



# Documento di ePolicy

BRIC825006

PRIMO I.C. ORIA

VIA RENATO LOMBARDI 7 - 72024 - ORIA - BRINDISI (BR)

Prof.ssa Camero Francisca

# 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.

Attraverso l'E-policy la nostra scuola potrà attuare le "Linee guida per l'uso positivo delle tecnologie digitali e la prevenzione dei rischi nelle scuole" redatte dal Ministero dell'Istruzione, dell'Università e della Ricerca per promuovere le politiche del cosiddetto "Better Internet for Kids" attraverso le iniziative nell'ambito del Piano Nazionale Scuola Digitale e delle Linee di Orientamento per Azioni di prevenzione e Contrasto al Bullismo e al Cyberbullismo.

I contenuti delle linee guida sono suddivisi in sette aree:

- 1) L'adozione di una strategia integrata e globale
- 2) L'adozione di una politica di prevenzione
- 3) La segnalazione e presa in carico di situazioni potenzialmente a rischio
- 4) La valutazione dei bisogni e la definizione degli obiettivi
- 5) L'approccio metodologico
- 6) La valutazione degli interventi al fine di promuovere pratiche di comprovata efficacia
- 7) La protezione dei dati personali.

---

## ***1.2 - Ruoli e responsabilità***

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

Il Dirigente Scolastico garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica; promuove la cultura della sicurezza online e organizza, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC. Egli ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

L'animatore digitale in collaborazione con le Funzioni Strumentali presenti all'interno dell'Istituto supporta il personale scolastico da un punto di vista tecnico-informatico ed in riferimento ai rischi online, alla protezione e gestione dei dati personali. Promuove percorsi di formazione negli ambiti di sviluppo della "scuola digitale". Monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola.

Il referente per la prevenzione ed il contrasto del bullismo e cyber bullismo coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, si avvale anche della collaborazione delle forze di polizia, associazioni e centri di aggregazione giovanile del territorio. Inoltre coordina la revisione e aggiornamento del documento.

I Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Essi integrano parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo anche l'uso delle tecnologie digitali nella didattica. Supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete. Segnalano al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il dirigente scolastico e con il personale docente tutto. Diverse figure che, in sinergia, si occupano ciascuno per le proprie competenze, del funzionamento dell'Istituto scolastico che passa anche attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola. Il personale ATA deve, all'interno dei singoli regolamenti d'Istituto, essere coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

Gli Studenti e le Studentesse devono, in relazione al proprio grado di maturità e consapevolezza raggiunta, 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; partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

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; devono relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet. È estremamente importante che condividano quanto scritto nell'ePolicy dell'Istituto.

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 e assicurare la protezione degli studenti e delle studentesse durante le attività svolte 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).

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

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse.

Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat,

profili di social network). I soggetti esterni saranno informati relativamente al documento e-policy redatto dalla nostra scuola tramite una brochure che sintetizzi il nostro documento illustrando un decalogo e rimandando al sito istituzionale della scuola.

---

## ***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.

L'e-policy sarà presentata dai docenti, ai ragazzi e alle ragazze, ai bambini e alle bambine, in forma semplificata in modo da renderla più facilmente fruibile.

---

## ***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.

Le possibili condotte sanzionabili in relazione all'uso improprio delle TIC e della Rete a scuola da parte degli studenti e delle studentesse sono: 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 di scatti intimi e a sfondo sessuale; la condivisione di dati personali; l'invio di immagini o video volti all'esclusione di compagni/e. A seconda dell'età dello studente o della studentessa si interverrà sul contesto classe con attività specifiche educative e di sensibilizzazione

---

## ***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.

Inoltre i tre documenti (Patto di corresponsabilità, Regolamento d'istituto, e-policy) saranno riesaminati periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola, utilizzo di G suite, didattica a distanza.

---

## ***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 referente coordinerà la revisione e/o l'aggiornamento dell'ePolicy, inoltre con l'Animatore Digitale valuterà l'efficacia degli interventi e si considererà l'eventuale

necessità di apportare modifiche alla e-Policy e ai regolamenti in vigore.

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

---

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

Organizzare 1 evento di presentazione e conoscenza delle variazioni apportate all'e-Policy precedente ( del 2017/2018) rivolto ai docenti (Collegio dei docenti)

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

Organizzare dei momenti di confronto in classe per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.

Organizzare 1 evento di presentazione del progetto Generazioni Connesse dell'ePolicy rivolto agli studenti

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

Organizzare 1 evento di presentazione del progetto Generazioni Connesse e dell'ePolicy rivolto ai genitori

Continuare a partecipare attivamente al Safer Internet Day con varie iniziative.

# Capitolo 2 - Formazione e curriculum

---

## ***2.1. Curricolo 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.

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. Nel nostro Istituto ciò avviene attraverso la progettazione di un curriculum verticale per le competenze digitali. Al fine di permettere agli studenti di acquisire competenze chiave digitali, intendendo per competenze digitali quanto raccomandato dal Consiglio

europeo, la scuola si impegna ad organizzare percorsi volti a promuovere l'acquisizione di tali competenze, al fine di educare gli studenti e le studentesse ad un uso consapevole e responsabile delle tecnologie digitali, quale presupposto di una cittadinanza attiva. Ciò avviene attraverso un curriculum verticale per le competenze digitali, trasversale alle varie discipline e, naturalmente, adeguato al target di riferimento. Il curriculum digitale nel nostro istituto ha le sue basi, oltre che nel PNSD, nel quadro comune di riferimento europeo DigComp 2.1, il quale prevede:

#### Elaborazione delle informazioni

1.1 Navigare, ricercare e filtrare le informazioni

1.2 Valutare le informazioni

1.3 Memorizzare e recuperare le informazioni

#### Comunicazione

2.1 Interagire con le tecnologie

2.2 Condividere informazioni e contenuti

2.3 Impegnarsi nella cittadinanza online

2.4 Collaborare attraverso i canali digitali

2.5 Netiquette

2.6 Gestire l'identità digitale

#### Creazione di contenuti

3.1 Sviluppare contenuto

3.2 Integrare e rielaborare

3.3 Copyright e licenze

3.4 Programmazione

#### Sicurezza

4.1 Proteggere i dispositivi

4.2 Proteggere i dati personali

4.3 Tutelare la salute

4.4 Proteggere l'ambiente

#### Risoluzione dei problemi

- 5.1 Risolvere problemi tecnici
- 5.2 Identificare i bisogni e le risposte tecnologiche
- 5.3 Innovare e creare utilizzando la tecnologia
- 5.4 Identificare i gap di competenza digitale.

La valutazione avviene attraverso l'uso di rubriche valutative con descrittori e livelli di padronanza.

---

## ***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.

Consapevole dell'importanza che l'integrazione delle TIC rappresenti nella didattica tradizionale, il nostro Istituto continua ad impegnarsi affinché gli insegnanti raggiungano un buon livello di formazione in merito a ciò, ossia che "imparino a nuotare nell'oceano digitale" come viene metaforicamente affermato nel DigComp. Dalla formazione del corpo docente, infatti, dipende il livello che gli studenti raggiungeranno in materia di competenze digitali. E' 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 (DaD), ormai una modalità naturale di apprendimento al di fuori della scuola. Inoltre, le TIC permettono di sviluppare negli studenti 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. L'Istituto, quindi, attraverso il Collegio dei Docenti, favorisce la partecipazione del personale ad iniziative promosse dalla scuola (ad es. con l'aiuto dell'animatore digitale), dalle reti di scuole, dall'amministrazione

da corsil'Istituto deve promuovere la condivisione di buone pratiche nell'utilizzo consapevole delle TIC e prevenire e contrastare ogni forma di discriminazione, offesa, denigrazione e lesione della dignità dell'altro, nonché fenomeni di bullismo e cyberbullismo. E' necessario che i docenti dell'Istituto scolastico seguano percorsi formativi specifici ed adeguati e che sappiano di conseguenza educare i ragazzi a gestire le emozioni in un contesto online, che sappiano aiutarli ad esprimere se stessi e a sviluppare l'identità personale e sociale e, quindi, a modulare e gestire i propri ed altrui comportamenti, favorendo e promuovendo forme di convivenza civile. Per tali ragioni, l'Istituto deve prevedere specifici momenti di formazione permanente (inseriti anche nel PTOF) per gli insegnanti: iniziative seminariali con professionisti-esperti interni ed esterni alla scuola, giornate-settimane di approfondimento in accordo con la rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...) ecc. Sarebbe auspicabile pensare a momenti formativi di approfondimento che coinvolgano anche la famiglia e che sensibilizzino l'intera comunità educante. La scuola potrebbe inserire sul proprio sito istituzionale link e materiali informativi specifici come ad esempio quelli relativi al progetto "Generazioni connesse". liberamente scelti dai docenti (anche online).

---

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

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

L'Istituto promuove la condivisione di buone pratiche nell'utilizzo consapevole delle TIC e previene e contrasta ogni forma di discriminazione, offesa, denigrazione e lesione della dignità dell'altro, nonché fenomeni di bullismo e cyberbullismo. Pertanto si rende necessario che i docenti dell'Istituto scolastico seguano percorsi formativi specifici ed adeguati e che sappiano di conseguenza educare i ragazzi a gestire le emozioni in un contesto online, che sappiano aiutarli ad esprimere se stessi e a sviluppare l'identità personale e sociale e, quindi, a modulare e gestire i propri ed altrui comportamenti, favorendo e promuovendo forme di convivenza civile. Per tali

ragioni, l'Istituto prevederà momenti di formazione permanente per gli insegnanti: iniziative seminariali con professionisti-esperti interni ed esterni alla scuola, giornate-settimane di approfondimento in accordo con la rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...) ecc.

---

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

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

Il "Patto di Corresponsabilità" è un documento centrale per ogni istituzione scolastica, per cui è il nostro Istituto provvede ad aggiornarlo o integrarlo, insieme al Regolamento Scolastico, introducendo specifici riferimenti alle tecnologie digitali e all'ePolicy, al fine di creare una maggiore collaborazione e condivisione degli interventi di formazione e di contrasto al bullismo e al cyberbullismo da parte di tutta la comunità educante.

E' 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 e informazioni su iniziative e azioni della scuola in riferimento ai rischi connessi ad un uso distorto della Rete da parte degli studenti anche per regolamentare l'insieme dei provvedimenti sia di natura disciplinare che educativa nonché di prevenzione al fenomeno

Sul sito della scuola saranno condivise le attività svolte dal nostro Istituto in relazione ai temi del bullismo e del cyberbullismo e sarà indicata una sitografia da cui trarre informazioni utili.

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

---

### **AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023)**

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

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

- Organizzare e promuovere per il corpo docente e per le famiglie, incontri formativi sull'utilizzo 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 il corretto uso dei dati il nostro istituto scolastico:

Redige e mantiene un registro dei trattamenti dei dati

Valuta i rischi sulla privacy soprattutto in relazione a dati sensibili

Analizza il processo sulla raccolta/gestione del consenso

Adotta misure tecniche e organizzative idonee a garantire la sicurezza dei trattamenti

Pubblica in modo appropriato attività sul proprio sito istituzionale

Utilizza la G-suite con regole condivise e chiare.

Inoltre, il nostro Istituto, come già ha fatto nello scorso anno scolastico, organizzerà per i docenti ed il personale ATA, corsi di aggiornamento sulla legge relativa alla privacy.

Sul nostro sito, al seguente [link](#) è presente la liberatoria per a pubblicazione di dati e immagini degli alunni a fini didattici.

<http://www.ic1oria.edu.it/circolari/circolare-n-73-liberatoria-foto-video-dati-attivita-scolastica/>

---

## **3.2 - Accesso ad Internet**

- 1. L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
- 2. Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
- 3. Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
- 4. L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
- 5. Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento*

*di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola".

Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

Il nostro Istituto ha elaborato una liberatoria ed informativa relativa all'utilizzo della piattaforma G-suite for education che i genitori hanno sottoscritto.

<http://www.ic1oria.edu.it/8035-circolare-n-51-informativa-e-liberatoria-per-lutilizzo-della-piattaforma-gsuite-for-education/>

Il nostro istituto scolastico garantisce l'accesso ad internet in tutti gli ambienti nonché la sicurezza di tale accesso sia per la safety che per la security. Il primo termine, safety, riguarda la prevenzione dei rischi, a partire dalla consapevolezza, conoscenza e preparazione per un uso consapevole delle tecnologie digitali. Il secondo termine, security, in relazione ad Internet e ai media si riferisce a tutte quelle risorse tecnologiche che rendono sicuro l'ambiente digitale, dall'antivirus al firewall, da un protocollo di trasmissione dei dati sicuro (https) all'aggiornamento di software e sistemi operativi. Per garantire safety e security la scuola:

Mantiene separate le reti della didattica e della segreteria

Aggiorna periodicamente software e Sistema operativo

Definisce la programmazione di backup periodici

Garantisce formazione adeguata allo staff, incluso il corpo docenti

Testa regolarmente le possibili vulnerabilità

Predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo

Imposta il browser per l'eliminazione dei cookies alla chiusura

Definisce una policy sulle password le quali devono essere forti, non memorizzate nei dispositivi, non condivise

Sviluppa il regolamento sull'uso delle tecnologie a scuola (policy di uso accettabile).

---

### ***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.

Gli 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. Fra gli strumenti di comunicazione utili alla nostra utenza citiamo il sito web della scuola, la pagina facebook ed Instagram, il registro elettronico, la G-suite for education, le e-mail. Nell'utilizzo di tali strumenti la scuola adotta regole condivise e chiare ed utilizza una adeguata netiquette.

---

### ***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.

L'utilizzo delle TIC personali nella nostra scuola sarà regolamentato sia da un adeguamento del Regolamento d'istituto e del Patto di corresponsabilità .

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

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

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

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse

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

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

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

# 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.

La necessità di supportare gli alunni affinché abbiano un approccio positivo e consapevole delle TIC, inteso come protezione dai rischi della rete ma anche come capacità di saper cogliere le opportunità insite in essa, induce la scuola e i genitori a non perdere di vista il proprio ruolo educativo, le proprie responsabilità. A tal fine la scuola deve promuovere azioni di Sensibilizzazione e Prevenzione, cioè informare sui

rischi che potrebbero presentarsi in rete e fornire agli studenti gli strumenti idonei per prevenirli. La prevenzione va distinta in: Prevenzione Universale, fatta su tutti gli alunni, perché potrebbero essere tutti potenzialmente a rischio; Prevenzione Selettiva, rivolta ad un gruppo di studenti in cui il rischio online si sia già manifestato e sia già stato segnalato; si agirà per migliorare le competenze; Prevenzione Indicata, finalizzata a ridurre le problematiche emerse oppure a dare supporto alle vittime.

---

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

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

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

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

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

giovanile del territorio.

- Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Il nostro Istituto si propone di dare piena attuazione alla recente normativa in materia di bullismo e cyber bullismo ( legge 71/2017), con l'obiettivo di contrastare tali fenomeni in tutte le loro manifestazioni.

---

### ***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.

La scuola si propone, in un clima di convivenza civile, di far acquisire a tutti gli alunni attitudini di rispetto verso l'unicità di ciascuno, nell'accettazione dell'altro. Essa ha il dovere di creare e mantenere un ambiente sano e sereno, per facilitare lo studio e la crescita personale. Gli insegnanti insieme ai genitori hanno l'obbligo di aiutare gli alunni a diventare adulti responsabili, in grado di partecipare in modo positivo alla nostra società; prevenire e contrastare ogni forma di discriminazione anche informatica, nel pieno rispetto delle differenze, il sostegno dell'assunzione di responsabilità, la consapevolezza dei diritti e dei doveri e il dialogo tra le culture,

decostruendo ogni forma di stereotipo ed educando all'empatia.

Per attuare quanto detto sopra la nostra scuola attuerà progetti specifici come ha già fatto negli anni precedenti, avvalendosi anche del supporto di "generazioni connesse"

---

## **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 promuoverà percorsi formativi, attività progettuali che aiutano gli studenti a cogliere i pericoli insiti nella dipendenza da Internet che, come tutte le altre forme di dipendenza, mette a rischio la loro vita, ripercuotendosi sulla sfera delle relazioni interpersonali che diventano via via più aride fino ad essere sostituite da quelle virtuali. Se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi, questo deve essere il messaggio di cui la scuola deve farsi promotrice.

Inoltre, qualora si presentassero casi che coinvolgano i nostri studenti, di come accordo con la famiglia, saranno predisposti percorsi di supporto psicologico.

---

## **4.5 - Sexting**

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

Sicuramente il "sexting" rientra tra i rischi incontro ai quali gli alunni possono imbattersi se non utilizzano Internet con consapevolezza. Pertanto la scuola si propone

sia di organizzare incontri con personale specializzato che svolga attività di informazione e sensibilizzazione, sia di progettare percorsi mirati, relativi all'educazione alla sessualità e all'affettività, come ha già fatto in passato, magari coinvolgendo anche gli alunni delle ultime classi della scuola primaria.

---

## **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.

E' sempre più frequente che le giovani generazioni facciano conoscenze e amicizie attraverso l'uso della Rete, con utilizzo di chat e social network. La mancanza di un contatto diretto con le persone conosciute comporta il rischio che gli amici virtuali siano in realtà persone male intenzionate, che adescano bambini o adolescenti su Internet allo scopo di intrecciare relazioni intime. Il grooming è un fenomeno molto diffuso che non conosce distinzione di genere. I soggetti più esposti sono gli adolescenti, non solo perché vivono nella specifica fase della vita destinata alla costruzione di un'identità sessuale, ma anche a causa della curiosità insita all'adolescenza; ciò li porta a voler conoscere persone che possano iniziarli ad esperienze nuove. Il grooming è particolarmente pericoloso perché l'adescatore cerca di intercettare i bisogni e i desideri dell'adolescente e manipolarli a proprio vantaggio, attraverso una dinamica non violenta ma instaurando un rapporto di fiducia con lo scopo di renderlo poi una relazione di tipo intimo. La comunità educante ha dunque il compito di preparare gli studenti ai rischi nascosti in rete, attraverso incontri con

esperti che trattino la tematica in un discorso più ampio di sicurezza e uso consapevole del web. Qualora si riscontrino casi che coinvolgano gli studenti dell'Istituto in accordo con le famiglie saranno applicate le procedure previste dalla normativa vigente e proposti eventuali percorsi educativi e/o di supporto psicologico con l'appoggio dello Sportello psicologico attivo presso il nostro istituto.

---

## 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](#).**

Tenuto conto della delicatezza dell'argomento e, al contempo, della necessaria informazione ai fini preventivi e considerati gli evidenti legami con il fenomeno del sexting, l'istituto affronterà la tematica tenendo in considerazione la maturità, la fascia d'età e il tipo di informazioni che si possono condividere; inoltre, la trattazione sarà affidata a personale esperto (ad esempio la Polizia Postale o altro personale adeguatamente formato). Al fine di informare e sensibilizzare tutta la comunità scolastica (genitori compresi) nei confronti della problematica, l'apposita sezione del sito di istituto sarà implementata con opportune informazioni, tra cui la sezione "Segnala contenuti illegali" (Hotline) del sito [www.generazioniconnesse.it](http://www.generazioniconnesse.it). Qualora si riscontrino casi che coinvolgano studenti dell'istituto, in accordo con le famiglie saranno applicate le procedure previste dalla normativa vigente, dal Regolamento di istituto, dal Patto di corresponsabilità e saranno proposti eventuali percorsi educativi o momenti di supporto psicologico ad opera di personale specializzato.

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

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

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

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

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

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

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

- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.
  
- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

# Capitolo 5 - Segnalazione e gestione dei casi

---

## 5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

- **Cyberbullismo:** è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/le studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online:** se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenni e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting:** nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

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

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di [Helpline 19696](#) e [Chat di Telefono Azzurro](#) per supporto ed emergenze;
- [Clicca e segnala di Telefono Azzurro](#) e [STOP-IT di Save the Children Italia](#) per

segnalare la presenza di materiale pedopornografico online.

## **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 fare 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).

Tra le possibilità sopra elencate l'istituto in particolare si servirà

di un docente Referente per la lotta al bullismo e al cyberbullismo a cui comunicare le segnalazioni, prontamente riferite al Dirigente;

un docente (uno dei Vicari) a cui comunicare le segnalazioni, prontamente riferite al Dirigente;

un docente (Funzione Strumentale preposta) che si occuperà, all'occorrenza, di problemi collegati all'inclusione di ragazzi coinvolti in situazioni a rischio nella rete;

uno sportello di ascolto o psicologico gestito da professionisti, esterni

modulistica utile per la segnalazione, a disposizione degli studenti tramite il sito di istituto

si cercherà di portare a conoscenza degli studenti e delle studentesse il servizio Helpline del progetto Generazioni Connesse, contattabile tramite il numero gratuito 1.96.96.

---

### ***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.

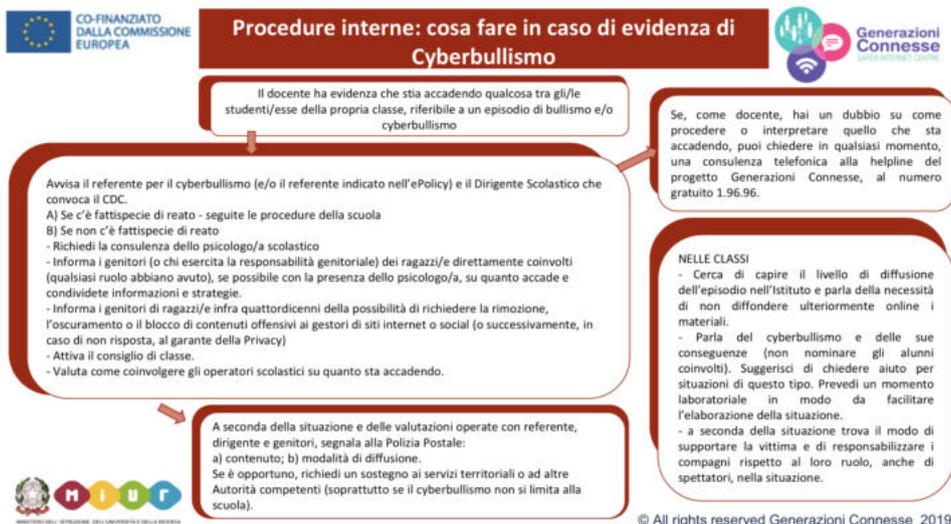
- **Ufficio Scolastico Regionale:** supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni:** accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete 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.

Eventuali associazioni sul territorio verranno individuate e contattate in caso di necessità specifiche.

---

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

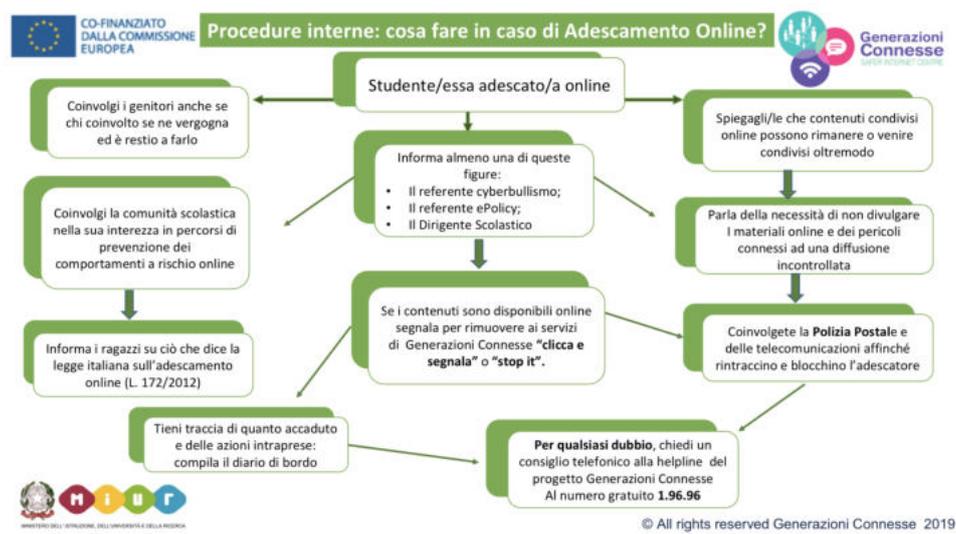
### **Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?**



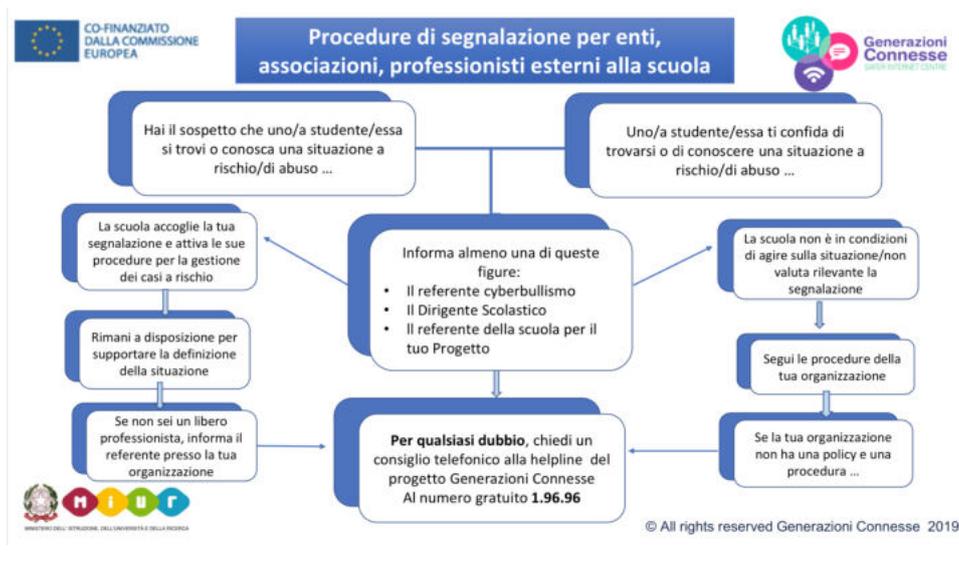
## Procedure interne: cosa fare in caso di sexting?



## 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 Regolamento di Istituto prevede alcune procedure da attivare e le sanzioni da applicare nei casi previsti dalla normativa in vigore.

<http://www.ic1oria.edu.it/regolamento/>

## *Il nostro piano d'azioni*

Monitoraggio e perfezionamento delle procedure di segnalazione

Condivisione delle procedure con la comunità scolastica tramite il sito istituzionale

Formazione e aggiornamento delle varie componenti presenti nell'istituto.

