



# Documento di ePolicy

---

RMIC8AG009

I. C. KAROL WOJTYLA

VIA CONCESIO 2 - 00188 - ROMA - ROMA (RM)

GARRITANO LOREDANA

# Capitolo 1 - Introduzione al documento di ePolicy

---

## 1.1 - Scopo dell'ePolicy

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

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

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

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

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

## Argomenti del Documento

### 1. Presentazione dell'ePolicy

1. Scopo dell'ePolicy
2. Ruoli e responsabilità
3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

5. Gestione delle infrazioni alla ePolicy
6. Integrazione dell'ePolicy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

## **2. Formazione e curriculum**

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

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

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

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

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

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

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

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

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

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

Il nostro Istituto elabora il presente documento E-POLICY seguendo le indicazioni delle LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo, cyberbullismo e rischi legati

ad internet elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con Generazioni Connesse.

L'obiettivo è educare e sensibilizzare gli adolescenti, gli insegnanti e i genitori all'uso sicuro e consapevole di Internet. Il curriculum scolastico deve prevedere che gli studenti imparino utilizzando le TIC ( Tecnologie dell'informazione e della comunicazione) e la scuola deve proporre agli studenti e agli insegnanti di utilizzare internet al fine di promuovere l'apprendimento in ambito didattico attraverso la condivisione delle risorse, l'innovazione e la comunicazione.

Gli insegnanti hanno la responsabilità di guidare gli studenti nell'attività online, di stabilire contatti chiari per un uso responsabile di internet. Negli ultimi anni, la scuola ha cercato di dotarsi di strumenti tecnologici e di favorire la formazione del personale per far crescere le competenze professionali specifiche nell'impiego delle nuovetecnologie.

A tal fine, potrebbe essere formulato un regolamento per l'utilizzo e il corretto funzionamento delle aule e delle postazioni informatiche , tramite l'indicazione di pratiche opportune e l'invito ad un uso responsabile da parte di tutto il personale.

In particolare l'intento della scuola è quello di promuovere l'uso consapevole e critico da parte degli alunni delle tecnologie digitali e di internet, di far acquisire loro procedure e competenze "tecniche" ma anche corrette norme comportamentali, di prevenire ovvero rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali .

Gli utenti, soprattutto minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la Scuola propone di promuovere l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti.

Gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose.

---

## ***1.2 - Ruoli e responsabilità***

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

Dirigente scolastico

Il ruolo del Dirigente scolastico nel promuovere l'uso consentito delle tecnologie di internet include i seguenti compiti:

- garantire la sicurezza (tra cui la sicurezza on-line) dei membri della comunità scolastica;
- garantire che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC);
- garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- comprendere e seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.

#### Animatore digitale

Il ruolo dell'Animatore digitale include i seguenti compiti:

- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite password personali applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio)nella partecipazione ad attività e progetti attinenti la "scuola digitale".

#### Direttore dei servizi generali e amministrativi

Il ruolo del direttore dei servizi generali e amministrativi include i seguenti compiti:

- assicurare, 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;
- garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

#### Docenti

Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il sottomettere e di rispettare la normativa sul diritto d'autore;
- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, cellulari, da parte degli alunni durante le lezioni e ogni altra attività scolastica;
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni(ovvero valutazioni sulla condotta non adeguata degli stessi)rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all'Animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- segnalare al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.

#### Alunni

Il ruolo degli alunni include i seguenti compiti:

- essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il sottomettere e rispettare i diritti d'autore;

- comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

#### Genitori

- Il ruolo dei genitori degli alunni include i seguenti compiti:
    - Sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;
    - Seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet;
    - Concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet;
    - Fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e del telefonino in generale.
- 

### ***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).

Gli enti educativi esterni e le associazioni che entrano in relazione con la scuola devono conformarsi all'uso consapevole della rete e delle TIC, devono promuovere comportamenti sicuri, la sicurezza online assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme, in più l'istituto deve avere un regolamento da seguire, rispettando regole o norme comportamentali, per tutelare tutti e anche loro.

Devono avere una buona preparazione linguistica, molto scorrevole, essendo che si tratta di studenti minorenni, in più una buona conoscenza sull'informazione della privacy, un buon curriculum adeguato alla situazione e la conoscenza delle TIC riguardante i dispositivi di internet e le sue reti.

---

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

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

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

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

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

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

### **ALUNNI**

Tutti gli alunni saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione.

L'istruzione degli alunni riguardo all'uso responsabile e sicuro di internet precederà l'accesso alla rete;

L'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule o laboratori con accesso a internet;

Sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili”.

#### PERSONALE

La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà discussa negli organi collegiali e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web;

Per proteggere tutto il personale e gli alunni, la scuola metterà in atto una linea di condotta di utilizzo accettabile, controllato e limitato alle esigenze didattiche essenziali;

Il personale docente sarà reso consapevole del fatto che il traffico in internet può essere monitorato e si potrà risalire al singolo utente registrato;

Un'adeguata informazione/formazione on-line del personale docente nell'uso sicuro e responsabile di internet, sia professionalmente che personalmente, sarà fornita a tutto il personale, anche attraverso il sito web della scuola;

Il sistema di selezione adottato e il monitoraggio sull'utilizzo delle TIC sarà supervisionato dall'Animatore digitale, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici;

L'Animatore digitale metterà in evidenza on-line utili strumenti che il personale potrà usare con gli alunni in classe. Questi strumenti varieranno a seconda dell'età e della capacità degli alunni;

Tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

#### GENITORI

L'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà attirata nelle news o in altre aree del sito web della scuola;

Sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione degli incontri scuola-famiglia, assemblee, collegiali e individuali;

L'Animatore digitale fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di internet anche a casa;

L'Animatore digitale e i docenti di classe forniranno ai genitori indirizzi sul web relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni, sistemi di selezione e attività educative per il tempo libero.

---

## ***1.5 - Gestione delle infrazioni alla ePolicy***

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali di internet di cui si dispone per la didattica, in relazione alla fascia di età considerate, sono prevedibilmente le seguenti:

un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;

l'invio imprudente o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;

la condivisione di immagini intime o troppo spinte;

la comunicazione incauta e senza permesso con sconosciuti;

il collegamento a siti web non indicati dai docenti.

Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo dell'alunno. Infatti più gli alunni sono piccoli, più i comportamenti "da correggere" sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, che devono essere compresi e orientati proprio dagli educatori, nella prospettiva del raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno.

Sono previsti pertanto da parte dei docenti provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento, quali:

il richiamo verbale;

il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);

il richiamo scritto con annotazione sul diario;

la convocazione dei genitori da parte degli insegnanti;

la convocazione dei genitori da parte del Dirigente scolastico.

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

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono diverse e alcune possono determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli alunni:

un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;

un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;

un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;

una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;

una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile delle tecnologie digitali e di internet;

una vigilanza raggirata dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;

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 controllare l'utilizzo 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 inadeguati o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali successive investigazioni. 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 di procedimenti che possono avere carattere organizzativo gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

Disciplina dei genitori In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico.

Le situazioni familiari meno favorevoli sono:

la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai;

una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio;

una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone;

un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei;

un utilizzo del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei. I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli

altri.

---

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

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

1. Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.
2. I laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.
3. Quando un insegnante, da solo o in classe, usufruisce del laboratorio deve obbligatoriamente registrare il proprio nome e l'eventuale classe nell'apposito registro delle presenze di laboratorio, indicando l'orario di ingresso, quello di uscita e motivazione dell'uso delle postazioni informatiche.
4. L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.
5. Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.
6. Nei laboratori è vietato utilizzare CD personali o dischetti se non dopo opportuno controllo con sistema di antivirus aggiornato.
7. E' vietato cancellare o alterare file - dati presenti sull'hard disk.
8. Il laboratorio non deve mai essere lasciato aperto o incustodito quando nessuno lo utilizza. All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare l'aula in ordine, le macchine spente correttamente.
9. In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile del laboratorio.
10. In caso di malfunzionamento non risolvibile dal responsabile di laboratorio si contatterà personalmente o attraverso il Responsabile di laboratorio, la segreteria.
11. Per motivi di manutenzione straordinaria, in caso di guasti o di virus, i PC possono essere formattati senza preavviso. Si consiglia pertanto di salvare i dati importanti su Cd o pendrive periodicamente. In caso di formattazione ordinaria ci sarà un preavviso.

---

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

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

Il monitoraggio dell'implementazione della e-policy e del suo eventuale aggiornamento deve essere svolto ogni anno. Tale monitoraggio sarà curato dal Dirigente Scolastico con la collaborazione dell'Animatore digitale e dai docenti delle classi. Sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di internet. Il monitoraggio sarà rivolto anche agli insegnanti, al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti. L'aggiornamento della policy sarà curato dal Dirigente Scolastico, dall'Animatore digitale, dagli Organi Collegiali

---

### ***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 incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori 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 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

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

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori 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 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 competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell’informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Deve essere supportata da abilità di base nelle TIC: l’uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet. Il Curriculum della scuola d’istruzione sulle competenze digitali per gli alunni è trasversale alle discipline previste dalle Indicazioni Nazionali: la competenza digitale è ritenuta dall’Unione Europea competenza chiave, per la sua importanza e capacità di diffondersi nel mondo d’oggi. Si ritrovano quindi abilità e conoscenze che fanno capo alla competenza digitale in tutte le discipline e tutte concorrerebbero a costruirla. Competenza digitale significa padroneggiare certamente le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzare con “autonomia e responsabilità” nel rispetto degli altri e sapendone prevenire ed evitare i pericoli. In questo senso, tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione.

L’istituto ,deve impartire agli studenti alcune lezioni riguardanti le nuove tecnologie didattiche da

utilizzare, in modo corretto, attraverso corsi. Bisogna organizzare le varie lezioni con il supporto di tutti i docenti, ma con presenza di tecnici

---

## ***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.

Ogni docente necessita di corsi di formazione e aggiornamento, sulla tematica delle TIC, almeno 1 volta l'anno, per poter affrontare ogni richiesta che l'alunno fa ad un suo dubbio ed essere pronti nell'affrontare una lezione.

Il corpo docente potrebbe partecipare ai corsi di formazione anche nell'ambito di piani nazionali, oltre che ad iniziative organizzate dall'istituzione o dalle scuole associate in rete e possiede generalmente una buona base di competenze e nel caso delle figure di sistema, anche di carattere specialistico. E' inoltre disponibile ad aggiornamenti per mantenere al passo la propria formazione, in rapporto al rinnovo della dotazione multimediale. Il percorso complesso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica, non esauribile nell'arco di un anno scolastico, può pertanto prevedere momenti di auto aggiornamento, momenti di formazione personale o collettiva anche all'interno dell'istituto, con la condivisione delle conoscenze dei singoli e il supporto dell'Animatore digitale, la partecipazione alle iniziative promosse dall'Amministrazione centrale e dalle scuole polo; potrebbe comprendere la fruizione dei materiali messi a disposizione dall'Animatore stesso sulle bacheche virtuali appositamente create, corsi di aggiornamento online.

---

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

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

Il DS in collaborazione con gli esperti esterni del progetto, all'inizio o fine anno, deve proporre a tutti i docenti, collaboratori e amministratori corsi di aggiornanento riguardante il problema dei rischi che ogni alunno incorre nell'utilizzo non corretto di internet sul territorio

Il percorso della formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet, può prevedere momenti di auto aggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui possono accedere sempre di più ed autonomamente anche i ragazzi. Potrebbe essere predisposta una bacheca online per la messa a disposizione e la condivisione di materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di internet, collegata alla homepage del sito scolastico. Si potrebbe trovare materiali informativi sulla sicurezza in internet per l'approfondimento personale, per le attività con gli studenti e gli incontri con i genitori, costituiti da guide in pdf, video, manuali a fumetti, link a siti specializzati e contributi della Polizia di Stato, dell'Arma dei Carabinieri, di Telefono Azzurro, dal sito "Generazioni connesse",ecc.

---

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

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

Per prevenire ogni rischio scuola e famiglia devono collaborare, insieme a docenti ed esperti esterni. Con la consapevolezza che l'tilizzo on line sia uno strumento importante per arricchire i proprio

bagaglio culturale. Il DS deve tenere sempre informate le famiglie delle varie attività e iniziative che l'istituto propone agli alunni.

L' Istituto dovrebbe attivare iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine potrebbero essere previsti incontri fra docenti e genitori per la diffusione del materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati e dalle forze dell'ordine. Potrebbero essere favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo. Sul sito scolastico e sulla relativa bacheca virtuale relativa a "Generazioni connesse" possono essere messi in condivisione materiali dedicati ad alunni e alle famiglie come guide in formato .pdf e video che possono fornire spunti di approfondimento e confronto. La scuola si dovrebbe impegnare alla diffusione delle informazioni e delle procedure contenute nel documento (e-Policy ) per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e prevenire i rischi legati a un utilizzo non corretto di internet.

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

---

### **AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020)**

**Scegliere almeno 1 di queste azioni**

- 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.
- 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.

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

**Scegliere almeno 1 di queste azioni**

- 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.
- 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.

I.C. KAROL WOJTYLA ROMA

## INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI DEGLI STUDENTI E DELLE FAMIGLIE

Art. 13 del Regolamento (UE) 2016/679

Ai sensi del Regolamento Generale dell'UE sulla Protezione dei Dati (RGPD o GDPR nel prosieguo "Regolamento") n. 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 e che abroga la Direttiva 95/46/CE, considerando le disposizioni del d.lgs. 196/2003 e s.m.i. c.d. "Codice privacy", come novellato dal d.lgs. 101/2018, la informiamo che i dati personali forniti all'Istituto scolastico saranno trattati secondo i principi di liceità, correttezza e trasparenza al fine di garantire i diritti, le libertà fondamentali, nonché la dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

### TITOLARE DEL TRATTAMENTO

Il Titolare del Trattamento Dati Personali (di seguito Titolare), è: l'Istituto Comprensivo "Karol Wojtyla", con sede in Roma - Via Concesio, 2, nella persona del Dirigente Scolastico pro tempore Prof.ssa Loredana Garritano. Dati di contatto:

Tel. +39 06 33610055 - Email: rmic8ag009@istruzione.it - PEC: rmic8ag009@pec.istruzione.it

### RESPONSABILE DELLA PROTEZIONE DATI

Il Responsabile della Protezione dei Dati personali (RPD o anche DPO) è: Massimo Corinti Dati di contatto: Mob. +39 335 7687380 - E-mail: dpo@corinti.eu - PEC: dpo@pec.corinti.eu.

### FINALITÀ E BASI GIURIDICHE DEL TRATTAMENTO

Ai sensi dell'art. 6 del Regolamento, in particolare al paragrafo 1, lettera e), considerando l'art. 2-ter del d.lgs. 101/2018, i dati personali di studenti e famiglie, sono trattati per l'assolvimento degli obblighi istituzionali dell'Istituto scolastico e, in particolare, per la partecipazione alle attività educative, formative e di istruzione stabilite dal Piano dell'Offerta Formativa, svolte sia in presenza sia attraverso didattica a distanza, nonché per finalità strettamente connesse e strumentali alla gestione dei rapporti con gli alunni, per finalità connesse agli obblighi previsti da leggi e da regolamenti in materia di istruzione ed assistenza scolastica, attività didattica- formativa, di valutazione e attività propedeutiche all'avvio dell'anno scolastico.

La base giuridica per le suddette finalità è l'esecuzione di un compito d'interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare. Per tali finalità non è richiesto il consenso dell'interessato.

## CATEGORIE DEI DATI TRATTATI

Considerato i principi applicabili al trattamento dei dati personali previsti dall'art. 5 del Regolamento (UE), le categorie di dati personali di studenti e famiglie che potranno essere trattati dall'Istituto scolastico sono:

- Dati personali "comuni" nei quali rientrano, a titolo esemplificativo, le generalità, l'anagrafica completa inclusi eventuali numeri di identificazione personale, i recapiti (ad es. numero di cellulare, indirizzo e-mail);
- Dati personali "particolari" che le istituzioni scolastiche sono autorizzate a trattare ai sensi dell'art. 9 paragrafo 2, lettera g) del Regolamento e considerando gli artt. 2-sexies comma 2 lettera bb) del d.lgs. 101/2018, indicando anche le operazioni ordinarie che i Titolari devono necessariamente svolgere per perseguire le finalità di rilevante interesse pubblico.
- Dati "giudiziari" ai sensi dell'art. 2-octies del d.lgs. 101/2018.

Per comodità di riferimento, all'interno delle presenti informazioni, l'espressione "dati personali" dovrà essere intesa come riferimento a tutti i Suoi dati personali, salvo diversamente specificati.

La informiamo che i dati personali di studenti e famiglie oggetto di trattamento, potranno essere:

a) nelle attività propedeutiche all'avvio dell'anno scolastico:

o dati relativi alle origini razziali ed etniche, per favorire l'integrazione degli alunni con cittadinanza non

italiana;

o dati relativi alle convinzioni religiose, per garantire la libertà di credo religioso e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento;

o dati relativi allo stato di salute e alla situazione vaccinale, per assicurare l'erogazione del sostegno agli alunni diversamente abili per la composizione delle classi, per alla gestione del percorso integrato per la somministrazione dei farmaci in ambito scolastico con riferimento al protocollo di intesa MIUR - Ufficio

scolastico regionale per il Lazio e Regione Lazio;

o dati relativi alle vicende giudiziarie, per assicurare il diritto allo studio anche a soggetti sottoposti a regime

di detenzione (i dati giudiziari emergono anche nel caso in cui l'autorità giudiziaria abbia predisposto un

programma di protezione nei confronti degli alunni che abbiano commesso reati). b) nell'espletamento dell'attività educativa, didattica, formativa e di valutazione:

o dati relativi alle origini razziali ed etniche per favorire l'integrazione degli alunni con cittadinanza non italiana;

o dati relativi alle convinzioni religiose per garantire la libertà di credo religioso;  
o dati relativi allo stato di salute e alla situazione vaccinale, per assicurare l'erogazione del servizio di refezione scolastica, del sostegno agli alunni con disabilità o disturbi specifici dell'apprendimento (art.3 comma 1 e 3 della L. 104/92 e L. 170/2010), dell'insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività educative e didattiche

programmate, a quelle motorie e sportive, alle visite guidate e ai viaggi di istruzione;  
o dati giudiziari, per assicurare il diritto allo studio anche ai soggetti sottoposti a regime di detenzione; o dati relativi all'esame dei provvedimenti atti a dimostrare l'esercizio della responsabilità genitoriale;

c) nella gestione del contenzioso tra la scuola e le famiglie degli alunni:

dati sensibili giudiziari concernenti tutte le attività connesse alla difesa in giudizio dell'Istituto scolastico.

Il Titolare potrà trattare i dati per immagini, foto e riprese audio-video all'interno dell'attività educativa e didattica, per scopi formativi e informativi, da affiggere all'interno dell'Istituto scolastico o da pubblicare sul sito web istituzionale, il trattamento avrà natura temporanea ovvero, per il tempo necessario per le finalità a cui sono destinati. Inoltre, il Titolare ogni qualvolta si dovesse presentare la necessità di effettuare foto o riprese audio- video afferenti a specifici progetti, invierà una specifica informativa. Per tutti i trattamenti di dati per immagine sarà richiesto un apposito consenso facoltativo e liberamente espresso da parte delle famiglie.

#### MODALITA' DI TRATTAMENTO E TRATTAMENTI AUTOMATIZZATI

I dati personali forniti all'Istituto, saranno trattati nel rispetto della normativa sopracitata e degli obblighi di riservatezza e liceità cui è ispirata l'attività del Titolare. I dati verranno trattati sia su supporti cartacei sia attraverso strumenti informatici per lo svolgimento delle attività educative, ivi comprese eventuali piattaforme e-learning per la didattica a distanza (DAD) (ad esempio Microsoft 365 Education, G Suite for Education, Edmodo), nell'osservanza e nel rispetto delle misure previste dal GDPR. Non esistono processi decisionali automatizzati e non viene attuata una profilazione dei dati.

#### DIFFUSIONE, COMUNICAZIONE E SOGGETTI CHE ACCEDONO AI DATI

I dati personali forniti all'Istituto potranno essere comunicati al personale scolastico adeguatamente formato ed autorizzato per lo svolgimento delle attività educative ed amministrative ad esse connesse - ex art. 2-quaterdecies del d.lgs. 101/2018. Tali dati, inoltre, potranno risultare accessibili a soggetti esterni individuati dal Titolare e nominati Responsabili esterni del trattamento dei dati personali (es. società di servizio, fornitori di piattaforme e-learning o cloud), per la fornitura dei servizi necessari alla realizzazione delle attività educative ed amministrative sopra richiamate. L'elenco dei soggetti esterni che trattano dati per conto dell'Istituto è disponibile facendone richiesta al Titolare, l'accesso a questi dati è subordinato alla valutazione della legittimità della richiesta.

Da ultimo, la comunicazione dei dati personali potrà essere effettuata verso enti e/o autorità pubbliche in base agli obblighi previsti dalla legge e/o da regolamenti. L'istituto non trasferisce dati

personali in paesi terzi o organizzazioni internazionali. Qualora ciò si rivelasse necessario ai fini istituzionali, per lo svolgimento delle attività educative e di didattica a distanza, l'Istituto provvederà ad adottare misure idonee affinché il trasferimento presenti un adeguato livello di sicurezza e garanzia.

#### .DURATA DEL TRATTAMENTO E CONSERVAZIONE DEI DATI PERSONALI

#### DIRITTI DELL'INTERESSATO

Contattando il Titolare, per tramite del Responsabile della Protezione dei Dati, l'interessato può esercitare i diritti previsti di cui agli artt. da 15 a 22 e per quanto applicabili in considerazione dell'art. 23 del Regolamento. Laddove richiesto, l'interessato ha il diritto di accesso ai propri dati personali, alla rettifica dei dati inesatti, alla cancellazione, alla limitazione o alla possibilità di opporsi al trattamento, di richiedere la portabilità dei dati, di revocare il consenso. La risposta alle richieste sarà fornita entro un mese, se la richiesta è troppo complessa o in presenza di numerose richieste tale periodo può prorogarsi di altri due mesi.

Inoltre, l'interessato ha sempre il diritto di proporre reclamo al Garante ai riferimenti presenti nel sito web: [www.garanteprivacy.it](http://www.garanteprivacy.it), o di adire le opportune sedi giudiziarie.

Aggiornato il 31 marzo 2020

---

## 3.2 - Accesso ad Internet

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

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva

2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

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

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

L'accesso a internet è possibile e consentito per la didattica nei laboratori multimediali. Si potrebbe affermare che solo il docente dalla propria postazione può consentire agli alunni di accedere a internet. L'accesso è per tutti schermato da filtri che dal server impediscono il collegamento a siti appartenenti a black list o consentono il collegamento solo a siti idonei alla didattica, secondo le impostazioni che darà l'Animatore digitale che periodicamente provvederà alla manutenzione e aggiornamento del sistema informatico del laboratorio, ove necessario richiedono l'intervento di tecnici esterni. Le postazioni degli alunni sono occasionalmente utilizzate anche dai docenti, quando questi si servono dei laboratori. I docenti hanno piena autonomia nel collegamento ai siti web.

. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;

. E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza. Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario al regolamento interno deve darne comunicazione al Dirigente Scolastico.

---

### **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.

Con l'avvento di internet sono cambiate molte cose e anche il modo di promuovere la propria attività, la comunicazione, prodotti e servizi deve adeguarsi a questo cambiamento. Diventa

fondamentale imparare a comunicare sul web e le sue numerose piattaforme.

Cisco

Classroom

Weschool

---

### **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.

- Per gli studenti: Non è consentito alcun uso di strumenti elettronici personali e solo eccezionalmente quello del cellulare in caso di urgenza per comunicazioni tra gli alunni e le famiglie, su autorizzazione e con controllo dell'identità dell'interlocutore verificata dal docente.

Per i docenti: Durante le ore delle lezioni non è consentito l'utilizzo del cellulare, mentre è consentito l'uso di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili. Durante il restante orario di servizio è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente mentre è permesso l'uso di altri dispositivi elettronici personali per attività funzionali all'insegnamento, ad integrazione di quelli scolastici disponibili.

Per il personale della scuola: gestione degli strumenti personali- cellulari, tablet ecc. Durante l'orario di servizio al restante personale scolastico è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente.

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

---

### **AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).**

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

- 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
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

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

- 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
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

---

## 4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

Massima attenzione deve essere data al rischio online che il minore corre e ovvero:

- commettere azioni on line che potrebbero danneggiare se stesso o altri
- essere una vittima di questi avvenimenti
- essere spettatore e osservatore di queste azioni e non intervenire affinché vengano eliminate

Per questo è importante sensibilizzare l'intera comunità scolastica a:

- Saper riconoscere e distinguere questi fenomeni tra loro
- Sapere quali sono le migliori strategie da mettere in campo per ridurre il fenomeno

Per poter ridurre le situazioni di rischio saranno importantissime le campagne di sensibilizzazione e prevenzione:

#### Sensibilizzazione

In questo caso la sensibilizzazione coincide con l'informazione, che si configura sia come informazioni necessarie utili a conoscere il fenomeno, sia illustrare i possibili comportamenti e soluzioni da adottare.

#### Prevenzione

La prevenzione coincide con la serie di attività e interventi attuati per promuovere le corrette competenze digitali negli alunne e alunni al fine di evitare rischi in rete.

---

## 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).

## a legg

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 avrà il compito di coordinare le iniziative di prevenzione e contrasto, anche avvalendosi di esperti come la Polizia postale e le Associazioni preposte.

## ***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.

L'Hate speech, letteralmente "discorso d'odio", indica un'offesa (post, immagini, commenti, ecc) fondata su una qualsiasi discriminazione razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, ecc etera ai danni di una singola persona o di un gruppo.

E' un fenomeno sempre più diffuso per questo è importante :

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano le varie forme sopra esplicitate di hate speech.
- promuovere nei giovani la partecipazione civica e l'impegno, non solo attraverso la scuola ma anche attraverso i media digitali e i social network.

---

## ***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?*

Particolare attenzione deve essere data alla dipendenza da Internet e gioco online. L'eccessivo e incontrollato utilizzo della Rete può causare comportamenti patologici e dipendenze e causare o essere associato a isolamento sociale, problematiche a livello scolastico e sintomi da astinenza.

---

## 4.5 - Sexting

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

Il “Sexting” indica un fenomeno di frequente ascesa e si identifica nello scambio di contenuti medialmente (immagini, foto, video) sessualmente espliciti tra giovanissimi. Spesso i minori non si rendono conto di scambiare materiale pedopornografico che non solo potrebbe arrivare in mani sbagliate ma anche e soprattutto avere conseguenze importanti sulla psiche emotiva dei protagonisti

---

## 4.6 - Adescamento online

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

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

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

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

Il grooming (dall’inglese “groom” - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenzialmente abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare con essi 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, Instagram , 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 - 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.

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

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

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

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

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

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

---

## 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](#).**

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"

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

---

**AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).**

**Scegliere almeno 1 di queste azioni:**

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.
- Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.
- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

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

**Scegliere almeno 1 di queste azioni:**

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



# Capitolo 5 - Segnalazione e gestione dei casi

---

## 5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

I.C. KAROL WOJTYLA ROMA

PROTOCOLLO D'AZIONE

PREVENIRE E CONTRASTARE IL FENOMENO DEL BULLISMO E CYBERBULLISMO

## OBIETTIVI DEL PROTOCOLLO

L' Istituto Comprensivo Karol Wojtyla vista:

- Legge 71 del 29 maggio 2017: disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo pubblicata in Gazzetta Ufficiale il 3 giugno 2017.
- D.M. 05/ 02/2007 n.16 linee di indirizzo generali ed azioni a livello nazionale per la prevenzione e la lotta al bullismo
- Direttiva del Ministero della Pubblica Istruzione 15 Marzo 2014: OGGETTO: linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità dei genitori e dei docenti
- Linee guida del MIUR del 13 Aprile 2015: Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e la cyberbullismo
- Direttiva Ministeriale del 15 marzo 2007 - Linee di indirizzo utilizzo telefoni cellulari

Pone i seguenti obiettivi per prevenire e contrastare il fenomeno del Bullismo e Cyberbullismo:

1. Aumentare la consapevolezza del fenomeno all'interno dell'Istituto negli alunni, nei docenti e nelle famiglie
2. Disporre modalità di prevenzione e intervento per contrastare il fenomeno
3. Definire le modalità di intervento nei casi accertati di tale fenomeno

## DEFINIZIONE DI BULLISMO

Il Bullismo è un' azione di violenza perpetrata da uno o più adolescenti nei confronti di un altro a scuola o fuori il contesto scolastico.

Un azione si può definire bullismo quando vi è:

1. Intenzionalità
2. Prepotenza continuativa e ripetuta nel tempo
3. Danneggiamento della persona in modo verbale, fisico e psicologico
4. Disparità di forze tra chi fa azione di prepotenza e chi la subisce
5. Isolamento della vittima caduta dell'autostima

## DEFINIZIONE DI CYBERBULLISMO

Azione perpetrata attraverso i mezzi di comunicazione:

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 minori, realizzata per via telematica, nonché la diffusione di contenuti online 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" (art. 1 comma 2 della legge 71/2017)

Le misure messe in campo dalla scuola per contrastare il fenomeno del Bullismo - Cyberbullismo:

1. La prevenzione
2. La collaborazione con l'esterno
3. L'intervento in caso di fenomeno Bullismo-Cyberbullismo: misure correttive, educative e sanzioni.

N.B.

Per la Prevenzione e Come segnalare si rimanda al paragrafo 5.2

Per la Collaborazione con l'esterno si rimanda al paragrafo 5.3

Per le Misure educative, correttive e sanzioni si rimanda al cap. 5.4

---

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

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

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

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

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

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

---

### Strumenti a disposizione di studenti/esse

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

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

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

### PREVENZIONE

E' necessario organizzare Corsi di formazione per il corpo docenti, questo al fine di fare in modo che, chi sta a contatto con i bambini e adolescenti , possa avere validi strumenti conoscitivi per essere in grado di:

1. Sensibilizzare e lavorare nel gruppo classe per la condivisione di regole di convivenza civile attraverso metodologie cooperative atte a incrementare comportamenti corretti per garantire il rispetto e la dignità di ogni persona.
2. Riconoscere ed interpretare gli stati di sofferenza che si manifestano nell'ambito scolastico.
3. Individuare stati d'animo derivanti da sofferenza dovuta al cyberbullismo e bullismo.

Utilizzo piattaforma on-line del sito istituzionale dedicato ai fenomeni del bullismo e del cyberbullismo [www.generazioniconnesse.it](http://www.generazioniconnesse.it) al fine di garantire una maggiore consapevolezza sul tema.

Riconoscimento della fenomenologia

Individuare i sintomi in una vittima.

Agli insegnanti è richiesta la capacità di cogliere ed interpretare i messaggi di sofferenza che manifestano gli alunni in ambito scolastico.

Nel caso del bullismo o del cyberbullismo è importante non sottovalutare il problema ed agire tempestivamente, poiché le conseguenze del fenomeno sul piano psicologico, sia a breve che a lungo termine, possono essere gravi sia per le vittime, sia per i bulli e per gli spettatori passivi. Per le vittime il rischio è quello di manifestare il disagio innanzitutto attraverso sintomi fisici (es. mal di pancia, mal di testa) o psicologici (es. incubi, attacchi d'ansia), associati ad una riluttanza nell'andare a scuola.

In caso di azioni protratte nel tempo LE VITTIME possono intravedere come unica possibilità per sottrarsi al bullismo quella di cambiare scuola, fino ad arrivare in casi estremi all'abbandono scolastico; alla lunga, le vittime mostrano una caduta della propria autostima mostrandosi insicuri, hanno problemi sul piano relazionale, fino ad arrivare in alcuni casi, a veri e propri disturbi

psicologici, tra cui quello dell'ansia o della depressione.

I BULLI possono presentare: un calo nel rendimento scolastico, difficoltà relazionali, disturbi della condotta per incapacità di rispettare le regole che possono portare, nel lungo periodo, a veri e propri comportamenti antisociali e devianti o ad agire con comportamenti aggressivi e violenti in famiglia e sul lavoro.

GLI SPETTATORI vivono in un contesto di disagio nel quale aumenta la paura e l'ansia sociale e rafforza una logica di indifferenza e scarsa empatia, portando i ragazzi a negare o sminuire il problema.

Gli insegnanti che notano atteggiamenti o comportamenti che suggeriscono una situazione di malessere sono tenuti a darne segnalazione tempestiva alla Dirigente scolastica, alla famiglia dell'alunno.

#### COME SEGNALARE

Sicurezza informatica l'istituto farà attenzione a disciplinare gli accessi al web, richiedendo il rigoroso rispetto del regolamento relativamente all'uso dei cellulari e smartphone.

Provvederà ad una formazione specifica rivolta agli studenti, ai docenti e ai genitori per quanto riguarda l'utilizzo consapevole e sicuro delle tecnologie digitali.

Importante che i genitori conoscano la proprie responsabilità, le conseguenze legali dei comportamenti dei figli e che siano consapevoli delle necessità di un'adeguata vicinanza cercando di controllare e monitorare le amicizie virtuali e i siti frequentati dai figli.

#### Interventi educativi

Le azioni educative devono essere rivolte al bullo, alla vittima e agli spettatori, che possono rivestire una funzione sia attiva (ad esempio scaricando e diffondendo in rete il materiale postato dal cyberbullo) sia passiva (limitandosi a rilevare gli atti di cyberbullo rivolti ad altri senza intervenire).

Gli interventi educativi saranno effettuati: dai docenti stessi, avvalendosi anche della collaborazione

di Enti e associazioni presenti sul territorio.

Questa prevenzione verterà su tutti gli utenti della scuola :

- 1) Docenti e Personale ATA
- 2) Studenti
- 3) Famiglie

#### PIANIFICAZIONE INTERVENTI

Verso gli studenti

Progetti - Incontri durante l'anno scolastico, per sensibilizzare sul tema del bullismo e del cyberbullismo.

L'educazione trasversale alle competenze sociali.

La promozione di progetti, con l'eventuale contributo esterno di figure professionali (psicologi, educatori, polizia postale, ...) in cui gli alunni acquisiscano le competenze per relazionarsi correttamente.

La predisposizione di materiali e di incontri specifici che diano agli alunni regole concrete all'uso dei social network, che suggeriscano buone pratiche e indichino riferimenti da usare in caso di un abuso e una informativa sui pericoli che corrono in rete.

Predisposizione di moduli da mettere in Istituto per segnalazioni di episodi gravi.

Per la Scuola Primaria verranno effettuati degli interventi nelle classi con la partecipazione dei ragazzi della Secondaria di Primo Grado.

### Verso i genitori

La scuola coinvolge attivamente le famiglie, principali responsabili dell'educazione dei ragazzi, attraverso eventi che prevedono l'intervento di altri enti e del territorio. Sarà a disposizione dei genitori una sezione, sul sito internet della scuola, con link delle principali autorità in materia per l'informazione e la formazione delle famiglie per il contrasto del cyberbullismo

### Verso i docenti

FORMAZIONE CONTINUA DEGLI INSEGNANTI perché possano avere validi strumenti conoscitivi per essere in grado di:

- Sensibilizzare e lavorare sull'intero gruppo classe per la condivisione di regole di convivenza civile attraverso metodologie cooperative atte a implementare comportamenti corretti per garantire il rispetto e la dignità di ogni persona.
- Cogliere ed interpretare i messaggi di sofferenza che si manifestano nell'ambito scolastico.
- Individuare e capire i sintomi derivanti da sofferenza dovuta al cyberbullismo e bullismo.

---

## 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.

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.

#### COLLABORAZIONE CON L'ESTERNO

La collaborazione si esplica principalmente attraverso:

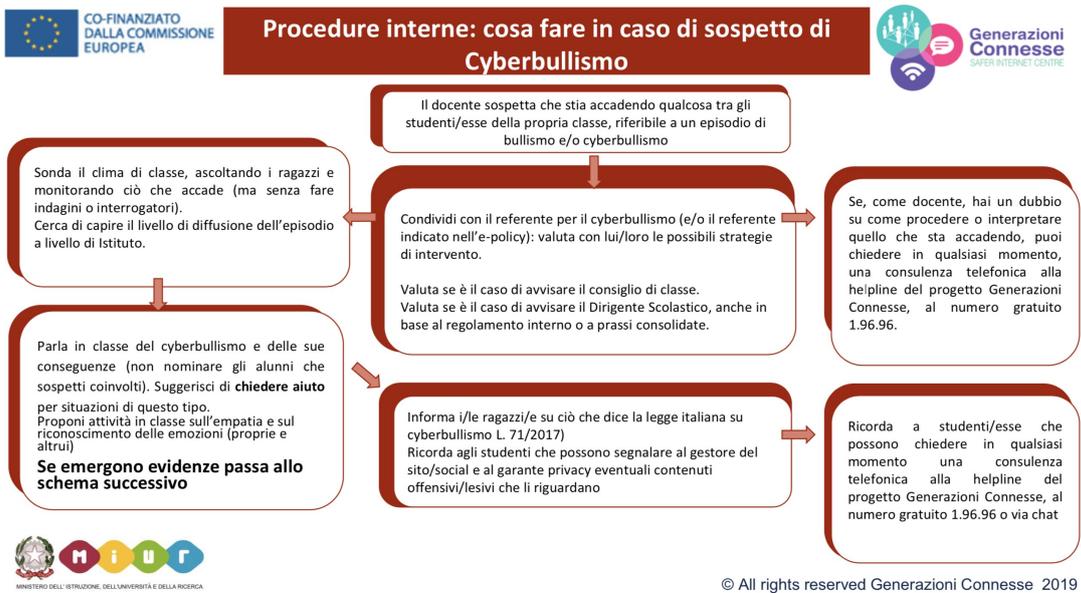
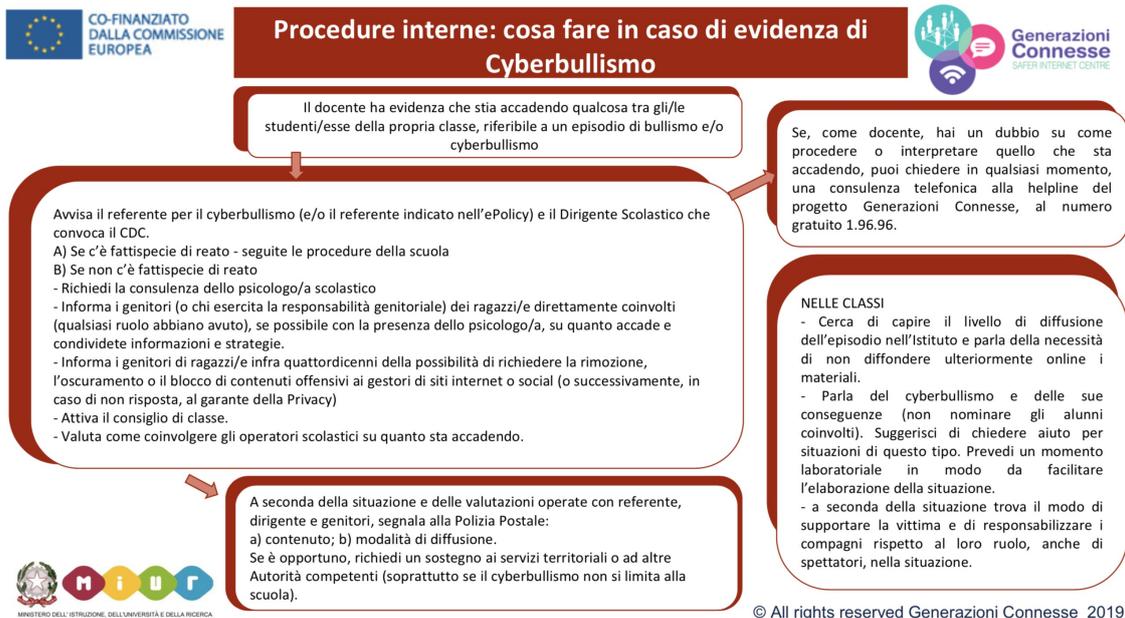
Azioni di supporto, di monitoraggio e di dialogo costante con Enti Locali, Polizia Locale, ASL, Tribunale dei Minori, Associazioni del territorio e/o nazionali e incontri a scuola con le Forze dell'Ordine e con la Polizia Postale, nell'ambito di progetti tesi ad attivare la riflessione sul rispetto delle persone e delle cose, sulle conseguenze del proprio comportamento e sulla responsabilità per contribuire a costruire un ambiente accogliente e sereno per tutti, diffondendo la cultura del rispetto e della non violenza fra le giovani generazioni.

Si segnalano inoltre:

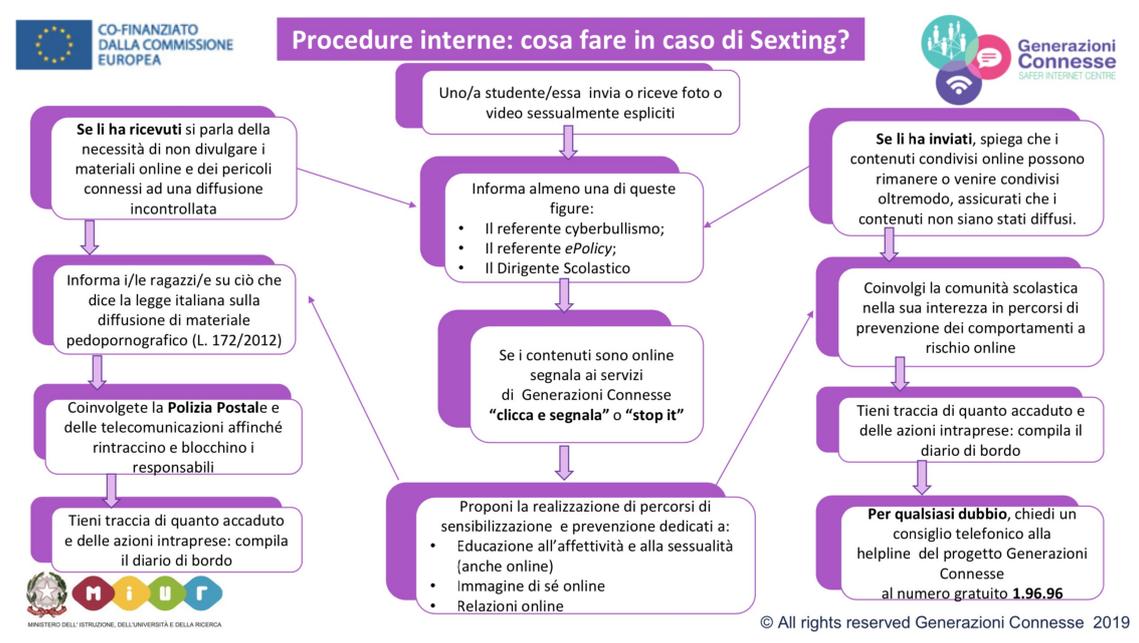
- Servizio di [Helpline 19696](#) e [Chat di Telefono Azzurro](#) per supporto ed emergenze;
- [Clicca e segnala di Telefono Azzurro](#) e [STOP-IT di Save the Children Italia](#) per segnalare la presenza di materiale pedopornografico online.

## 5.4. - Allegati con le procedure

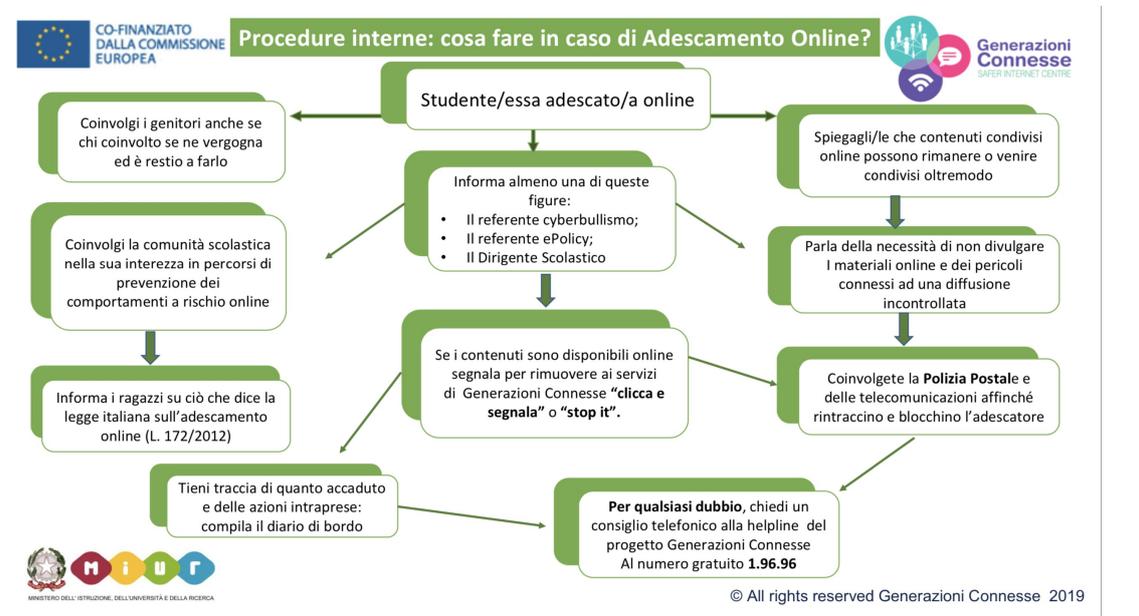
### Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



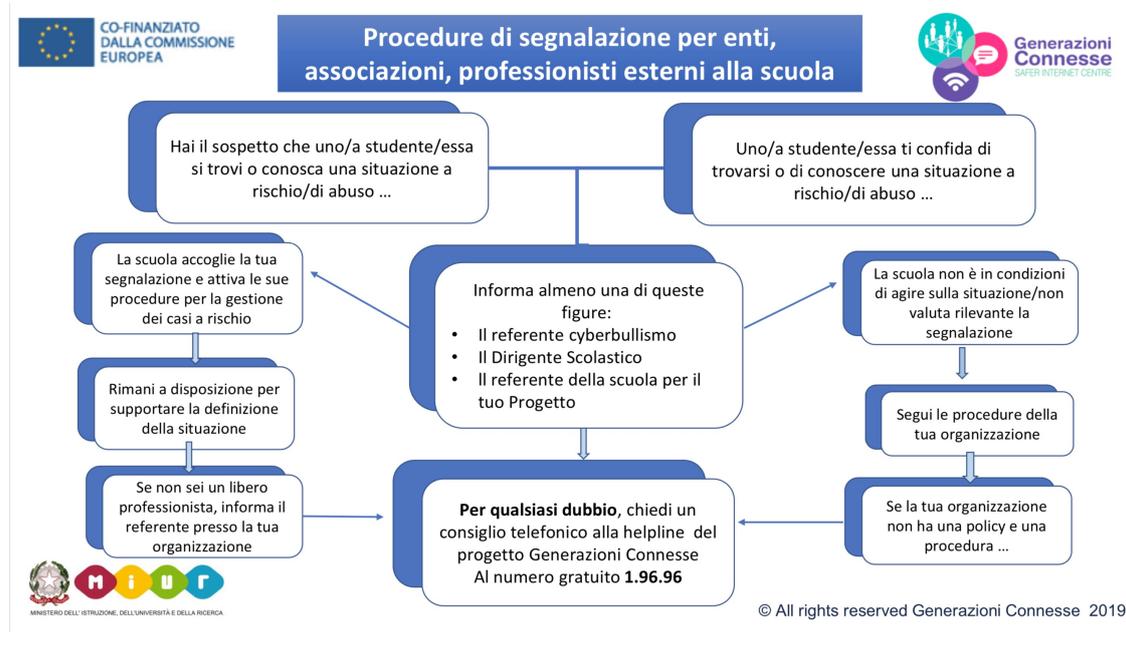
## Procedure interne: cosa fare in caso di sexting?



## 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](#)

### INTERVENTO IN CASI ACCERTATI: MISURE CORRETTIVE E SANZIONI

L'Istituto ha un Regolamento di disciplina che prevede di sanzionare episodi di mancato rispetto delle regole nell'ambito del bullismo e del cyberbullismo prevedendo specifiche sanzioni disciplinari.

Sono precisate le regole di utilizzo a scuola di computer, smartphone e altri dispositivi elettronici con le rispettive sanzioni disciplinari.

### PROCEDURE IN CASI ACCERTATI DI BULLISMO-CYBERBULLISMO

a) Piano D'azione

b) Team D'azione

Il Team d'azione prende in carico la segnalazione, valuta l'accaduto, decide l'intervento, monitora il caso, decide i tempi di azione per verificare l'efficacia, infine nei casi gravi da codice rosso contatta i servizi del territorio; il team è composto:

- Dirigente scolastico
- Referente Bullismo - Cyberbullismo
- Docente scuola d'Infanzia
- Docente scuola Primaria
- Docente scuola Secondaria Primo grado
- Docente con competenze trasversali
- Figure professionali

Piano D'azione

Comprende quattro fasi:

1. Prima segnalazione
2. Valutazione
3. Gestione del caso scelta dell'intervento
4. Monitoraggio

1. Prima Segnalazione tutti possono fare la segnalazione e consegnarla al personale scolastico, si allega scheda di segnalazione:

#### MODULO DI SEGNALAZIONE

Persona che compila la segnalazione: \_\_\_\_\_

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

Luogo: \_\_\_\_\_

1- La persona che segnala il caso del presunto bullismo é

La vittima \_\_\_\_\_

un compagno della vittima \_\_\_\_\_

padre/madre/tutore della vittima: \_\_\_\_\_

un insegnante \_\_\_\_\_

altri \_\_\_\_\_

2-Vittima: \_\_\_\_\_ classe \_\_\_\_\_

altre vittime \_\_\_\_\_ classe \_\_\_\_\_

altre vittime \_\_\_\_\_ classe \_\_\_\_\_

3-Bullo o bulli (o presunti)

Nome \_\_\_\_\_ classe \_\_\_\_\_

Nome \_\_\_\_\_ classe \_\_\_\_\_

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

\_\_\_\_\_  
\_\_\_\_\_

5. Quante volte sono successi gli episodi?

Orario scolastico o extrascolastico, luogo

\_\_\_\_\_  
\_\_\_\_\_ Data compilazione: \_\_\_\_\_

Firma compilatore \_\_\_\_\_

Firma del segnalatore \_\_\_\_\_

2) Valutazione

Il team prende in consegna la segnalazione, analizza la fenomenologia del caso e decide il livello di gravità diviso in:

- CODICE VERDE (Situazione da monitorare con interventi preventivi, non esiste un caso acclamato con ripetizione, ma atteggiamenti)
- CODICE GIALLO (Interventi indicati su bullo e vittima, azioni con ripetizione nel tempo, interventi mirati e strutturati)
- CODICE ROSSO (Interventi di emergenza con supporti rete, caso acclamato che non si risolve con i soli interventi scolastici)

### 3) Gestione del caso scelta dell'intervento

In base al codice assegnato l'intervento che si attua può essere:

1. Approccio educativo con la classe interventi preventivi (codice verde-giallo )
2. Caso accertato intervento individuale, coinvolgimento della famiglia (codice giallo-rosso)
3. Gestione della relazione (codice verde-giallo-rosso)
4. Coinvolgimento bullo-vittima (codice giallo-rosso)
5. Supporto intensivo a lungo termine con coinvolgimento della rete(codice rosso)

### 4) Monitoraggio

Si valutano i cambiamenti a seguito dell'intervento che può essere:

1. A breve termine: tempo 1 settimana, capire il cambiamento nella

Vittima e nel bullo

2. A lungo termine: tempo 1 mese, si verifica l'efficacia

dell'intervento

Dopo la valutazione del caso sono previsti questi percorsi percorso:

a) Con la vittima:

- convocazione tempestiva della famiglia (esposizione del caso);
- Promozione di una rete di supporto, di comunicazione e di collaborazione con la famiglia;
- Indicare alla famiglia le agenzie preposte ad un percorso di assistenza, di sostegno educativo e psicologico, soprattutto al fine di incrementare autostima e assertività; azioni di supporto educativo in classe.

b) Con il bullo o cyberbullo:

- Convocazione tempestiva della famiglia;
- Promozione di una rete di supporto, di comunicazione e di collaborazione con la famiglia;
- Attivazione di interventi rieducativi
- Inserimento nel registro classe della descrizione oggettiva della condotta del bullo/ cyberbullo;
- Comminazione inflessibile delle sanzioni previste dal regolamento di Istituto;
- Eventuale collaborazione con i servizi pubblici e/o privati che accompagnano il percorso riabilitativo dei minori coinvolti.

c) Con la classe:

Ai fini dell'inclusione, attivazione di un progetto di intervento che preveda:

- Colloqui personali con gli alunni, affinché possano emergere gli stati d'animo e i vissuti degli alunni;
- Sensibilizzazione degli studenti mediante il rinforzo dell'informazione e della formazione sul fenomeno;

**SANZIONI DISCIPLINARI**

Situazione accertata di Bullismo e Cyberbullismo specificato nelle tabelle seguenti.

L'uso di smartphone, tablet e altri dispositivi mobili, o delle funzioni equivalenti presenti sui telefoni cellulari è pertanto consentito, ma unicamente su indicazione del docente, con esclusiva finalità didattica, in momenti ben definiti e con modalità prescritte dall'insegnante. L'attività deve prevedere La scuola promuove iniziative di informazione e formazione sui temi dell'uso consapevole dei dispositivi informatici, dei nuovi media, dei social network e in generale delle applicazioni web e mobili.

MANCANZA	FREQUENZA	PROVVEDIMENTO	SOGGETTI
L'alunno ha lo smartphone acceso (riceve chiamata/notifica di messaggio)	1° volta	Segnalazione sul registro di classe a cura del docente (prima volta) e trascritto sul diario o libretto personale dell'alunno/a con nota che sarà firmata dai genitori.	Docente Docente / DS Docente/DS
	2° volta	Comunicazione immediata ai genitori per la convocazione con il docente interessato o Coordinatore di classe o Dirigente.	"
	3° volta	Previa comunicazione alla famiglia, dell'alunno/a sarà comunicata una sanzione disciplinare di sospensione fino a tre giorni anche con eventuale obbligo di frequenza. Al termine del periodo di sospensione il docente annoterà sul registro di classe l'ammissione al regolare svolgimento delle lezioni.	"
Effettua telefonate e/o attività non consentita	1° volta	Comunicazione immediata ai genitori per la convocazione con il docente interessato o Coordinatore di classe o Dirigente.	Docente/ DS Consiglio di classe Docente/ DS Consiglio di classe
	2° volta	Previa comunicazione alla famiglia, dell'alunno/a sarà comunicata una sanzione disciplinare di sospensione fino a tre giorni anche con eventuale obbligo di frequenza. Al termine del periodo di sospensione il docente annoterà sul registro di classe l'ammissione al regolare svolgimento delle lezioni	"
	3° volta	L'Istituto scolastico sanzionerà con l'allontanamento fino a sette giorni con o senza obbligo di frequenza. L'istituto valuterà la partecipazione dello studente ad attività utili alla maggiore consapevolezza del gesto compiuto. Obbligo di rimozione del materiale dal proprio profilo.	DS / Consiglio di classe / Consiglio di Istituto

Nei casi più gravi  
(sexting,  
cyberstalking, cyber  
bashing...)

L'Istituto scolastico sanzionerà con  
l'allontanamento fino a quindici giorni con o  
senza obbligo di frequenza.  
L'Istituto valuterà la partecipazione dello  
studente ad attività utili alla maggiore  
consapevolezza del gesto compiuto. Obbligo di  
rimozione del materiale dal proprio profilo.  
Sarà coinvolta la polizia postale o altra forza  
dell'ordine per  
ipotesi "Culpa in educando".

DS /  
Consiglio di  
classe /  
Consiglio di  
Istituto

---

