La dipendenza si realizza quando c'è un abuso, ossia un utilizzo continuativo e sistematico della Rete al fine di giocare impegnando la maggior parte delle giornate, con la conseguente sottrazione del tempo alle altre attività quotidiane del minore.

Anche in questo caso, la scuola ha la possibilità di fare formazione e di indicare strategie per un uso più consapevole delle tecnologie per favorire il "benessere digitale", cioè la capacità di creare e mantenere una relazione sana con la tecnologia.

Questo è un argomento trasversale, se ne può parlare quando si parla di cittadinanza digitale, di cyberbullismo, di uso integrativo e non sostitutivo dei dispositivi e della Rete; tanto più può essere utile dedicare al tema un momento specifico e riflettere con alunni e alunne, per fare in modo che la tecnologia sia strumento per raggiungere i propri obiettivi e non sia solo distrazione o addirittura ostacolo.

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

Diventa utile riflettere con i ragazzi e le ragazze rispetto all'uso della tecnologia in termini di qualità e tempo.

Se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi.

Strutturare regole condivise e stipulare con loro una sorta di "patto" d'aula e, infine, proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali

È importante, quindi, non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli/le studenti e delle studentesse, stabilendo chiare e semplici regole di utilizzo.

Il nostro Istituto mette in atto una serie di azioni e progetti per gli alunni della scuola dell'infanzia e della scuola primaria, al fine di guidarli ad un uso corretto della tecnologia:

- Partecipazione alla Code Week
- Partecipazione al Safer Internet Day
- Predisposizione del curriculum di Cittadinanza Digitale

---

## **4.5 - Sexting**

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti mediati 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.

E' fondamentale far capire ai ragazzi come un banale "scherzo" si possa diffondere a macchia d'olio in rete e quanto sia facile sottovalutare le reali conseguenze di tale diffusione, spesso molto dannose per le vittime dello scherzo.

I contenuti sessualmente espliciti, per esempio, possono diventare materiale di ricatto.

E' necessario far maturare nei ragazzi la consapevolezza, o comunque la sola idea, che la diffusione di contenuti personali si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla.

---

## **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.

Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e perché no, della sessualità.

Con un'adeguata competenza digitale ed emotiva, Internet potrebbe essere un valido supporto per i/le ragazzi/e nel loro percorso di esplorazione della sessualità.

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.

## 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.**

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).

Parallelamente, se si ravvisa un rischio per il benessere psicofisico dei/lle bambini/e, ragazzi/e

coinvolte nella visione di questi contenuti sarà opportuno ricorrere a un supporto psicologico anche passando per una consultazione presso il medico di base o pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza: Consultori Familiari, Servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, etc.

Se si è a conoscenza di tale tipologia di reato è possibile far riferimento alla: Polizia di Stato - Compartimento di Polizia postale e delle Comunicazioni; Polizia di Stato - Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri - Comando Provinciale o Stazione del territorio di competenza;

Fondamentale è la prevenzione: i più giovani devono acquisire quelle competenze in grado di orientarli e guidarli nelle loro scelte anche online; per questo motivo, come già sottolineato, l'educazione, compresa l'educazione all'affettività, riveste un ruolo fondamentale.

In un'ottica di attività preventiva, 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. Risulta utilissima l'attività educativa sull'affettività e le relazioni, sottolineando sempre la necessità di rivolgersi ad un adulto quando qualcosa online mette a disagio.

Data l'età degli alunni dell'Istituto, è preferibile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico, promuovendo i servizi delle hotline.

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

---

### **AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021).**

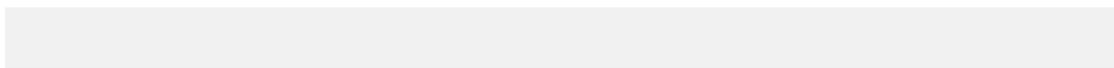
Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

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

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

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

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/le studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online:** se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting:** nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di [Helpline 19696](#) e [Chat di Telefono Azzurro](#) per supporto ed emergenze;
- [Clicca e segnala di Telefono Azzurro](#) e [STOP-IT di Save the Children Italia](#) per segnalare la presenza di materiale pedopornografico online.

Le procedure previste dall'Istituto sono esplicitate nel Regolamento d'Istituto per la prevenzione e il contrasto del bullismo e del cyberbullismo, che è parte integrante del Regolamento d'Istituto, del Regolamento alunni e del Patto di Corresponsabilità.

---

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

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

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

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

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

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

---

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

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

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

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

Nel CASO A, si deve coinvolgere innanzitutto il referente d'Istituto per il contrasto del bullismo e del

cyberbullismo, valutando insieme le possibili strategie d'intervento. Si avvisa l'intero consiglio di classe e, se si ravvisa la necessità e l'urgenza, si coinvolge il Dirigente Scolastico (considerando il regolamento interno o le prassi già consolidate).

Nel frattempo, il docente (e i docenti informati) ascolta gli alunni e le alunne.

Inoltre, il docente deve cercare di capire se gli episodi sono circoscritti al gruppo o se interessano l'intero Istituto.

Nel CASO B, il docente deve condividere immediatamente quanto osservato con il referente per il bullismo e il cyberbullismo, valutando insieme le possibili strategie di intervento. Si avvisa anche il Dirigente Scolastico che convoca il consiglio di classe. Se non si ravvisano fattispecie di reato, si deve:

- informare i genitori degli/delle studenti/studentesse direttamente coinvolti/e
- richiedere, in concomitanza, la consulenza dello psicologo scolastico
- informare i genitori degli/delle studenti/studentesse infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o
- attivare il consiglio di classe;
- valutare come coinvolgere gli operatori scolastici su quello che sta accadendo.

A seconda della situazione e delle valutazioni effettuate con referente, dirigente e genitori, si può poi segnalare alla Polizia Postale: a) contenuto del materiale online offensivo; b) modalità di diffusione; c) fattispecie di reato eventuale.

È bene sempre dialogare con la classe, attraverso interventi educativi specifici, cercando di sensibilizzare studenti e studentesse sulla necessità di non diffondere ulteriormente online i materiali dannosi, ma anzi di segnalarli e bloccarli.

---

### ***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.

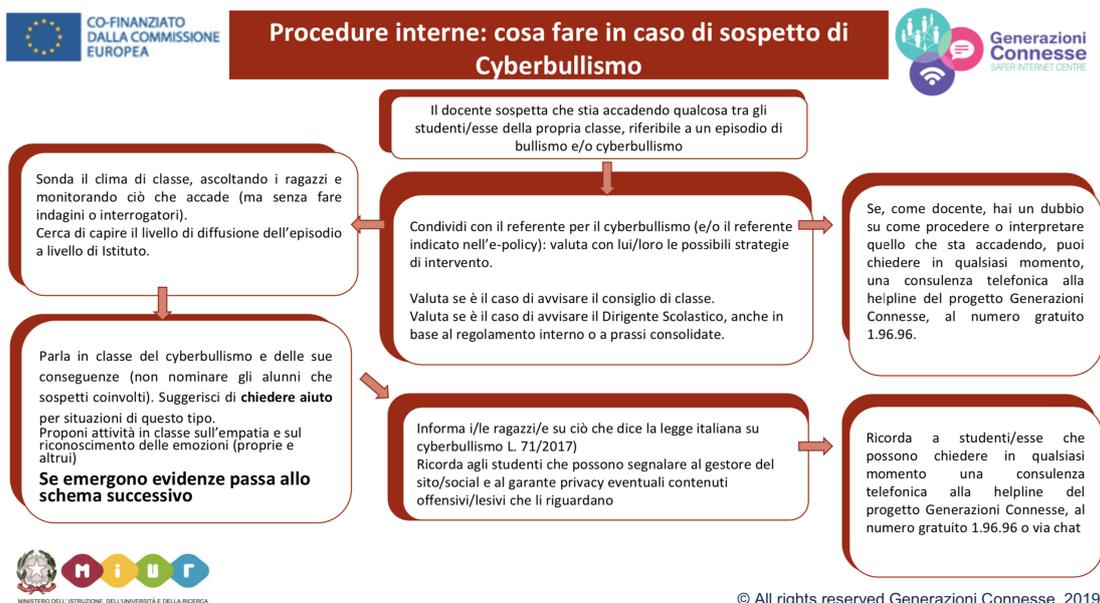
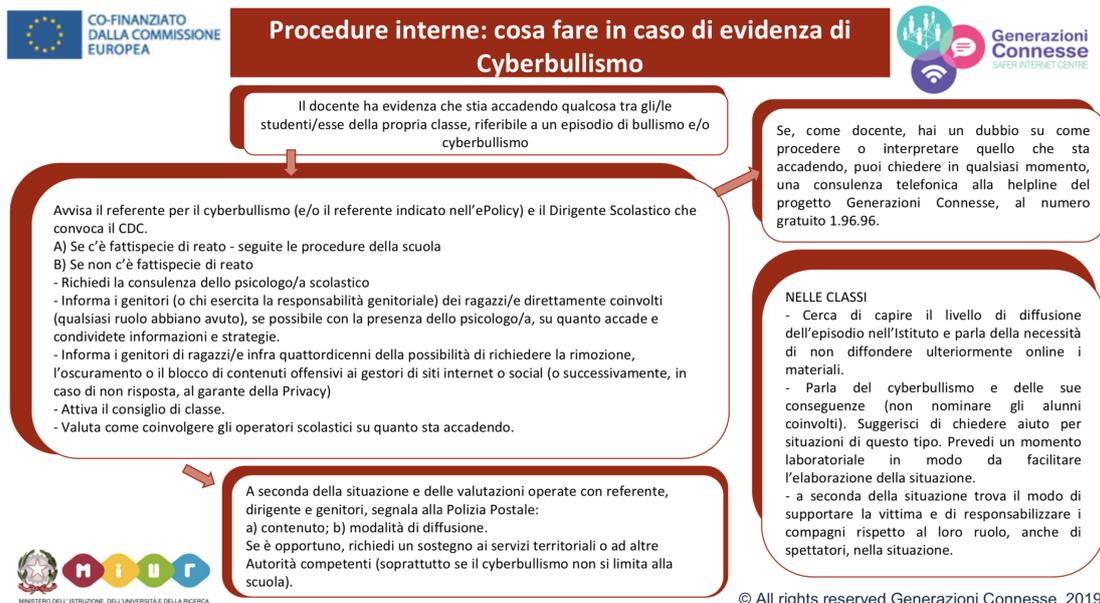
Per una mappatura degli indirizzi di tali strutture è possibile consultare il [Vademecum](#) di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza 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.

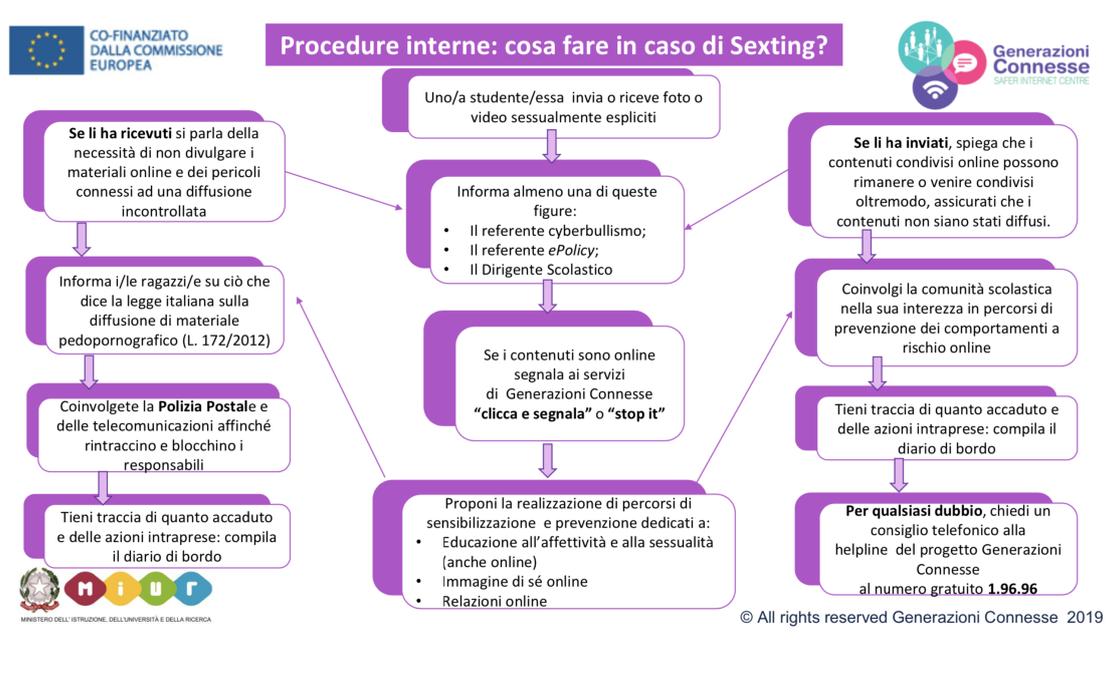
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

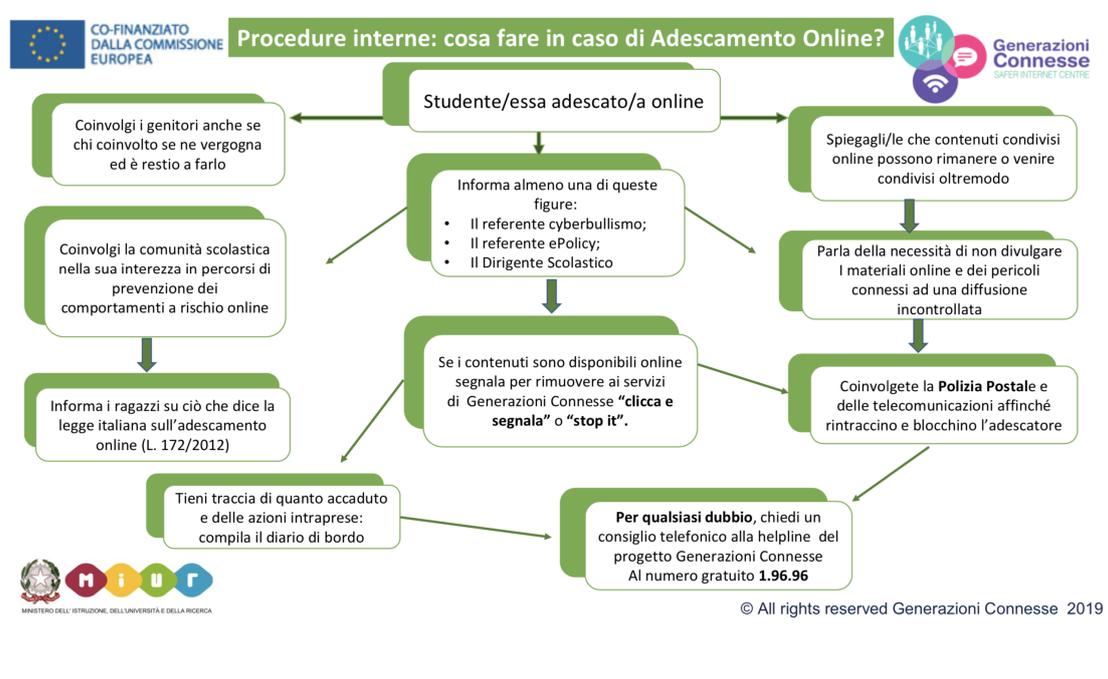
### **Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?**



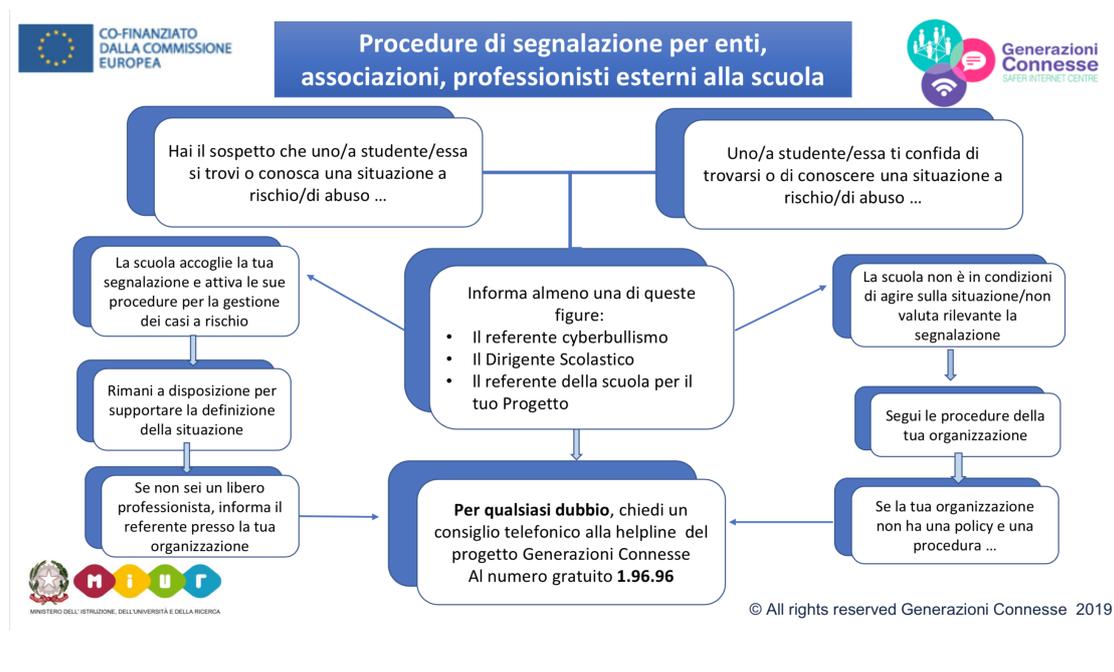
## Procedure interne: cosa fare in caso di sexting?



## 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](#)

Per quanto riguarda le procedure da seguire in caso di sospetto di Cyberbullismo, si fa riferimento al Protocollo per la gestione delle emergenze previsto al capitolo "Comportamenti illeciti e sanzioni" del Regolamento d'Istituto per la prevenzione e il contrasto del bullismo e del cyberbullismo.

## *Il nostro piano d'azioni*

**Non è prevista nessuna azione.**

