



# Documento di ePolicy

RAIC81300N

I.C. "DON STEFANO CASADIO"

VIA DANTE ALIGHIERI 8 - 48033 - COTIGNOLA - RAVENNA (RA)

Paolo Taroni

# 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.

Gli ultimi anni di emergenza sanitaria hanno contribuito ad accelerare ulteriormente lo sviluppo delle nuove tecnologie, il loro utilizzo nell'ambito didattico e la maggiore diffusione nella vita di tutti i giorni. E' compito dell'intera comunità scolastica, genitori inclusi, garantire che gli studenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo sicuro, responsabile e consapevole.

In coerenza con il Piano e Regolamento per la Didattica Digitale Integrata elaborato dal nostro Istituto e a sua integrazione, la presente e-policy ha lo scopo di definire le linee guida in materia di:

- utilizzo consapevole delle TIC negli ambienti scolastici e nella didattica;
- prevenzione e gestione di situazioni problematiche relative all'uso delle tecnologie digitali;
- segnalazione dei casi individuati all'interno della scuola;
- gestione dei casi, ovvero le misure che la scuola intende attivare a supporto delle famiglie e degli studenti vittime o spettatori attivi e/o passivi di quanto avvenuto.

L'IC don Stefano Casadio sta aderendo al progetto "Generazioni Connesse, promosso dal MIUR in collaborazione con l'Unione Europea. Ha elaborato il presente documento in conformità con le LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto del bullismo e del cyberbullismo emanate dal Ministero dell'Istruzione, dell'Università, della Ricerca in collaborazione con il Safer Internet Center per l'Italia. Si premette:

- li progetto "Generazioni connesse" sarà inserito nel nostro Piano Triennale dell'Offerta Formativa e le azioni preventivate nel Piano d'Azione della nostra scuola (prodotto nel mese di giugno 2021), verranno portate avanti progressivamente nei prossimi anni;

- le attività di promozione all'utilizzo delle tecnologie digitali nella didattica costituiscono un tema centrale per l'attuazione del Piano Nazionale Scuola Digitale e sono già previste nel Piano Triennale dell'Offerta Formativa.
- 

## ***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 on-line dei membri della comunità scolastica;
- garantisce agli insegnanti una formazione adeguata al fine di promuovere l'utilizzo delle TIC in modo efficace dal punto di vista Didattico, sicuro e consapevole rispetto ai rischi di Internet e della rete;
- garantisce un sistema di monitoraggio e di controllo interno delle TIC e della sicurezza on-line;
- attiva le procedure previste in caso di violazione del regolamento nell'utilizzo delle TIC a scuola.

L' Animatore digitale (con il Team Digitale e F.S. per l'Innovazione Didattica)

- pubblica e diffonde la ePolicy sul sito della Scuola;
- stimola la formazione di competenze relative alla "scuola digitale" e fornisce consulenza in merito alla conoscenza, prevenzione e gestione dei rischi on-line;
- osserva l'evoluzione relativa all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, propone la diffusione di pratiche innovative o migliorative e i conseguenti aggiornamenti dei regolamenti dell'Istituto
- assicura che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate

- coinvolge la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti alla "scuola digitale".

#### Il Referente del bullismo e cyberbullismo

- promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e cyberbullismo, avvalendosi anche della collaborazione delle Forze di polizia, associazioni e centri di aggregazione giovanile del territorio;
- coinvolge (ove possibile), con progetti e percorsi formativi, studenti, colleghi e genitori.

#### Il Direttore dei servizi generali e amministrativi

- assicura, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;
- garantisce il funzionamento dei diversi canali di comunicazione della scuola all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di Internet.

#### Personale A.T.A. (Amministrativi)

- si informa sul Regolamento di utilizzo sicuro delle TIC e sulla Policy;
- utilizza, in modo professionale, i canali ufficiali della scuola per le comunicazioni digitali con gli studenti e le loro famiglie;
- assicura la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- segnala problemi o formula proposte all'Animatore Digitale, per l'elaborazione di soluzioni e innovazioni sul piano dell'utilizzo e della sicurezza delle Tic.

#### Personale A.T.A. (collaboratori scolastici)

- si informa sul Regolamento di utilizzo sicuro delle TIC e sulla Policy;

- si assicura che i dispositivi informatici (lim, schermi, pc) trovati in funzione siano nelle condizioni di essere chiusi (che non siano per esempio in fase di aggiornamento o che la ventola del proiettore stia raffreddando la lampada), quindi provvede al loro spegnimento e alla disconnessione della rete elettrica.
- esegue la pulizia di PC, laptop, cavi e proiettori cercando di non muoverli e senza utilizzare supporti umidi o bagnati per evitare danni di carattere elettrico;
- assicura la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- segnala problemi o formula proposte all'Animatore Digitale e/o al referente del cyberbullismo, per l'elaborazione di soluzioni e innovazioni sul piano dell'utilizzo e della sicurezza delle Tic.

#### I Docenti

- si informano sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di Internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- diffondono tra gli alunni le modalità per utilizzare le TIC in modo sicuro e corretto;
- sensibilizzano gli alunni riguardo le potenzialità del Web in quanto strumento di ricerca, da utilizzarsi nel rispetto della normativa sui diritti d'autore
- utilizzano, in modo professionale, il canale ufficiale della scuola per le comunicazioni digitali con gli studenti e le loro famiglie;
- assicurano la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllano l'uso delle tecnologie digitali e dispositivi mobili da parte degli alunni durante le lezioni, i cambi d'ora e ogni altra attività scolastica (ove consentito);
- nelle lezioni in cui è programmato l'utilizzo di Internet, verificano che gli alunni accedano con le proprie credenziali e li guidano a siti adatti all'attività prevista;

- comunicano ai genitori le eventuali problematiche emerse nel caso di un utilizzo non appropriato delle TIC da parte dei propri figli, al fine di concordare coerenti linee di intervento a carattere educativo;
- segnalano problemi o formulano proposte all'Animatore Digitale, per l'elaborazione di soluzioni e innovazioni sul piano dell'utilizzo e della sicurezza delle Tic.

#### Gli Alunni

- Si informano sul Regolamento di utilizzo sicuro delle TIC e sulla ePolicy
- Rispettano tutti i Regolamenti scolastici e il Patto di Corresponsabilità, le indicazioni per l'accesso a Internet e rispettano quanto richiesto dai docenti in merito a sicurezza e correttezza nell'utilizzo delle TIC, del Web e della Rete Scolastica.
- esprimono domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di Internet ai docenti e ai genitori;
- partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e si fanno promotori di quanto appreso anche attraverso possibili percorsi di peer education

#### I Genitori

- Si informano sul Regolamento di utilizzo sicuro delle TIC e sulla ePolicy;
- contribuiscono in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- incoraggiano l'impiego delle TIC da parte degli alunni nello svolgimento del compito a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza;
- sostengono i figli nel rispettare i regolamenti scolastici per l'utilizzo delle TIC, le indicazioni per l'accesso a Internet e l'utilizzo sicuro dello stesso, il regolamento interno di Istituto e il patto di corresponsabilità in conformità con quanto richiesto dai docenti;



- agiscono in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite.  
LINKKK

Gli Enti esterni e le Associazioni

- Si conformano alla politica della scuola riguardo l'uso consapevole delle TIC e della Rete;
- Promuovono comportamenti sicuri, la sicurezza online e assicurano la protezione degli studenti 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).

Le organizzazioni/associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve o/e lungo periodo, dovranno prendere atto di quanto stilato nell'E-policy dell'Istituto o eventualmente sottoscrivere un'informativa sintetica del documento in questione, presente nel contratto.

---

## ***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.

**Gli Studenti e le Studentesse saranno adeguatamente formati e informati in modo da:**

- **essere autonomi nell'uso consapevole e maturo dei dispositivi e della tecnologia informatica;**
- **condividere regole di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici;**

- **essere in grado di riconoscere e quindi prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e.**

**Inoltre gli studenti e le studentesse sapranno che, a scuola, la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione.**

**Per una condivisione chiara, l'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule o laboratori con accesso a Internet**

---

## ***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.

I provvedimenti disciplinari da adottare da parte dei docenti o dei consigli di classe nei confronti dell'alunno che ha commesso un'infrazione alla Policy (in proporzione sia all'età dello studente, sia alla gravità dell'infrazione commessa) saranno i seguenti:

- rimprovero verbale;
- richiamo scritto comunicato tramite cartaceo/registro elettronico
- nota disciplinare comunicata tramite cartaceo/registro elettronico
- sanzione commisurate alla gravità della violazione decisa estemporaneamente dal docente o deliberata dal Consiglio di Classe sulla base di quanto previsto dal Regolamento d'Istituto e dal Regolamento di Disciplina (<http://www.iccotignola.edu.it/index.php/il-nostro-istituto/regolamenti>)

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni.

Infrazioni del personale scolastico

Le infrazioni alla ePolicy da parte del personale scolastico possono riguardare sia la mancata osservanza delle regole sulla gestione della strumentazione, sia la mancata sorveglianza e pronto intervento nel caso di infrazione da parte degli alunni.

La gestione delle infrazioni in quest'ambito ricade nella disciplina contrattuale.

---

## ***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.

Per quanto riguarda l'armonizzazione dei Regolamenti con la presente ePolicy si fa riferimento ai seguenti documenti, presenti nel Sito della scuola:

Patto di corresponsabilità

Regolamento di Istituto

Piano e regolamento per la Didattica Digitale Integrata

Regolamento di disciplina

---

## ***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.

**da compilare con le indicazioni contenute nella lezione**

## **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 del progetto Generazioni Connesse rivolto ai docenti
- 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 il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare un evento di presentazione e conoscenza dell'epolicy rivolto ai genitori.
- Realizzare un modello di segnalazione di eventuali casi di bullismo/cyberbullismo;
- Realizzare un'area del sito web con riferimenti e documenti su bullismo/cyberbullismo

# 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.

Competenza digitale significa non solo padroneggiare le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con "autonomia e responsabilità" nel rispetto degli altri e sapendone prevenire ed evitare i pericoli. In questo senso, tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione. Per questo l'IC Don Stefano Casadio sta progettando, grazie ai fondi PON, un percorso di formazione delle classi prime con i seguenti obiettivi:

- promuovere un uso consapevole delle nuove tecnologie;
- sensibilizzare e attivare gli studenti sui rischi e i pericoli derivanti dalla rete
- sviluppare le abilità di base nelle TIC (uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni);
- acquisire consapevolezza su come le TIC possono coadiuvare la creatività e

l'innovazione.

L'Istituto ha in fase di elaborazione un curriculum trasversale specifico per le competenze digitali.

---

## ***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.

Nel PTOF dell'Istituto Comprensivo Don Stefano Casadio è previsto un piano triennale per la formazione del personale sulle TIC. Sono stati tenuti corsi interni di formazione sull'uso di GSuite for Education e sul Coding. Sono inoltre presenti progetti di formazione Peer to Peer (progetto Giocodiamo).

Il corpo docente ha partecipato a corsi di formazione anche nell'ambito del Piano Nazionale per la Scuola Digitale, organizzati dall'USR Emilia Romagna attraverso il "Servizio Marconi - Tecnologie della Società dell'Informazione (TSI)", oltre che da iniziative organizzate dall'Ambito 17 USR ER, dalla piattaforma SOFIA, dal MIUR-PON, MIUR ELISA. per cui generalmente la maggior parte dei docenti di ruolo possiede una buona base di competenze. Il percorso complesso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica e sulla sicurezza on-line può prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva all'interno dell'istituto e/o on-line, con la condivisione delle conoscenze dei singoli e il supporto dell'Animatore digitale.

Il team per l'innovazione digitale organizza eventi formativi per la diffusione delle buone pratiche in tema digitale (progetto Digital Week-End).

---

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

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

L'Istituto Comprensivo 'Don Stefano Casadio' si avvale della figura dell'Animatore digitale e di un team di docenti che, con il Dirigente Scolastico e il D.S.G.A., collabora per raggiungere gli obiettivi di innovazione del PNSD nella scuola. Inoltre è attiva la figura del Referente d'Istituto per le attività di prevenzione e contrasto al bullismo e al cyberbullismo (L.107/2015). Nell'anno 2020/2021 si è svolto un corso di formazione interno specifico "Gestione delle classi, relazioni interpersonali all'interno della scuola e prevenzione degli atti di bullismo". Si rende, comunque, necessaria la formazione di tutti i docenti sull'uso consapevole e sicuro di Internet e sui rischi della rete.

Per corrispondere alle esigenze di docenti e studenti l'Istituto ha in programma diverse azioni specifiche:

- 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.

L'Istituto ha in programma l'inserimento di un'area specifica sul sito dell'Istituto con materiali formativi ed informativi per docenti, personale scolastico, genitori e alunni.



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

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

Scuola e famiglia sono chiamate a collaborare per garantire la crescita formativa di ciascun alunno, perciò stipulano all'inizio dell'anno scolastico il Patto Educativo di Corresponsabilità. Alla luce del progresso e dell'evoluzione delle tecnologie, l'Istituto promuoverà iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, favorendo la conoscenza delle numerose situazioni di rischio online. A tal fine saranno probabilmente previsti incontri fra docenti e/o esperti e genitori sui temi oggetto della Policy per la diffusione del materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati (Generazioni Connesse) e dalle forze dell'ordine. Sul sito della scuola, inoltre, sarà pubblicato il presente documento per la divulgazione delle informazioni e delle procedure contenute, per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'Istituto e per prevenire i rischi legati ad un utilizzo scorretto di Internet.

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

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

**Scegliere almeno 1 di queste azioni**

- Effettuare un'analisi del fabbisogno formativo 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.

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

---

## 3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

In merito alla protezione dei dati personali, si fa riferimento a quanto previsto dal Decreto Legislativo del 30 giugno 2003, n.196 (cosiddetto Codice della Privacy), integrato dal D. Lgs. 10 agosto 2018, n. 101, e dal GDPR (General Data Protection Regulation) n. 679 del 2016. All'atto dell'iscrizione viene fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori, come ad esempio l'utilizzo di fotografie, video o altri materiali audiovisivi contenenti l'immagine e/o il nome del proprio figlio/a all'interno di attività educative e didattiche per scopi documentativi, formativi e informativi, durante gli anni di frequenza della scuola. A tale proposito si evidenzia che le immagini e le riprese audiovideo realizzate dalla scuola, nonché gli elaborati prodotti dagli studenti durante le attività scolastiche, potranno essere utilizzati esclusivamente per documentare e divulgare le attività della scuola tramite il sito Internet di Istituto. L'autorizzazione non consente l'uso dell'immagine in contesti che pregiudichino la propria dignità personale ed il decoro e comunque per uso e/o fini diversi da quelli sopra indicati. Inoltre, in caso di partecipazioni a concorsi o manifestazioni l'Istituto richiede apposita autorizzazione, chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato all'interno di modulistica o sul proprio sito web istituzionale. La formula utilizzata per chiedere il consenso è, in ogni caso, comprensibile, semplice e chiara. Pertanto, in ottemperanza al GDPR (General Data Protection Regulation) e al D. Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre, la scuola non si impegna solo a tutelare la privacy degli/le studenti/esse e delle loro famiglie, ma anche ad informare e soprattutto rendere consapevoli gli/le studenti/esse di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri. Allo stesso modo sono forniti ai genitori, o ai tutori legali degli studenti, modelli di liberatoria per ogni attività interna ed esterna alla scuola (uscite, gite, interventi di esperti esterni...) e, negli ultimi anni, per la creazione e l'utilizzo di account istituzionale sulla piattaforma GSuite. Tale modulistica sarà allegata al presente documento di ePolicy.

---

## **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.

L'accesso a Internet è possibile e consentito per la didattica in tutti i plessi della infanzia, primaria e della secondaria di primo grado attraverso reti WiFi o cablaggio. La Dirigenza e l'Amministrazione hanno una rete separata. Le impostazioni dei computer presenti nei laboratori e nelle aule sono definite e mantenute dal responsabile dei laboratori, il quale segnala alla segreteria e ai tecnici competenti eventuali malfunzionamenti e disservizi.

Le Postazioni di Lavoro degli alunni sono occasionalmente utilizzati anche dai docenti, quando questi si servono dei laboratori, ma gli alunni non possono utilizzare le PdL dei docenti.

Nelle postazioni non è consentito l'uso della webcam, a meno che la programmazione didattica non richieda lo svolgimento di videoconferenze o altro. I docenti possono accedere alla propria sezione del registro elettronico con credenziali personali. L'account di posta elettronica è quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. Anche tutti i docenti dell'Istituto e gli studenti della Scuola Primaria e Secondaria di I grado possiedono un account generato dalla scuola per consentire loro l'accesso a piattaforme didattiche come Classroom o per consentire la didattica a distanza sperimentata già lo scorso anno scolastico su Meet.

Il regolamento d'Istituto, 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;
- durante le attività che prevedono lo smartphone, utilizzarlo esclusivamente per svolgere le attività didattiche previste;
- segnalare immediatamente materiali inadeguati ai propri insegnanti.

I docenti si impegnano a:

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

---

## **3.3 - Strumenti di comunicazione online**

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

L'istituto comprensivo don Stefano Casadio ha attivato Google Suite per i docenti di tutti gli ordini e per gli alunni della Primaria e della Secondaria di primo grado. Gli alunni si attengono al Regolamento specifico per l'uso di Gsuite, disponibile sul sito della scuola al link [Regolamenti di Istituto](http://iccotignola.it/index.php/il-nostro-istituto/regolamenti) <http://iccotignola.it/index.php/il-nostro-istituto/regolamenti>. Pertanto la comunicazione online può avvenire sia attraverso posta istituzionale (@iccotignola.edu.it) sia mediante registro elettronico ARGO sia mediante sito web [www.iccotignola.it](http://www.iccotignola.it) dove è disponibile una pagina comunicazioni famiglie costantemente aggiornata sulle informazioni da fornire ai genitori. La scuola non dispone di canali di social network, ma promuove l'insegnamento di comportamenti corretti e sicuri da parte degli studenti stutturando percorsi specifici per l'uso sicuro dei social network, per il rispetto della netiquette ecc.

---

## **3.4 - Strumentazione personale**

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle 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.

**Come da Regolamento d'Istituto agli studenti è fatto assoluto divieto di usare all'interno dell'Istituto scolastico, se non per scopi esclusivamente didattici autorizzati dal docente, smartphone e/o ogni altro apparato multimediale ( mp3, ipod, ipad, notebook, fotocamera, videocamera, ecc...). Il divieto non si applica soltanto all'orario delle lezioni, ma all'intera permanenza dell'alunno all'interno della struttura scolastica (intervalli, pausa mensa...) e anche in corrispondenza delle uscite o dei viaggi di istruzione, durante i quali l'utilizzo può essere autorizzato solo dal docente. I predetti dispositivi devono essere tenuti spenti e opportunamente custoditi. Come da Regolamento d'Istituto ai sensi della C.M. n.362 del 25/08/98, i docenti non possono utilizzare i telefoni cellulari durante l'orario di lavoro se non per comprovata necessità lavorativa (per esempio la compilazione del registro per la mancata funzionalità dei dispositivi in dotazione nelle classi), a scopo didattico ed integrativo di quelli scolastici disponibili o per motivi di emergenza. (CONTROLLARE!!!)**

**Per quanto riguarda il comodato d'uso agli studenti delle strumentazioni in dotazione alla scuola è stato stilato un regolamento con criteri secondo i quali viene redatta una graduatoria in base a diversi elementi quali ad esempio l'indicatore ISEE. (CONTROLLARE)**

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

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

**Scegliere almeno 1 di queste azioni:**

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

**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.
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare 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.

In questi anni la sensibilizzazione e prevenzione dei rischi connessi all'uso della rete ha riguardato principalmente gli alunni della secondaria.

Anche se non ci sono pervenute segnalazioni di abusi gravi, l'uso di dispositivi connessi alle rete è sempre più precoce e spesso previsto dalla scuola stessa.

Il nostro Istituto da alcuni anni si avvale di interventi di esperti (Polizia di Stato, Carabinieri, ) che operano attraverso incontri specifici rivolti agli alunni e aventi come tematica il rispetto della legalità e l'uso corretto delle nuove tecnologie.

Si ritiene comunque necessario un ripensamento degli interventi, che dovranno riguardare un numero crescente di studenti e, possibilmente, tutte le famiglie e tutti gli insegnanti.

---

## ***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, in ottemperanza alla legge 71/2017, si è dotato di un referente per la prevenzione e il contrasto del cyberbullismo con il compito di coordinare le iniziative di prevenzione del fenomeno.

Il cyberbullismo è una forma di prepotenza virtuale e non, attuata attraverso l'uso di internet e delle tecnologie digitali. L'Istituto Comprensivo Don Stefano Casadio promuove le seguenti azioni volte a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli studenti:

- diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web.
- organizzare incontri con esperti (psicologo, Polizia Postale, ecc.) nelle singole classi e aventi per oggetto le tematiche del cyberbullismo, del sexting e dell'adescamento.
- richiedere autorizzazione esplicita da parte dei genitori all'utilizzo dei dati personali degli alunni (es. liberatoria per la pubblicazione di foto, immagini, video relativi al proprio/a figlio/a per la partecipazione a progetti didattici e altro).
- Condurre un attento monitoraggio da parte del personale docente affinché il regolamento venga rispettato.
- strutturare percorsi di segnalazione di atti di cyberbullismo e di bullismo chiari e accessibili a tutti, personale ATA, docenti e studenti.
- Intervenire tempestivamente tramite opportuna sanzione qualora il regolamento venga disatteso.

---

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

## ***prevenirlo***

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

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

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

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

Il fenomeno denominato "hate speech" si sta diffondendo in maniera sempre più frequente, pertanto il nostro Istituto promuove tutte le iniziative che consentono di affrontare il problema. Oltre ad interventi curati da esperti esterni sul tema specifico, si realizza una didattica improntata al rispetto degli altri sin dall'infanzia, con attività creative di gioco, il confronto sociale, informazione globale.

---

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

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

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

L'Istituto Comprensivo Don Stefano Casadio ritiene fondamentale promuovere azioni

che favoriscano il benessere digitale degli studenti. Pertanto, soprattutto nell'ottica di un utilizzo frequente delle tecnologie in ambito didattico, prevede di strutturare delle attività di riflessione e consapevolezza che permettano agli studenti di interiorizzare meccanismi di autocontrollo nell'utilizzo della Rete e stabilendo chiare e semplici regole di utilizzo.

---

## **4.5 - Sexting**

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

Per quanto riguarda il rischio del sexting, interventi di sensibilizzazione sui ragazzi appaiono connessi ad una generale educazione all'affettività. Questa viene svolta nella secondaria in maniera trasversale da docenti di varie discipline, coordinati da quelli di scienze e religione.

---

## **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.

Le tecnologie digitali consentono ai giovani di ampliare la propria rete di amicizie in modo quasi smisurato: non di rado gli adolescenti "concedono" la loro amicizia non solo a persone che conoscono direttamente, ma anche ad "amici di amici". Questo li espone a rischi notevoli, come quello di dare accesso a sconosciuti al loro mondo online e quindi a informazioni personali. L'adescamento online (grooming) consiste nel tentativo, da parte di un adulto, di avvicinare un/a bambino/a o adolescente per scopi sessuali, conquistandone la fiducia attraverso l'utilizzo della rete Internet, per cui una volta che i docenti abbiano riconosciuto alcuni segni che possano rinviare ad una situazione di adescamento on line, procederanno ad informare tempestivamente:

- la referente tramite modulo;
- il Consiglio di Classe;
- lo psicologo della Scuola;
- i genitori dell'alunno oggetto di adescamento.

La Dirigente Scolastica valuterà se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia di Stato o i Servizi Sociali.

---

## **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](#).**

Come per quanto riguarda il problema del grooming, si tratta di una questione molto delicata: se da una parte gli adulti, genitori e docenti, sono tenuti a documentarsi e conoscere il fenomeno, interventi diretti ai ragazzi non sono sempre opportuni.

La nostra scuola ritiene che i più giovani debbano acquisire competenze in grado di orientarli e guidarli nelle loro scelte anche online grazie ai percorsi di educazione civica e in particolare di educazione all'affettività.

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

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



- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/le studenti/studentesse, con il coinvolgimento di esperti.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/le studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.
- Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.
- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

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

**Scegliere almeno 1 di queste azioni:**

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/le

studenti/studentesse, con il coinvolgimento di esperti.

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

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

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

Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/le studenti/studentesse.

Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.

Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

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

# Capitolo 5 - Segnalazione e gestione dei casi

---

## 5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

segnalare la presenza di materiale pedopornografico online.

Pertanto sono da considerare degni di segnalazione:

contenuti afferenti la violazione della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);

contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);

contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

---

## **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).

Docente referente per le segnalazioni.

Non è stato predisposto un indirizzo e-mail specifico per le segnalazioni, ma con l'introduzione dell'email istituzionale anche per i ragazzi, è stata incoraggiata la comunicazione attraverso questo canale.

Gli studenti compilando apposito modulo di richiesta possono accedere ad uno sportello di ascolto con professionisti;

---

## 5.3. - *Gli attori sul territorio*

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

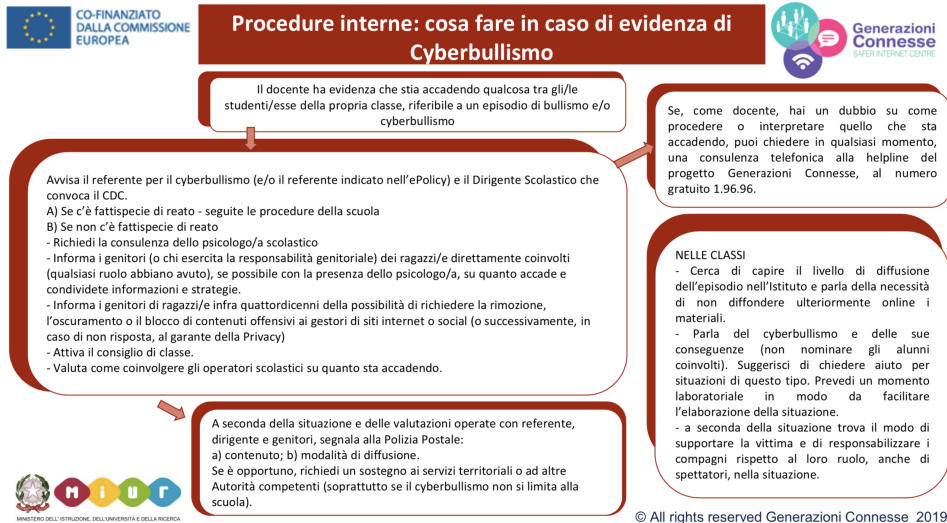
Per una mappatura degli indirizzi di tali strutture è possibile consultare il [Vademecum](#) di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza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

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

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

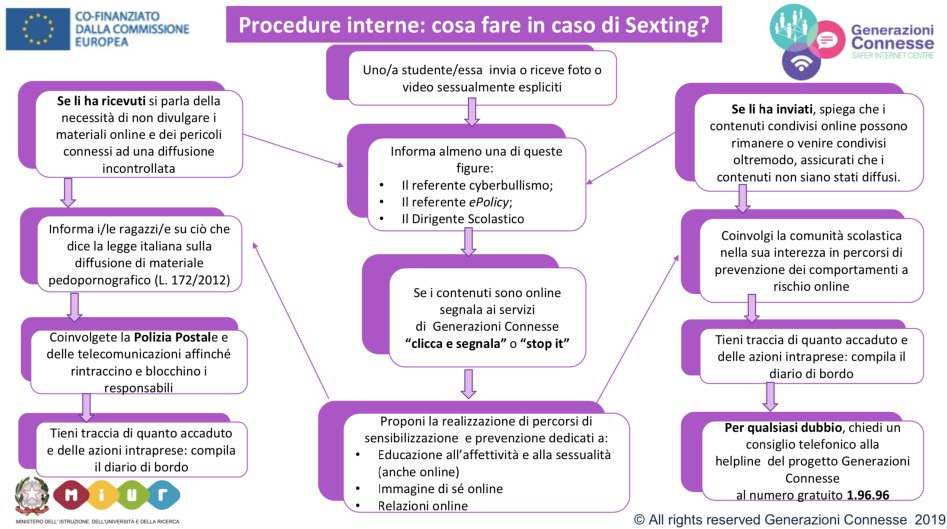
## ***5.4. - Allegati con le procedure***

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

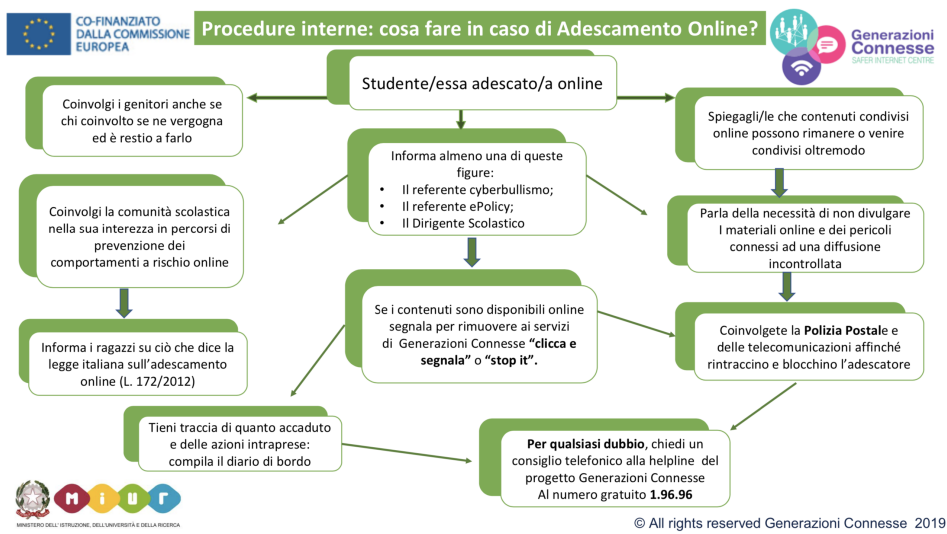


## Procedure interne: cosa fare in caso di sexting?

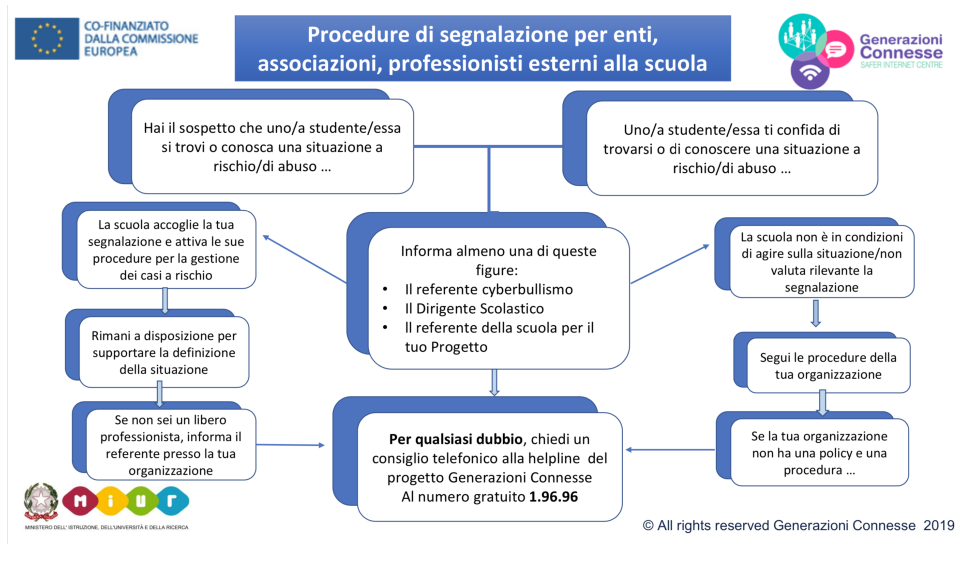




## Procedure interne: cosa fare in caso di adescamento online?



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



## Altri allegati

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

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

Vista le delicatezza dei temi in questione e data l'età degli alunni coinvolti, l'Istituto ritiene necessario applicare le procedure coinvolgendo le famiglie degli ragazzi.

