



# Documento di ePolicy

VVIC82600R

I.C. "AMERIGO VESPUCCI"

VIA STAZIONE - VIBO MARINA - 89900 - VIBO VALENTIA - VIBO VALENTIA (VV)

GIUSEPPE SANGENITI

# 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.

L' ePolicy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali.

In data 30 Settembre 2023, al termine del percorso e-learning di Generazioni Connesse, l'I.C "A.Vespucci" si è dotato di una e-Safety Policy interna, documento programmatico, autoprodotta dalla scuola, volto a promuovere le competenze digitali ed un uso delle tecnologie digitali positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo.

Il regolamento di sicurezza descrive:

- l'approccio della scuola alle tematiche legate alle competenze digitali, alla sicurezza online e ad un uso positivo delle tecnologie digitali nella didattica;
- le norme comportamentali e le procedure per l'utilizzo delle Tecnologie dell'informazione e della comunicazione (TIC) in ambiente scolastico;
- le misure per la prevenzione;
- le misure per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

In una società online, le competenze digitali a scuola, costituiscono una forma di alfabetizzazione primaria, come leggere, scrivere e far di conto. Internet e le tecnologie digitali fanno parte ormai della vita quotidiana, non solo scolastica, degli studenti e delle studentesse.

Nella prospettiva dell'educazione alla cittadinanza attiva e responsabile e dell'inclusione sociale nell'era della società dell'informazione in cui le tecnologie informatiche e dei media assumono un ruolo fondamentale nello sviluppo dell'attività dell'uomo, è importante far acquisire agli stessi competenze di alfabetizzazione su informazioni e dati e competenze di comunicazione e collaborazione, in totale sicurezza formando cittadini capaci di individuare bisogni e risolvere problemi attraverso l'utilizzo creativo delle tecnologie digitali.

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, come ribadito dalla nuova Raccomandazione del Consiglio Europeo del 22 maggio 2018 relativa alle competenze chiave per l'apprendimento permanente. Recentemente, la comunità europea ha messo a disposizione di ogni cittadino framework efficaci come il Digcomp 2.2, il Lifecomp e l'Entrecomp al fine di educare persone che siano padrone il più possibile di sé stesse,

delle proprie azioni anche nel digitale e che siano capaci di relazioni efficaci e costruttive.

In un contesto sempre più complesso, i/le ragazzi/e sono esposti a occasioni di interazione con Internet attraverso una gamma via via più ricca di dispositivi facilmente alla loro portata. L'accesso a Internet, soprattutto per i bambini e gli adolescenti, rappresenta da una parte un'opportunità di accrescimento del sapere, di incremento delle capacità comunicative, di sviluppo delle competenze e di miglioramento delle prospettive di lavoro, ma dall'altra può esporre a situazioni di vulnerabilità che richiedono interventi specifici.

Occorre pertanto, che i ragazzi siano educati, sin dai primi approcci, ad un uso critico, sicuro e consapevole della rete e dei dispositivi digitali e che alla base del loro utilizzo ci sia una politica di utilizzo condivisa tra tutti gli utenti.

A tal proposito, l'IC "A. Vespucci" di Vibo Valentia Marina con il presente documento descrive sia per gli alunni e le alunne e sia per gli adulti coinvolti nel processo educativo, le norme comportamentali e le procedure per l'utilizzo delle ICT (Tecnologie dell'Informazione e della Comunicazione) per un uso consapevole delle nuove tecnologie oltre che sviluppare le competenze digitali e prevenire i rischi della "vita online".

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 che trovano un irrinunciabile fattore di consolidamento nell'implementazione del progetto "Generazioni Connesse", si definiscono le misure che la nostra istituzione scolastica intende adottare con le seguenti finalità:

- promuovere l'educazione all'uso consapevole della rete internet e l'educazione ai diritti e ai doveri legati all'utilizzo delle tecnologie informatiche
- prevenire fenomeni legati ai rischi delle tecnologie digitali;
- segnalare i casi individuati all'interno della scuola;
- gestire i casi, ovvero le misure che la scuola intende attivare a supporto delle famiglie e degli studenti che sono stati vittime o spettatori attivi e/o passivi di quanto avvenuto.

---

## ***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.

Fermo restando quanto statuito e riportato nel Regolamento d'Istituto, la presente e-Policy intende evidenziare quanto segue con lo scopo di indicare, per ogni componente scolastica, linee guida chiare e finalizzate ad un uso critico, sicuro e consapevole di Internet.

### **Il Dirigente Scolastico:**

- garantisce la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- individua attraverso il Collegio dei Docenti un referente del bullismo e cyberbullismo;
- garantisce ai propri docenti una formazione di base sulle Tecnologie dell'Informazione e della Comunicazione (ICT) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;
- promuove azioni di sensibilizzazione sui fenomeni del cyberbullismo in rete con enti, associazioni, istituzioni locali ed altre scuole, coinvolgendo alunni, docenti, genitori ed esperti;
- garantisce l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on line;
- informa tempestivamente, qualora venga a conoscenza di atti di cyberbullismo che non si configurino come reato, i genitori dei minori coinvolti (o chi ne esercita la responsabilità genitoriale o i tutori);
- regola il comportamento degli studenti ed impone sanzioni disciplinari in caso di comportamento inadeguato.

### **L' animatore digitale:**

- favorisce la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornisce consulenza e informazioni al personale in relazione ai rischi on line e alle misure di prevenzione e gestione degli stessi;
- rileva le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola;
- assicura che gli utenti possano accedere alla rete della scuola solo tramite password;
- cura la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);
- coinvolge la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti alla "scuola digitale";
- assicura la massima diffusione della e-policy dentro la comunità scolastica e in tutte le sue componenti (docenti/ata, genitori e studenti), mediante pubblicazione sul sito della scuola.

**Il referente del "bullismo e cyberbullismo":**

- promuove la conoscenza e la consapevolezza dei rischi connessi al bullismo e al cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale;
- coordina le attività di prevenzione ed informazione sulle sanzioni previste e sulle responsabilità di natura civile e penale, anche con eventuale affiancamento di genitori e studenti;
- si rivolge a partner esterni alla scuola, quali servizi sociali e sanitari, aziende del privato sociale, forze di polizia, per realizzare un progetto di prevenzione;
- cura rapporti di rete fra scuole per eventuali convegni/seminari/ corsi e l'organizzazione della giornata mondiale sulla Sicurezza in Internet, la "Safer Internet Day".
- Commissione bullismo e cyberbullismo:
- cura la redazione e la revisione annuale della policy sulla base delle osservazioni ricevute da tutti i soggetti interessati;
- all'interno della scuola, in riferimento ai diversi ordini scolastici e alle diverse collocazioni territoriali dei plessi, garantisce la comunicazione (sportello, circolari, sito web, ecc.) e il funzionamento di ogni mezzo e attività connessa all'uso corretto della TIC;
- coordina, nei diversi plessi, le attività relative alla prevenzione del fenomeno del bullismo e del cyberbullismo;
- riferisce al Dirigente Scolastico situazioni o problemi di particolare rilevanza su cui intervenire;
- si adopera per allargare quanto più possibile una "rete" che coinvolga al suo interno le diverse componenti scolastiche.
- 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;

**Personale ATA:**

- segnala qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'animatore digitale per le opportune indagini / azioni / sanzioni;
- mantiene tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e le realizza esclusivamente con sistemi ufficiali scolastici.

**Il collegio docenti:**

- promuove scelte didattiche ed educative, anche in collaborazione con altre scuole in rete, per la prevenzione del fenomeno del cyberbullismo e per la diffusione di pratiche corrette nell' uso di internet.

### **I docenti:**

- intraprendono azioni congruenti con l'utenza del proprio ordine di scuola, tenuto conto che l'istruzione ha un ruolo fondamentale sia nell'acquisizione e rispetto delle norme relative alla convivenza civile, sia nella trasmissione dei valori legati ad un uso responsabile di internet;
- valorizzano nell'attività didattica modalità di lavoro di tipo cooperativo e spazi di riflessioni adeguati al livello di età degli alunni, all'interno dei quali:
- illustrano ai propri alunni le regole di utilizzo contenute nel presente documento;
- forniscono chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti ecc);
- si assumono la responsabilità di segnalare prontamente eventuali malfunzionamenti o danneggiamenti al tecnico informatico;
- propongono agli alunni attività di ricerca di informazioni in rete, fornendo loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento.
- non si allontanano dalla postazione, lasciandola incustodita, se non prima di avere effettuato la disconnessione;
- non salvano sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili.
- segnalano al Dirigente Scolastico qualunque problematica, violazione o abuso, anche on line, che vede coinvolti alunni e alunne.

### **Gli alunni:**

- Sono coinvolti nella progettazione e nella realizzazione delle iniziative scolastiche, al fine di favorire un miglioramento del clima relazionale; in particolare, dopo opportuna formazione, possono operare come tutor per altri studenti;
- Imparano le regole basilari per rispettare gli altri quando sono connessi alla rete, facendo attenzione alle comunicazioni (email, sms, mms) che inviano;
- Durante le attività didattiche o comunque all'interno della scuola, possono acquisire, mediante telefonini cellulari o altri dispositivi elettronici (per gli alunni della scuola secondaria di primo grado) immagini, filmati o registrazioni



vocali, solo per finalità didattiche, previo consenso del docente. La divulgazione del materiale acquisito all'interno dell'istituto è utilizzabile solo per fini esclusivamente personali di studio o documentazione e comunque nel rispetto del diritto alla riservatezza di tutti;

- Durante le lezioni o le attività didattiche in genere non possono usare cellulari, giochi elettronici e riproduttori di musica, se non per finalità didattiche, previo consenso del docente;
- In caso di riscontro di malfunzionamenti della strumentazione e/o di contatto accidentale con informazioni, immagini e/o applicazioni inappropriate lo comunicano immediatamente all'insegnante;

### **I genitori:**

- partecipano alle azioni di formazione/informazione istituite dalla scuola, relativamente ai comportamenti sintomatici del bullismo e del cyberbullismo;
- contribuiscono, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- 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;
- rispondono per gli episodi commessi dai figli minori a titolo di colpa in educando
- (articolo 2048 del Codice civile);
- conoscono le azioni messe in campo dalla scuola e collaborano secondo le modalità previste dal Patto di corresponsabilità;
- conoscono il codice di comportamento dello studente;
- conoscono le sanzioni previste da regolamento d'istituto nei casi di bullismo, cyberbullismo e navigazione on line a rischio.

---

## ***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).

Tutti gli enti educativi esterni e le varie associazioni presenti sul territorio che entrano in relazione con il nostro Istituto si conformano alla politica riguardo all'uso consapevole e responsabile della Rete e delle TIC che la scuola ha condiviso. Essi promuovono comportamenti sicuri e assicurano la protezione degli alunni durante le attività che si svolgono insieme, segnalando ai docenti preposti e al Dirigente Scolastico eventuali comportamenti problematici o casi di abuso nell'uso della rete e delle TIC.

L'Istituto si riserva di richiedere ai soggetti esterni il casellario giudiziario come fattore ulteriore di protezione nei confronti dei minori (Condanne per alcuni reati previsti dal Codice penale e nello specifico gli articoli 600-bis (prostituzione minorile), 600-ter (pornografia minorile), 600-quater (detenzione di materiale pornografico), 600-quinquies (iniziative turistiche volte allo sfruttamento della prostituzione minorile), 609-undecies (adescamento di minorenni), o l'irrogazione di sanzioni interdittive all'esercizio di attività che comportino contatti diretti e regolari con i minori).

---

## ***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.

Al fine di condividere e comunicare al meglio il documento di ePolicy a tutta la comunità scolastica, sono previste le seguenti azioni, da ripetersi con cadenza annuale:

- presentazione e discussione del documento e di altro materiale informativo, inerente la linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet, nelle adunanze degli organi collegiali e durante uno specifico incontro di aggiornamento interno;
- presentazione del documento al personale A.T.A. durante uno specifico incontro di aggiornamento interno;
- presentazione del documento ai rappresentanti dei genitori e ai rappresentanti degli studenti
- durante incontri appositamente organizzati ad inizio anno scolastico;
- presentazione del documento a tutte le classi, ad inizio anno scolastico, e inserimento dei contenuti dello stesso nella programmazione didattica, nell'ambito dell'educazione alla cittadinanza digitale;
- organizzazione di momenti di formazione rivolti alle famiglie sulla conoscenza del documento di ePolicy e sull'approfondimento dell'uso corretto delle TIC, anche in presenza di esponenti delle Forze dell'ordine o della Polizia postale.

---

## ***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.

A seconda dell'età dell'alunno o dell'alunna, sarà importante intervenire su tutto il contesto classe con attività specifiche educative di sensibilizzazione, allo scopo di

promuovere una maggior consapevolezza circa l'utilizzo delle TIC e di internet. Per eventuali provvedimenti "disciplinari", che saranno comunque proporzionati all'età e alla gravità del comportamento, si farà riferimento al Regolamento d'Istituto. Saranno previsti interventi di carattere educativo finalizzati alla ri-definizione delle regole sociali di convivenza e alla gestione delle problematiche emerse anche con l'eventuale intervento di enti esterni.

#### Infrazioni degli alunni

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola utilizzando

le TIC e la rete internet, messe a loro disposizione per fini puramente didattici, sono prevedibilmente le seguenti:

- uso improprio della rete per giudicare, infastidire o impedire a qualcuno di esprimersi liberamente o partecipare al dialogo didattico-educativo;
- invio incauto e non autorizzato di foto o dati personali, quali l'indirizzo di casa o il telefono;
- condivisione di immagini non appropriate, violente, intime o troppo spinte; comunicazione incauta e senza permesso con sconosciuti o soggetti comunque estranei all'azione didattico-educativa;
- collegamento a siti web non indicati e, dunque, non autorizzati dai docenti durante le attività laboratoriali di qualsiasi genere.

I provvedimenti "disciplinari" da adottare da parte dei consigli di classe nei confronti degli alunni che abbiano commesso una o più infrazione al documento E-policy, secondo quanto sopra, saranno proporzionati all'età e alla gravità del comportamento e si sostanzieranno nei seguenti:

- richiamo verbale
- richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);
- richiamo scritto con annotazione sul Registro Elettronico;
- nota informativa ai genitori o tutori mediante registro elettronico;
- convocazione dei genitori o tutori da parte degli insegnanti;
- convocazione dei genitori o tutori da parte del Dirigente scolastico.

Le denunce di bullismo online saranno trattate in conformità alla legge.

Contestualmente sono previsti interventi educativi di rinforzo rispetto a comportamenti corretti e riparativi dei disagi causati, di ridefinizione delle regole sociali di convivenza, di prevenzione e gestione positiva dei conflitti, di pro-socialità, di conoscenza e gestione delle emozioni.

Possono essere presi in considerazione percorsi di formazione per tutta la classe, assegnazione di attività aggiuntive da svolgere a casa sui temi di Cittadinanza e Costituzione.

#### Infrazione del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico, in particolare idocenti, incorra nell'utilizzo delle tecnologie digitali e di internet sono prevedibilmente le seguenti:

- utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di docenza o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiale non idoneo;
- utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- trattamento dei dati personali e dei dati sensibili degli alunni non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi; diffusione delle password assegnate e incauta custodia degli strumenti e degli accessi di cui possono approfittare terzi;
- assente o carente istruzione preventiva degli alunni sull'uso corretto e responsabile delle TIC e di internet;
- vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili rischi connessi;
- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente Scolastico, all'Animatore digitale.

Il Dirigente scolastico può disporre il controllo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola;

- procedere alla cancellazione di materiali non adeguati o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali approfondimenti successivi.

Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio dei procedimenti che possono avere carattere organizzativo-gestionale, disciplinare, amministrativo, penale, a seconda del tipo e della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

#### Infrazioni dei genitori

In considerazione dell'età degli studenti e delle studentesse, anche talune condizioni e condotte dei genitori medesimi possono favorire o meno l'uso corretto e responsabile

delle TIC da parte degli allievi a scuola. Gli atteggiamenti da parte della famiglia meno favorevoli sono:

- l'idea che nell'uso del pc a casa il figlio sia al sicuro e che non corra alcun rischio;
- una posizione del computer in una stanza o in un posto non visibile a tutti e non controllabile dall'adulto;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'uso di cellulare o smartphone;
- un utilizzo di cellulari e smartphone in comune con gli adulti che possono conservare in memoria indirizzi di siti o contenuti non idonei a minori.

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionati a norma di legge in base alla gravità dei comportamenti dei loro figli.

#### Procedure operative per la gestione delle infrazioni alla E-Safety Policy

Infrazioni lievi	Sanzioni	Interventi educativi riparatori	Organo competente
Collegamento a siti web non indicati dai docenti	Richiamo verbale	Riflessione sul comportamento che l'alunno ha adottato e sulle motivazioni che l'hanno determinate	Insegnante di classe
Utilizzare la rete per interessi privati e personali che esulano dalla didattica	Nota sul diario/libretto personale dell'alunno	Richiesta di scuse verbali	
Scaricare file, video- musicali protetti da copyright	Annotazione sul registro di classe		
Infrazioni gravi	Sanzioni	Interventi educativi riparatori	Organo competente
	Comunicazione scritta alla famiglia	Riflessione sul comportamento che l'alunno ha adottato e sulle motivazioni che l'hanno determinato	Insegnante di classe
Deridere, denigrare, umiliare, calunniare attraverso l'uso delle TIC	Ammonimento del Dirigente (se reiterate)	Richiesta di scuse pubbliche	Responsabile cyberbullismo
	Convocazione dei genitori	Produzione obbligatoria di un elaborato (da svolgere a casa in collaborazione coi genitori) sui fatti accaduti e riflessioni sulle conseguenze delle proprie azioni	Dirigente Consiglio di classe

	Richiamo verbale	Riflessione sul comportamento che l'alunno ha adottato e sulle motivazioni che l'hanno determinato	
	Annotazione sul registro di classe		
Non rispettare le regole d'accesso alle strumentazioni	Comunicazione scritta alla famiglia	Assegnazione di un lavoro in classe durante i momenti di riposo o a casa	
Non rispettare le regole d'accesso ad internet	Sequestro temporaneo della strumentazione utilizzata in modo scorretto e restituzione all'alunno al termine della giornata scolastica	Assegnazione di un compito di rinforzo, da eseguirsi a casa, inerente l'attività svolta in classe al momento della mancanza disciplinare	Insegnante di classe Animatore digitale Dirigente Scolastico Consiglio di classe Consiglio Istituto
Uso scorretto della strumentazione personale	Sequestro temporaneo della strumentazione utilizzata in modo scorretto e restituzione al genitore al termine della giornata scolastica	Studio delle regole di sicurezza non rispettate	
	Convocazione dei genitori	Studio e ricerca di danni conseguenti a episodi di violazione delle regole e presentazione relazione in classe	
	Sospensione dalle lezioni	Svolgimento di mansioni utili alla comunità scolastica	

Infrazioni gravissime

Sanzioni

Interventi educativi riparatori

Organo competente

Isolare o emarginare attraverso l'uso delle TIC

Non rispettare i diritti altrui in ambito di cittadinanza digitale

Minacciare attraverso l'uso delle TIC

Attuare cyberstalking o altre forme di persecuzione e molestia attraverso l'uso delle TIC

Publicare sui social network o inviare tramite messaggistica immagini, video o testi che:

- siano offensivi della dignità personale violando le norme della Privacy
- non siano rispettosi dei valori di uguaglianza e di pari opportunità
- siano discriminanti (a sfondo etnico, religioso, sessuale...)
- incoraggino, atteggiamenti di maschilismo o stereotipi di genere

Annotazione sul registro di classe

Ammonimento del Dirigente

Convocazione immediata dei genitori

Sospensione dalle lezioni

Segnalazione agli assistenti sociali (se reiterate)

Segnalazione alle autorità competenti in caso di reati

Riflessione sul comportamento che l'alunno ha adottato e sulle motivazioni che l'hanno determinate

Produzione obbligatoria di un elaborato (da svolgere a casa in collaborazione coi genitori) sui fatti accaduti e riflessioni sulle conseguenze delle proprie azioni

Conversione della sospensione dalle lezioni con attività socialmente utili favorendo un reale e concreto confronto con i valori della solidarietà e l'assunzione di stili di comportamento positivo, che sviluppino la formazione di una coscienza responsabile e la crescita consapevole dei giovani

Insegnante di classe

Responsabile cyberbullismo

Dirigente Scolastico  
Consiglio di classe  
Consiglio Istituto  
Assistenti sociali  
Forze dell'ordine

---

## 1.6 - Integrazione dell'ePolicy con



## ***Regolamenti esistenti***

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

Il presente documento va ad integrare le norme già vigenti nell'Istituto e costituisce modello di riferimento per ulteriori regolamenti futuri. Si integra pienamente con obiettivi e contenuti dei seguenti documenti:

- PTOF
- Regolamento interno di Istituto
- Patto di Corresponsabilità

---

## ***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.

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

monitora l'implementazione della eSafety attraverso le seguenti azioni:

- presentazione ufficiale della e-Safety nei Consigli di classe/interclasse/intersezione;
- presentazione ai genitori degli alunni che iniziano per la prima volta il percorso scolastico;
- questionario finale per genitori, docenti e alunni sull'applicazione delle norme della e-Safety;
- rilevazione del numero dei casi di infrazione per anno scolastico (Diario di Bordo).

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

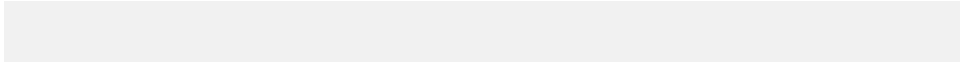
### **Azioni da svolgere entro un'annualità scolastica:**

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

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

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



# Capitolo 2 - Formazione e curriculum

---

## ***2.1. Curriculum sulle competenze digitali per gli studenti***

I ragazzi usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali".

Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico" (["Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente"](#), C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curriculum digitale.

La scuola, per implementare le competenze digitali degli studenti, ha adottato la piattaforma Google e Argo fornendo le credenziali di accesso e le procedure per attivare e utilizzare gli account personali.

Tenendo conto del Piano Scuola Digitale (PNSD), in particolar modo il paragrafo 4.2. su "Competenze e contenuti", il Sillabo sull'Educazione Civica Digitale, il DigComp 2.1 e la Raccomandazione del Consiglio Europeo relativa alle competenze chiave per l'apprendimento permanente (C189/9, p. 9), l'Istituto Comprensivo di Calvisano individua quattro aree di competenza da sviluppare e che sono incluse nel curriculum dello studente:

-Area 1: "Alfabetizzazione e dati";

-Area 2: "Comunicazione e collaborazione";

-Area 3: "Creazione di contenuti digitali"

-Area 4: "Sicurezza".

Descrittori, livelli di padronanza e modalità valutative verranno specificati nel Curricolo d'Istituto.

---

## ***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.

La competenza digitale, oggi, è imprescindibile per i docenti così come per studenti e studentesse e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa e in grado di venire incontro ai nuovi stili di apprendimento. Pertanto l'Istituto riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola (ad es. con l'aiuto dell'Animatore digitale), dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti (anche online) sulle TIC e si impegna a organizzare ogni anno momenti di formazione sui metodi e sugli strumenti della didattica digitale

---

## ***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.

Sarà predisposta un'area apposita nel sito della scuola dove il personale scolastico e le famiglie potranno trovare materiali informativi sulla sicurezza in Internet per l'approfondimento personale.

Anche il percorso relativo alla formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet può prevedere momenti di autoaggiornamento e momenti di formazione personale e collettiva.

Inoltre negli ultimi anni, un nutrito numero di docenti ha partecipato alla formazione sul tema dell'uso consapevole delle tecnologie e sulla conoscenza e prevenzione dei rischi attraverso gli interventi della Polizia Postale.

---

## ***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.

Le occasioni di informazione/formazione condotte dalla Polizia Postale sono state rivolte anche ai genitori, che hanno avuto l'opportunità di confrontarsi con gli esperti e i docenti sulle misure di prevenzione primaria al (cyber)bullismo e sulle strategie più opportune da adottare per un utilizzo consapevole e sicuro di Internet e delle TIC,

anche al di fuori della scuola.

Sarà necessario proporre ulteriori iniziative di sensibilizzazione che possano portare a una piena condivisione delle linee guida della ePolicy della scuola da parte della componente genitori anche al fine di implementarla.

La scuola si impegna a mettere in atto azioni continue di consulenza, orientamento e formazione per i genitori, tra cui:

- presentare ai genitori la E- Policy della scuola, al fine di far conoscere e divulgare i principi di comportamento sicuro on-line;
- informare l'utenza con e-mail, assemblee di classe, formazione specifica e pubblicazioni sul sito della scuola;
- organizzare incontri di consulenza con esperti;
- fornire informazioni sui siti nazionali di supporto per i genitori (es. il sito [www.generazioniconnesse.it](http://www.generazioniconnesse.it)).

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

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

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo 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)**

- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla

cittadinanza digitale



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

---

## 3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

Ogni giorno a scuola vengono trattati numerosi dati personali degli studenti e delle 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) .

In fase di iscrizione degli alunni alla scuola, i genitori sottoscrivono un'informativa sul trattamento dei dati personali in ottemperanza all'art. 13 D.Lgs 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali). All'inizio di ogni anno scolastico ai genitori è richiesta una "liberatoria immagini di minori" per una eventuale pubblicazione in rete o su piattaforme ministeriali. Le immagini, in questi casi, sono raccolte esclusivamente per scopi didattici. L'accesso ai dati riportati nel registro elettronico (ritardi, assenze, note e valutazioni) è riservato ai genitori dell'Istituto, tramite l'invio di una password di accesso strettamente personale.

---

## **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 diritto di accesso a Internet è 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.

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;
- 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.

---

## ***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.

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.

Registro elettronico

Argo Scuola è un software che permette di interagire in tempo reale con tutti i dati che la scuola vuole rendere disponibili ai destinatari (segreteria, docenti, famiglie).

La sicurezza e la privacy, nonché le prerogative di accesso, sono controllati da Scuola Next mediante chiavi d'accesso individuali, generate da un'apposita procedura interna e comunicati ai destinatari a mezzo posta elettronica o cartacea, in presenza. Il "modulo famiglia", completo di attivazione di tutti i nodi disponibili, permette di verificare in tempo reale alcuni dati sulla carriera scolastica del rispettivo figlio o della rispettiva figlia, tra cui: dati anagrafici; consultazione curriculum scolastico e situazione pagamento tasse. La consultazione del registro, inoltre, permette di

osservare le assenze/ritardi/permessi e giustificazioni per mese, per giorno e per materia con possibilità di giustificare direttamente. I "servizi classe" permettono di verificare ulteriori nodi: compiti assegnati nel registro di classe da parte del docente; l'indicazione dell'argomento trattato; promemoria di classe; consultazioni delle valutazioni ed altre funzionalità specifiche, se debitamente attivate. L'utilizzo del software è riservato esclusivamente ai fini didattici, nel rispetto di quanto indicato dal Software di gestione e sulla base di quanto stabilito dalla normativa vigente.

#### Sito web

Il sito Web dell'istituto è raggiungibile all'indirizzo [www.icsamerigovespuccivibovalentia.edu.it](http://www.icsamerigovespuccivibovalentia.edu.it).

Il sito web è gestito attraverso il pannello amministratore.

Nell'area riservata del sito sono caricate le comunicazioni, a cui è possibile accedere.

#### E-mail

Ogni docente possiede un account personale.

---

## **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.

Gli studenti non possono utilizzare i propri dispositivi durante le attività didattiche

come previsto dal regolamento disciplinare, né possono accedere alla Rete attraverso i dispositivi della scuola se non dietro previa autorizzazione dell'insegnante presente in aula e comunque solo per ricerche attinenti le attività didattiche.

I docenti possono utilizzare i dispositivi della scuola per realizzare tutte le attività connesse alla funzione docente.

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

---

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

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse.
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti.
- 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.
- Organizzare incontri per la consultazione degli studenti/studentesse, delle famiglie e del personale scolastico su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola.

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

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

Due interventi basilari da adottare per poter ridurre l'incidenza di situazioni di rischio consistono nella sensibilizzazione, tramite tutte azioni che hanno come obiettivo la promozione di un cambiamento e la prevenzione, grazie ad un insieme di attività attuate per promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale, in modo particolare per gli studenti ma coinvolgendo anche

tutti gli educatori adulti.

I rischi che possono avvenire, sia in ambiente scolastico che in quello familiare, derivano da un uso scorretto dei telefoni cellulari, smartphone, tablet e computer scolastici e personali.

Il nostro Istituto intende organizzare un ciclo di corsi di formazione rivolti a docenti, personale scolastico, genitori e studenti con esperti interni ed esterni per far conoscere i rischi e i pericoli di comportamenti e atteggiamenti non corretti sia nella Rete che nella quotidianità.

Gli interventi dovrebbero fornire non solo le informazioni necessarie, ma anche illustrare le possibili soluzioni e i comportamenti da adottare.

Gli alunni saranno coinvolti in incontri formativi con la Polizia di Stato, la Polizia Postale e Associazioni Educative .

---

## ***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).

Nel nostro Istituto è stata individuata, da circa due anni, un Referente che ha seguito il corso specifico on line sulla Piattaforma CFI svoltosi durante l'a.s. 2022/2023. In seguito sono stati organizzati incontri di sensibilizzazione e prevenzione con l'esperto di P.S., rivolti a docenti, alunni e genitori.

Le molestie che sono attuate attraverso strumenti tecnologici possono essere di vario tipo:

- litigare nei forum di discussione, con l'uso di un linguaggio violento e volgare; molestare attraverso l'invio ripetuto di messaggi offensivi;
- inviare ripetutamente messaggi che includono esplicite minacce fisiche;
- sparlare di qualcuno per danneggiare gratuitamente e con cattiveria la sua reputazione;
- registrare confidenze per poi inserirle integralmente in un blog pubblico;
- convincere, attraverso l'inganno, a rivelare informazioni imbarazzanti e riservate per renderle poi pubbliche in rete;
- insinuarsi all'interno dell'account di un'altra persona;
- estromettere intenzionalmente una persona da un gruppo online;
- riprendere, con il cellulare, macchina fotografica o videocamera, scene violente al fine di mostrarle ad amici o di diffonderle sulla Rete;
- pubblicare informazioni private e/o imbarazzanti su un'altra persona;
- inviare messaggi via smartphone ed Internet, corredati da immagini a sfondo sessuale.

Compito della comunità educante è vigilare sugli studenti, identificare vittime e prepotenti in divenire e intervenire sul gruppo classe con la collaborazione dei genitori. È infatti importante analizzare le relazioni sociali e l'ambiente in cui un fenomeno di cyberbullismo si verifica, per attuare un intervento mirato con la collaborazione del team docenti della classe. A ciò si aggiungono interventi mirati per le vittime, i bulli e i loro genitori.

## **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 si basa principalmente su pregiudizi e false notizie diffuse, oltre che sui social network, anche attraverso le diverse forme di comunicazione telematica ed è pratica che coinvolge tutte le fasce d'età. È fondamentale evitare che gli autori di tali episodi restino impuniti e che i messaggi si diffondano nella Rete velocemente e ampiamente.

Il nostro Istituto intende affrontare questo fenomeno sempre più diffuso a livello educativo e scolastico con tre obiettivi principali:

- favorire l'educazione interculturale, fornendo 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 per evitare che i discorsi di incitamento all'odio possano tradursi in offese e umiliazioni nei confronti delle vittime.
-

## **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?*

Appare sempre più urgente una presa di posizione circa l'uso smodato di Internet ad ogni livello, forse non rilevandone la potenziale pericolosità.

Il nostro Istituto intende promuovere incontri ed attività che permettano di acquisire competenze nella gestione del sovraccarico informatico e delle relative distrazioni, come continue notifiche, messaggi e giochi online.

---

## **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.

L'adolescenza è un periodo delicato della vita in cui c'è molta confusione, abbinata ad un grande desiderio di essere accettati dal gruppo.

Non è così insolito che gli adolescenti facciano sexting perché in questo periodo della loro crescita cercano di avvicinarsi al mondo degli adulti compiendo piccole trasgressioni, senza rendersi conto che la Rete non permette di controllarne la diffusione.

---

## **4.6 - Adescamento online**

Il **grooming** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di **teen dating** (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

**In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies - l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).**

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

Il 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, come 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).

In Italia l'adescamento si configura come reato dal 2012 (art. 609 undecies sull'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

Di seguito vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

Succede sempre più frequentemente che un adulto prenda contatto con dei bambini e bambine nei forum o nelle chat su Internet e che li metta di fronte a domande o messaggi sessuali o addirittura a immagini pornografiche. A volte l'adulto induce i bambini a spogliarsi davanti alla webcam oppure a inviare una fotografia che li ritrae nudi tramite Internet o sul cellulare, per poi ricattarli e costringerli a non rivelare gli abusi. Spesso l'adulto finge di essere minorenne.

La denuncia all'autorità giudiziaria o agli organi di Polizia, da parte degli insegnanti o

del Dirigente Scolastico, costituisce il passo necessario per avviare un intervento di tutela a favore della vittima e attivare un procedimento penale nei confronti del presunto colpevole.

La presa in carico di situazioni di abuso sessuale, così delicate e complesse, richiede un approccio multidisciplinare, da parte di diverse figure professionali. I versanti su cui si articola l'intervento possono essere essenzialmente tre: medico, socio-psicologico e giudiziario.

Il compito della scuola, per tutti i reati descritti, non è comunque solo quello di "segnalare", ma più ampio ed importante, soprattutto nella prevenzione dell'abuso, nonché nella ripresa della piccola vittima, in quanto ha al suo interno fattori relazionali ed educativi che possono aiutare il bambino a riprendere una crescita serena.

A tal fine la scuola lavora insieme alle altre figure professionali e alle famiglie, scambiando informazioni e condividendo progetti e prassi operative, favorendo le occasioni di confronto e di dialogo.

---

## 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](#).**

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.

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 e legge n. 38 del 6 febbraio 2020 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.

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.

Per contrastare tutte queste forme di cyberbullismo, la nostra scuola intende:

- organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse;
- pianificare e realizzare progetti di peer-education sui temi della sicurezza online nella scuola;
- 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;
- organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.

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

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

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti
- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale

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

- 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



# Capitolo 5 - Segnalazione e gestione dei casi

---

## 5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

segnalare la presenza di materiale pedopornografico online.

La gestione dei casi rilevati verrà differenziata a seconda della loro gravità.

Si rinvia al "Protocollo intervento gestione emergenza bullismo e cyberbullismo".

Alcuni avvenimenti di lieve rilevanza (ad esempio silenziare il microfono del compagno durante una videolezione o estrometterlo dalla stessa) possono essere affrontati e risolti con la discussione collettiva in classe.

Altri casi di rilevanza maggiore (insulti occasionali in chat invio di immagini improprie) verranno segnalati al referente del cyberbullismo e poi al Dirigente Scolastico, il quale potrà affrontarli convocando genitori e alunni, alla presenza di tutti gli attori in campo, per riflettere insieme sull' accaduto e individuare strategie comuni d'intervento.

Nei casi più gravi e in ogni ipotesi di reato, occorre valutare tempestivamente con il Dirigente Scolastico come intervenire, convocando con urgenza i genitori. Tutte le segnalazioni dei docenti devono essere messe a verbale e protocollate.

Particolare attenzione verrà posta alla rilevazione di rischi connessi alla navigazione sul web, in modo particolare legati al cyberbullismo, all'adescamento online e al sexting.

Rientrano nel cyberbullismo:

- FLAMING: Litigi nei forum di discussione, con l'uso di un linguaggio violento e volgare;
- HARASSMENT: molestie attuate attraverso l'invio ripetuto di messaggi offensivi;
- CYBERSTALKING: invio ripetuto di messaggi che includono esplicite minacce fisiche;
- DENIGRAZIONE: parlare di qualcuno per danneggiare gratuitamente e con cattiveria la sua reputazione;
- OUTING ESTORTO: registrazione di confidenze per poi inserirle integralmente in un blog pubblico
- TRICKERY: spinta, attraverso l'inganno, a rivelare informazioni imbarazzanti e riservate per renderle poi pubbliche in rete; IMPERSONATION: insinuazione all'interno dell'account di un'altra persona;
- ESCLUSIONE: estromissione intenzionale di una persona da un gruppo online;
- HAPPY SLAPPING: ripresa, con il videotelefono, macchina fotografica o videocamera, di scene violente al fine di mostrarle ad amici o di diffonderle in Rete;
- EXPOSURE: pubblicare informazioni private e/o imbarazzanti su un'altra persona;
- SEXTING: invio di messaggi via smartphone ed Internet, corredati da immagini a sfondo sessuale.

Dovranno essere segnalati su apposita scheda(allegata al paragrafo 3):

- 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 etc.);
- 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 etc.);
- 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 etc.).

---

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

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

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

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

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

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

---

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

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni

strumenti di segnalazione ad hoc messi a loro disposizione:

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

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

Per quanto riguarda la gestione dei casi, come già detto, il nostro Istituto ha individuato un Referente per il bullismo e il cyberbullismo.

La segnalazione del caso dovrà quindi essere fatta dal singolo docente o dall'adulto a conoscenza del fatto, tramite modulo per la segnalazione casi, alla referente, la quale, insieme al Team per le emergenze, si occuperà di raccogliere tutte le informazioni possibili, anche attraverso colloqui di approfondimento con gli attori coinvolti e di segnalare l'accaduto al Dirigente. Sarà poi il Dirigente, insieme al Team, a valutare se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali o se il caso vada gestito all'interno della scuola con il coinvolgimento del Consiglio di Classe e delle famiglie degli alunni coinvolti. Si sceglierà uno o più interventi da attuare a cui seguirà una fase di monitoraggio.

Il nostro Istituto ha elaborato il seguente protocollo "Gestione emergenze".

Quando emerge un fatto di bullismo/cyberbullismo vanno considerati tutti gli attori in gioco: vittima/e, bullo/i, spettatori o maggioranza silenziosa, aiutanti/sostenitori, difensori del bullo o della vittima, gli adulti.

Il docente informato del caso di bullismo o cyberbullismo, dopo aver ricostruito fatti e responsabilità informa:

- il Dirigente Scolastico;
- Il Referente del cyberbullismo;
- Il Coordinatore di classe.

Il Dirigente convoca gli alunni coinvolti direttamente (bullo/i, vittima/e) e i genitori degli stessi.

Il Dirigente Scolastico, se lo ritiene opportuno, convoca un Consiglio di classe straordinario, per stabilire le misure degli interventi e le sanzioni disciplinari.

Il Dirigente, in accordo con il Consiglio di Classe, informa le famiglie degli alunni coinvolti e attiva:

- gli interventi individuali: misure di supporto per la vittima;
- e sanzioni disciplinari e percorsi rieducativi per il/i bullo/i;
- gli interventi sulla classe.

Colloquio del Dirigente con i genitori

Avviene in tempi separati (genitori della vittima, genitori del bullo con i rispettivi figli).

Viene eseguita la comunicazione del fatto e firma da parte dei genitori del modulo di segnalazione, da conservare nel registro dei verbali.

I genitori vanno informati delle loro responsabilità civili e legali, in quanto genitori di minori di 14 anni, dell'eventuale reato del figlio/a.

Vanno anche informati dell'obbligo della scuola di fare segnalazione alle autorità competenti se il fatto si configura come reato.

Viene inoltre fatta richiesta ai genitori di collaborazione e vigilanza nei mesi successivi, secondo le indicazioni del "Patto educativo di Corresponsabilità".

La sanzione disciplinare stabilita, di tipo anche riparativo, oltre eventuale sospensione, può essere comunicata anche nei giorni successivi.

Se lo si ritiene necessario, il Dirigente organizza un incontro tra i genitori degli alunni/e coinvolti/e, in modo da favorire il dialogo e rasserenare il clima.

Interventi sulla classe

Parallelamente agli interventi individuali è importante che si avvii nella classe un momento di riflessione e discussione, allo scopo di modificare le relazioni tra gli alunni. Il coordinatore di classe si informa prima con i singoli alunni coinvolti direttamente, poi con la classe intera, esplicitando il problema e discutendo con gli studenti su quello che è accaduto.

Alcune ore delle attività curriculari vengono "sospese" per dedicare delle ore ad attività specifiche su questo tema (es. PROGRAMMA "MABASTA" UN CALCIO AL BULLISMO). Se lo si ritiene opportuno verrà coinvolto un esperto esterno (psicologo) di supporto alle attività della classe.

Nel periodo successivo in classe si manterrà alta la vigilanza sulle relazioni tra gli alunni/e, favorendo un clima collaborativo tramite didattiche di Cooperative Learning, il reinserimento dei compagni ex vittime, svolgendo giochi di ruolo per rendere consapevoli i ragazzi/e delle conseguenze delle loro azioni. Verranno inoltre condivise con gli alunni le regole ristabilite.

Sanzioni disciplinari

I comportamenti accertati che si configurano come forme di bullismo e cyberbullismo sono considerati come infrazioni gravi e vengono sanzionati sulla base del regolamento disciplinare degli studenti. La sanzione disciplinare, commisurata all' intensità dell'episodio, deve prevedere anche una attività riparatoria ed educativa che sia visibile e vada a beneficio della vittima e/o della classe.

La classe a sua volta dovrà fare una sua azione riparatoria nei confronti della vittima. Le sanzioni saranno particolarmente incisive per fatti di estrema gravità, preferibilmente con l'attivazione di percorsi educativi di recupero mediante lo svolgimento di attività di natura sociale, culturale e in generale a vantaggio della comunità scolastica. Vengono considerati deprecabili e sanzionabili anche le condotte dei compagni sostenitori del bullo.

In caso di episodi gravi di cyberbullismo, il Dirigente informa i docenti e attiva le procedure previste dal protocollo e dal Regolamento di disciplina.

Attenuanti e aggravanti:

1. il riconoscimento dell'errore, il risarcimento del danno e le scuse personali costituiscono attenuanti per le quali si applica la riduzione della pena (sono esclusi i reati di violenza fisica, psicologica o l'intimidazione del gruppo, specie se reiterata e il reato di cyberstalking);
2. aver commesso un'infrazione disciplinare, in concorso con una o più persone, costituisce aggravante per la quale si applica l'aumento della sanzione;
3. è possibile convertire parte della sanzione nello svolgimento di attività educative, definite in accordo con le famiglie secondo un piano educativo condiviso.

Obbligo di denuncia

Devono essere denunciati dal Dirigente Scolastico alle autorità competenti (Carabinieri, Polizia, Polizia Postale) i seguenti reati perseguibili d'ufficio:

- rapina ed estorsione (art 628 c.p. e art 629 c.p.) riferibili ad episodi di minacce e violenze per ottenere (o sottrarre) oggetti o somme di denaro;
- lesioni gravissime (art 582 c.p. - 585 c.p.) e lesioni guaribili in più di 40 giorni o che comportano una diminuzione permanente della funzionalità di un organo;
- violenza sessuale (art 609 s.p.) commessa singolarmente o in gruppo; in questo caso viene considerata più grave e punita più severamente (per chiarire cosa si intende per violenza sessuale, bisogna considerare che ogni atto sessuale rientra in questa definizione, ad esempio: se un gruppo di minori blocca fisicamente una compagna palpeggiandola, rispondono tutti penalmente e non solo la persona che materialmente esegue l'atto);
- violenza o minaccia a pubblico ufficiale per alunni che hanno compiuto il quattordicesimo anno di età (art. 336 c.p. e art. 337 c. p.).

Gli episodi di bullismo perseguibili in caso di querela sono:

- lesioni, percosse, minacce, ingiurie, diffamazione, molestia, atti persecutori/Stalking (art. 582,581, 612, 591, 595 ,660,612 del codice penale) :

in questi casi è necessario informare la famiglia (e/o i Servizi Sociali) che può procedere alla querela, a sua discrezione. Il mancato avviso alla famiglia, da parte della Istituzione scolastica, è passibile di denuncia.

---

### **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.

Il nostro Istituto, nell'ottica di una fattiva e proficua collaborazione scuola-famiglia, in linea con il Patto di Corresponsabilità, invita ad effettuare la segnalazione al Dirigente dei casi avvenuti nell'ambito scolastico.

Qualora i casi si verificassero al di fuori di esso è possibile consultare gli indirizzi degli enti presenti sul territorio nazionale è possibile consultare il Vademecum di Generazioni Connesse, suddiviso per Regioni;

- HELPLINE la linea d'ascolto di Generazioni Connesse operativa 24 ore su 24 tel. 1.96.96

oppure [www.commissariatodips.it](http://www.commissariatodips.it); • Stazione Carabinieri competente per la scuola

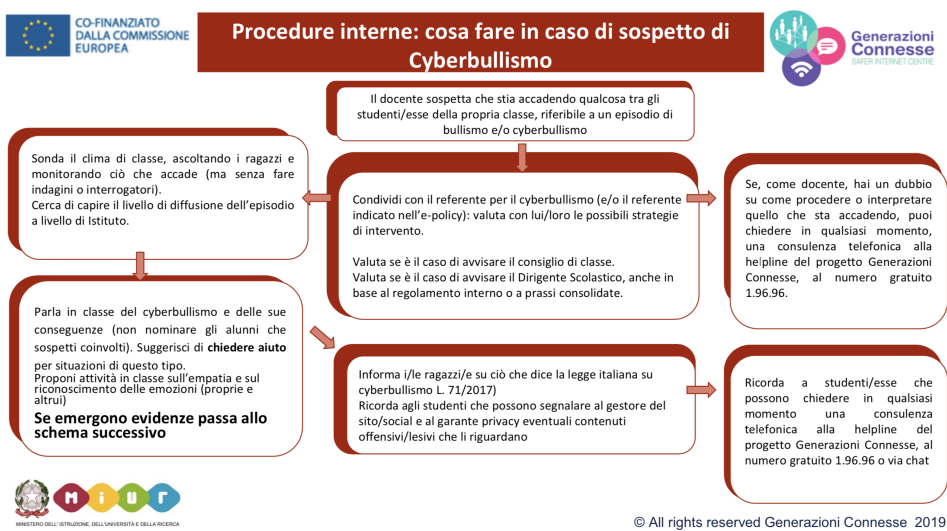
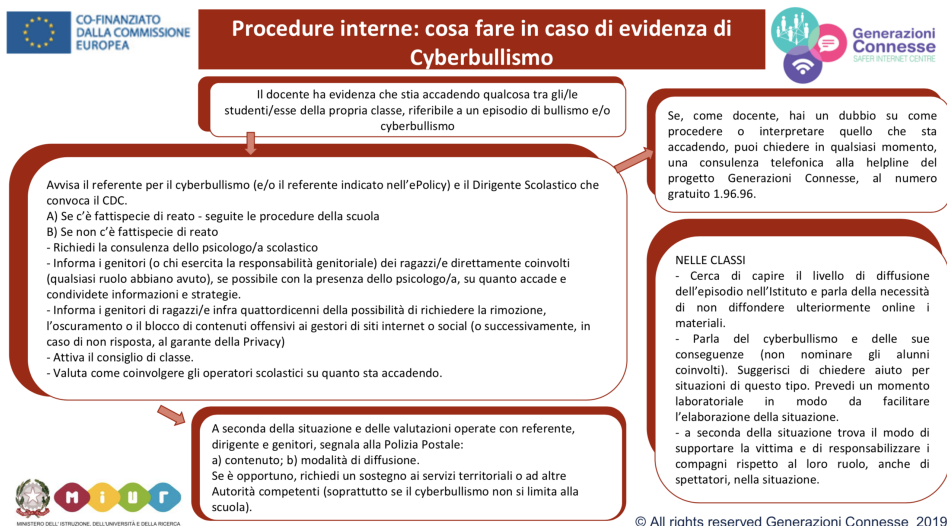
- Servizi messi a disposizione dal "Safer Internet Center" per segnalazione di contenuti illegali e dannosi:
- Telefono Azzurro: <http://www.azzurro.it/emergenza-0>;
- "Clicca e segnala" di Telefono Azzurro [www.azzurro.it/it/clicca-e-segnala](http://www.azzurro.it/it/clicca-e-segnala) Stop-it di Save the Children [www.stop-it](http://www.stop-it).

Queste strutture supportano la scuola in situazioni di emergenza, ma potrebbero essere coinvolte per poter svolgere momenti di formazione sul tema del Cyberbullismo.

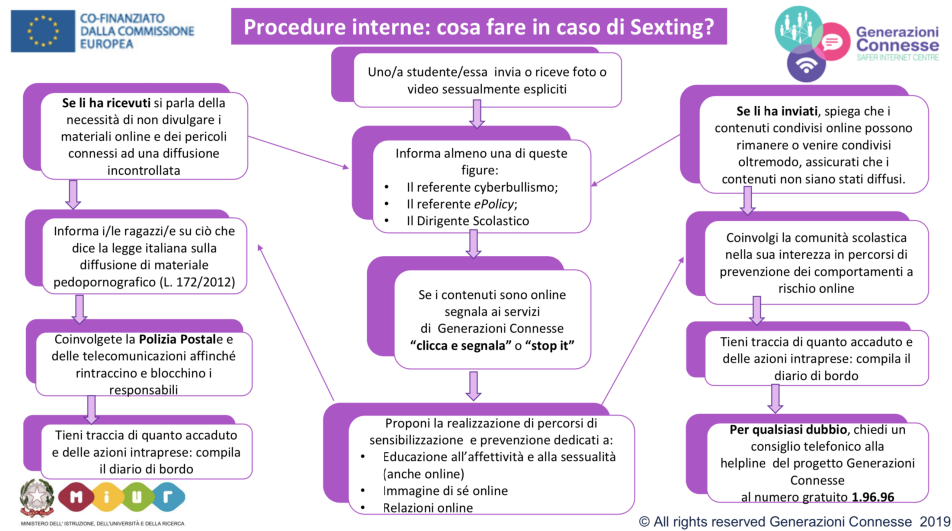
---

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

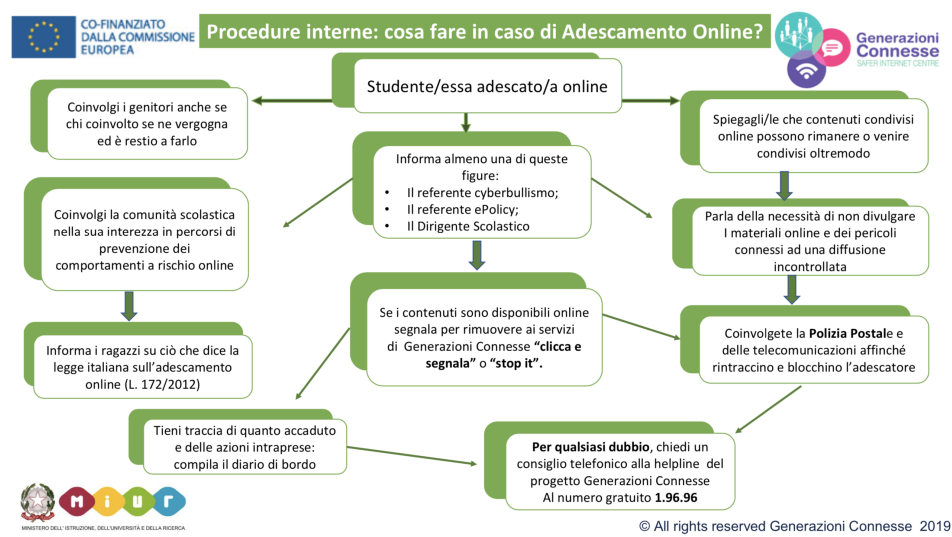
### **Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?**



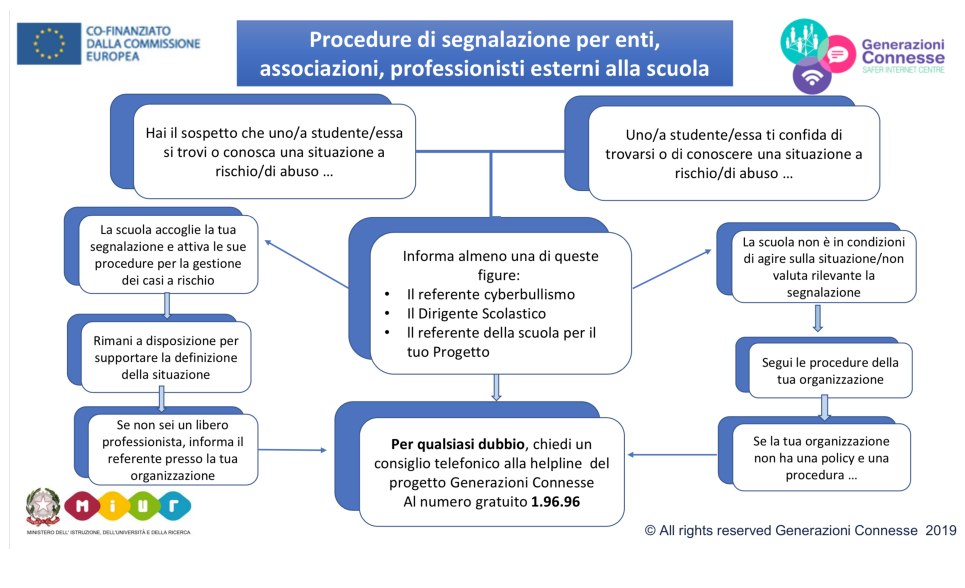
## Procedure interne: cosa fare in caso di sexting?



## 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](#)

Tenuto conto che nel nostro Istituto Comprensivo non si è mai verificato un caso di Bullismo e di Cyberbullismo, come completamento del presente documento si fa riferimento alle procedure da seguire secondo la E-Safety Policy e a cui il Regolamento di Istituto in materia di tali azioni si è redatto.

### ALLEGATO 1.

#### Procedure operative per la gestione delle infrazioni alla E-Safety Policy

Ogni volta che un membro del personale o studente viola la E-Safety Policy, la decisione finale sul livello di sanzioni sarà a discrezione del Dirigente Scolastico e rifletterà le procedure comportamentali e disciplinari della scuola. Di seguito sono fornite alcune procedure operative come esemplificazione:

#### STUDENTI:

#### INFRAZIONI POSSIBILI

- L'uso di siti non-educativi durante le lezioni.
- L'utilizzo non autorizzato di e-mail.
- L'uso non autorizzato del telefono cellulare (o di altre nuove tecnologie) durante le lezioni.

- Uso di instant messaging / Siti di social networking.
- L'uso continuato di siti non-educativi durante le lezioni dopo essere stato avvertito.
- L'uso non autorizzato di e-mail dopo essere stato avvertito.
- L'uso non autorizzato del telefono cellulare (o altre nuove tecnologie) dopo essere stato avvertito.
- L'uso continuato messaggistica / chat room istantanea, siti di social networking, newsgroup.
- L'uso di materiale offensivo.
- Rovinare o distruggere deliberatamente i dati di qualcuno, violare la privacy altrui o messaggi inappropriati, video o immagini su un sito di social networking.
- Invio di un messaggio e-mail o MSN che è considerato molestia o azione di bullismo.
- Cercare di accedere a materiale offensivo o pornografico.
- Invio di e-mail o messaggi di MSN considerati molestia o bullismo dopo essere stato avvertito.
- Accedere deliberatamente allo scaricamento o alla diffusione di qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofobico o violento.
- Trasmissione di materiale che viola i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati.

#### SANZIONI

Fare riferimento all'insegnante della classe/ ESafety Coordinator/Dirigente Scolastico  
Documento di e-policy

Fare riferimento all'insegnante della classe/ ESafety Coordinator/Dirigente Scolastico  
Escalation a:

1. rimozione dei diritti di accesso a Internet per un periodo;
2. rimozione del telefono fino a fine giornata;
3. contatto con i genitori.

Fare riferimento all'insegnante della classe/ ESafety Coordinator/Dirigente Scolastico  
Escalation a:

1. rimozione dei diritti di accesso a Internet per un periodo;
2. rimozione del telefono fino a fine giornata;
3. contatto con i genitori;
4. contattare le autorità competenti.

Fare riferimento all'insegnante della classe / contatto con i genitori Altre possibili azioni di salvaguardia:

1. conservare le prove;
2. informare i provider di servizi di posta elettronica del mittente;
3. fare rapporto alle autorità competenti dove si sospetti la pedofilia o altre attività illegali.

PERSONALE SCOLASTICO:

INFRAZIONI POSSIBILI

- L'uso di Internet per attività personali non legate allo sviluppo professionale (shopping online, email personali, instant messaging ecc).
- L'utilizzo di supporti di memorizzazione dei dati personali (ad esempio, chiavette USB) senza considerare l'accesso e l'adeguatezza di qualsiasi file memorizzato.
- Non implementare adeguate procedure di salvaguardia.
- Qualsiasi comportamento sul World Wide Web che compromette la professionalità del personale nella scuola e nella comunità.
- L'uso improprio di primo livello di sicurezza dei dati, ad esempio uso illecito di password.
- Violazione del copyright o della licenza per l'installazione di software.
- Gravi danni intenzionali all'hardware o software del computer.
- Qualsiasi tentativo deliberato di violare la protezione dei dati o di sicurezza informatica.
- Creare, accedere, scaricare e diffondere deliberatamente qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofobico o violento.
- Ricevere o trasmettere materiale che viola i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati.
- Portare il nome della scuola in discredito Fare riferimento all'E-Safety Coordinator/ DSGA / Dirigente Scolastico

SANZIONI

1. Avvertimento
2. rimuovere il PC in un luogo sicuro per garantire che non vi alcun ulteriore accesso al PC o laptop;

2. far verificare tutte le attrezzature per garantire che non vi sia alcun rischio di alunni che accedono a materiali inappropriati nella scuola.

Escalation a:

Contattare e fare rapporto alle autorità competenti

Laddove il docente colga possibili situazioni di disagio connesse ad uno o più di uno tra i rischi elencati, dovrà informare il Dirigente Scolastico anche attraverso la compilazione di una "scheda di segnalazione" (di seguito allegata e disponibile nell'area riservata del sito web istituzionale). La scheda di segnalazione potrà essere redatta dal docente sia sulla base di eventi osservati direttamente a scuola, sia su eventi particolari che gli sono stati confidati dall'alunno o comunicati da terzi.

## ALLEGATO 2

Prima segnalazione dei casi di (presunto) bullismo e vittimizzazione

Nome di chi compila la segnalazione:

Data: \_\_\_\_\_ Scuola: \_\_\_\_\_

La persona che ha segnalato il caso di presunto bullismo era

La vittima

Un compagno della vittima, nome \_\_\_\_\_

Madre/ Padre/Tutore della vittima, nome \_\_\_\_\_

Insegnante, nome \_\_\_\_\_

Altri: \_\_\_\_\_

2. Vittima \_\_\_\_\_ Classe \_\_\_\_\_

Altre vittime \_\_\_\_\_ Classe \_\_\_\_\_

Altre vittime \_\_\_\_\_ Classe \_\_\_\_\_

3. Bullo o i bulli (o presunti)

Nome \_\_\_\_\_ Classe \_\_\_\_\_

Nome \_\_\_\_\_ Classe \_\_\_\_\_

Nome \_\_\_\_\_ Classe \_\_\_\_\_

4. Descrizione breve del problema presentato. Dare esempi concreti degli episodi di prepotenza.

-----  
 \_\_\_\_\_

Quante volte sono successi gli episodi?

-----  
 -----  
 \_\_\_\_\_

ALLEGATO

3. PROCEDURA PER CASO DI PRESUNTO BULLISMO E VITTIMIZZAZIONE A SCUOLA

1. Prima segnalazione

2. Valutazione approfondita

3. Gestione del caso attraverso uno o più interventi:

- Approccio educativo con la classe Intervento individuale
- Gestione della relazione
- Coinvolgimento la famiglia
- Supporto intensivo a lungo termine e di rete

Il nostro Istituto possiede un Protocollo per la prevenzione e contrasto del bullismo e del cyberbullismo, pubblicato sul Sito e accoglie progetti ed eventi organizzati in merito, da parte dell'Ente Locale e del Comando dei Carabinieri.

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

### **IL NOSTRO PIANO DI AZIONI**

Sulla base delle "Linee guida per l'uso positivo delle tecnologie digitali e della prevenzione dei rischi nelle scuole", vengono assunti i seguenti punti per una collaborazione sinergica tra scuola-famiglia-servizi territoriali, al fine di creare un modello composito e lineare di azioni condivise:



- coinvolgimento di tutti gli attori della scuola: studenti e studentesse, docenti, genitori e personale ATA, per l'affermazione di un modello di scuola come comunità;
- alleanza educativa tra scuola e famiglia; interventi educativi ed azioni di supporto, quale prevenzione per eventuali comportamenti a rischio;
- misure preventive specifiche di tutela anche con l'ausilio di attori territoriali, come Polizia postale ed ATS per servizi specialistici;
- promozione dell'educazione al rispetto; sviluppo del pensiero critico;
- promozione dell'Educazione Civica Digitale.

