



# Documento di ePolicy

CBIC850008

"MONTINI"

VIA GIOVANNITTI SNC - 86100 - CAMPOBASSO - CAMPOBASSO (CB)

AGATA ANTONELLI

# 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 documento ha lo scopo di individuare e descrivere la linea di condotta dell'Istituto relativamente all'utilizzo delle TIC nella didattica, educare e sensibilizzare bambini/ragazzi, genitori, docenti e personale tutto della scuola all'uso consapevole di Internet; far acquisire norme comportamentali per prevenire le problematiche che derivano da un utilizzo non responsabile delle tecnologie digitali.

---

## **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.

Nell'ambito dell' E-Policy sono individuati i seguenti ruoli e le principali responsabilità correlate:

### **Dirigente scolastico**

- In collaborazione con figure di sistema (Animatore digitale, FF.SS. area informatica, referente bullismo cyberbullismo, DSGA), redigere/aggiornare e proporre agli OO.CC. l'e-Policy per l'approvazione;
- Unitamente al DSGA, garantire la tutela generale dei dati;
- promuovere la cultura della sicurezza on-line;
- assicurare una formazione adeguata al personale scolastico sull'uso positivo e responsabile delle TIC;
- ricevere relazioni di monitoraggio periodico della sicurezza on-line da parte del responsabile e ditta incaricata;
- garantire che vi sia un sistema di monitoraggio del personale di supporto che svolge le procedure di sicurezza on-line interne;
- intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

### **Responsabili della sicurezza on-line (DSGA e docente su nomina del DS)**

- promuovere la consapevolezza e l'impegno per la salvaguardia on-line in tutta la comunità scolastica

- garantire che tutto il personale conosca le procedure da seguire in caso di incidente nella sicurezza on-line
- garantire la tenuta di un registro sugli incidenti di sicurezza on-line
- favorire la formazione e la consulenza per tutto il personale
- assicurare l'educazione alla sicurezza on-line incorporata nel programma di studio di tutte le discipline
- controllare la condivisione di dati personali
- controllare l'accesso a materiali inadeguati/illegali
- controllare probabili azioni di cyberbullismo e/o altri rischi on-line
- 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

#### **Animatore Digitale ed il suo team**

- pubblicare la E-Policy sul sito della scuola
- diffondere la E-Policy attraverso schede semplificative
- garantire la tutela di tutti i dati relativi agli alunni pubblicati sul sito della scuola e/o altri siti
- supportare il personale scolastico sia dal punto di vista tecnico-informatico, sia in riferimento ai rischi online, alla protezione e gestione dei dati personali
- promuovere percorsi di formazione interna all'istituto negli ambiti di sviluppo della "scuola digitale"
- monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle TIC a scuola
- controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, 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"
- svolgere funzioni di supporto al D.S. e al DSGA (di cui ai punti precedenti Dirigente scolastico e Responsabili della sicurezza on-line (DSGA e docente su nomina del DS) ).

#### **Referente bullismo e cyberbullismo**

- coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo
- coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori
- coordinare attività e collaborare con le autorità locali e le altre agenzie competenti (Forze di polizia, associazioni e centri di aggregazione giovanile, ...)

- controllare probabili azioni di cyberbullismo e/o altri rischi on-line
- supportare il personale nell'adozione delle procedure da seguire in caso di incidente nella sicurezza on-line

### **Docenti**

- informarsi e 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
- inserire tematiche relative alla sicurezza on-line nel programma di studi della propria disciplina e di altre attività scolastiche
- promuovere l'uso delle tecnologie digitali nella didattica
- supervisionare, accompagnare e supportare gli alunni nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM e di altri dispositivi tecnologici che si connettono alla Rete
- garantire che gli alunni siano consapevoli dei problemi legali relativi ai contenuti elettronici (es. copyright) e posseggano reali capacità di ricerca
- segnalare al Dirigente Scolastico, all'animatore digitale, al referente per il bullismo e cyberbullismo, alle FF.SS. area informatica qualunque problema, violazione o abuso, anche online, che vede coinvolti gli studenti
- garantire che le loro comunicazioni digitali con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali
- illustrare ai propri alunni le regole di utilizzo contenute nel presente documento

### **Personale ATA**

- contribuire nella promozione di politiche scolastiche sulla sicurezza on-line
- avere consapevolezza dei problemi di sicurezza on-line connessi all'uso di telefoni cellulari, fotocamere e dispositivi portatili
- monitorare l'uso di dispositivi tecnologici
- segnalare qualsiasi abuso sospetto ai responsabili della sicurezza on-line
- raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo e cyberbullismo
- adottare comportamenti sicuri, responsabili e professionali nell'uso delle tecnologie
- controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti

### **Alunni**

- leggere, comprendere ed accettare la E-Policy
- utilizzare correttamente le tecnologie digitali
- partecipare a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete

- possedere capacità di ricerca e rispettare la normativa sul diritto d'autore
- segnalare abusi o l'uso improprio delle tecnologie digitali o l'accesso a materiali inappropriati da parte dei compagni
- tutelare e rispettare i propri compagni
- conoscere ed applicare le norme sulla sicurezza
- conoscere la politica scolastica relativa all'uso di telefoni cellulari, fotocamere digitali e dispositivi portatili
- conoscere la politica scolastica sull'uso di immagini e sul cyberbullismo
- adottare buone pratiche di sicurezza on-line dentro e fuori dalla scuola

#### **Genitori o coloro che detengono la responsabilità genitoriale**

- leggere, comprendere, accettare e condividere la E-Policy d'Istituto
- sostenere la scuola nella promozione della sicurezza on-line, anche partecipando a iniziative di sensibilizzazione e formazione organizzate dall'Istituto
- comunicare ai docenti problemi rilevati, relativi all'uso non responsabile delle tecnologie digitali o Internet da parte dei propri figli
- seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllando l'utilizzo del pc e di internet
- accedere al sito web della scuola ed al registro elettronico in conformità con quanto stabilito dalla scuola medesima
- collaborare con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite

---

## ***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).

**I soggetti esterni**, pertanto, sono tenuti a:

- avere consapevolezza dei problemi di sicurezza on-line connessi all'uso di telefoni cellulari, fotocamere e dispositivi portatili
- prendere visione del regolamento d'Istituto relativamente all'uso di telefoni cellulari, fotocamere digitali, dispositivi portatili,
- contribuire nella promozione di politiche scolastiche sulla sicurezza on-line
- monitorare l'uso di dispositivi tecnologici
- segnalare qualsiasi abuso sospetto ai responsabili della sicurezza on-line
- raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo e cyberbullismo
- adottare comportamenti sicuri, responsabili e professionali nell'uso delle tecnologie
- conoscere ed applicare le norme sulla sicurezza
- conoscere ed applicare le procedure di segnalazione
- conoscere i provvedimenti adottabili in caso di omessa segnalazione o di comportamenti adottati in violazione del codice di comportamento

---

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

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

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

- la pubblicazione del documento sul sito istituzionale della scuola;



- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

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

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

### **Condivisione e comunicazione della ePolicy agli alunni e alle alunne**

All'avvio dell'anno scolastico, ogni team docente e consiglio di classe illustrerà la presente e-policy agli alunni, insieme ai regolamenti correlati e al patto di corresponsabilità. Tutti gli alunni saranno informati delle modalità di utilizzo di internet, di ogni dispositivo digitale all'interno del contesto scolastico e delle buone norme da tenere relativamente all'uso delle TIC.

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, con specifico riferimento al contrasto di ogni forma di bullismo/cyberbullismo, mediante azioni mirate che coinvolgano il più possibile gli alunni e le alunne, anche nella eventuale stesura di un proprio vademecum delle regole per la sicurezza online di classe, al fine di prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e.

### **Condivisione e comunicazione della ePolicy al personale scolastico**

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.

### **Condivisione e comunicazione della ePolicy ai genitori**

È auspicabile una forte collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet. Gli incontri scuola- famiglia assembleari, collegiali e individuali rappresenteranno un'occasione utile per sensibilizzare le famiglie sui temi dell'uso delle TIC. Saranno organizzati incontri informativi per presentare e condividere la presente e-policy, nonché eventuali percorsi formativi online rivolti alle famiglie sul tema del bullismo e del cyberbullismo.

L'informazione tramite il sito di istituto e tramite il Registro elettronico sarà la modalità prioritaria per comunicare alle famiglie le iniziative attuate dall'istituto.

---

## **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 infrazioni alla e-Policy possono essere rilevate e segnalate dal personale docente ed ATA nell'esercizio delle proprie funzioni, dagli alunni e dai genitori ai docenti, al referente del Cyberbullismo e al Team Antibullismo. I docenti che eventualmente rilevino infrazioni ai regolamenti e alla e-Policy procederanno tramite richiamo verbale oppure tramite nota disciplinare sul registro elettronico, secondo l'entità della violazione; l'infrazione verrà segnalata al Dirigente Scolastico che valuterà quale condotta adottare: convocazione dello studente, comunicazione alla famiglia o a chi ne fa le veci e, nei casi più gravi, segnalazione alle autorità competenti, secondo quanto previsto dal Regolamento di Istituto, dal Patto di corresponsabilità, dalla normativa inerente alla privacy; eventuali provvedimenti disciplinari ritenuti necessari saranno adottati dal Consiglio di classe in accordo con il Dirigente Scolastico. Il Consiglio di classe, in accordo con la famiglia se lo studente è minorenni, potrà inoltre considerare l'eventualità di un supporto psicologico allo/la studente/ssa attraverso i servizi predisposti all'interno o all'esterno dell'istituto, qualora ciò fosse ritenuto necessario.

L'azione educativa prevista per gli alunni è rapportata - comunque - alla fascia di età e al livello di sviluppo e maturazione personale. In alcuni casi i comportamenti sanzionabili potrebbero essere dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, di cui gli educatori devono tenere conto per il raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno.

In ogni caso, sono previsti interventi educativi di rinforzo rispetto a comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza, di prevenzione e gestione positiva dei conflitti, di pro-socialità, di conoscenza e gestione delle emozioni. Verrà coinvolto tutto il contesto classe con attività specifiche educative e di sensibilizzazione.

### **1. Disciplina degli alunni**

Previo provvedimento disciplinare, per gli alunni che vengono meno ai doveri scolastici e alle norme, si attuano sanzioni rapportate alla gravità delle infrazioni. Tenuto conto di quanto previsto dal D.P.R. n. 235/07, concernente lo Statuto delle studentesse e degli studenti della scuola secondaria, potranno essere attuati percorsi di natura sociale e culturale finalizzati al perseguimento dell'interesse generale della comunità scolastica.

Le violazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali e di internet per fini didattici sono le seguenti:

- utilizzo del telefono cellulare e di altri dispositivi elettronici non autorizzati
- comportamento lesivo della propria e altrui incolumità fisica e psicologica (compresi bullismo e cyberbullismo)
- utilizzo improprio e danni arrecati a dispositivi e materiale Hardware e Software
- trasmissione non autorizzata via Internet di dati personali e immagini
- uso improprio della RETE

Così come indicato nel Regolamento d'Istituto, sono previsti i seguenti procedimenti disciplinari, distinti per organo competente:

### **Docente**

1. Annotazione nel registro di classe
2. Nei casi più gravi: a) ritiro del dispositivo con consegna della SIM allo studente  
b) comunicazione, con fonogramma, ai genitori dell'accaduto  
c) contestuale relazione scritta

### **Dirigente scolastico**

1. Comunicazione o convocazione dei genitori su segnalazione dei docenti e, in caso di particolare gravità, del Consiglio di Classe
2. Denuncia alle autorità competenti nei casi in cui si configuri l'ipotesi di reato

### **Consiglio di classe con la sola componente docente**

1. Provvedimento disciplinare (sanzione sospensione e/o percorso di recupero)
2. Risarcimento economico da parte della famiglia dell'alunno responsabile

Sia le sanzioni disciplinari, sia i percorsi educativi di recupero, vengono deliberati dai rispettivi Consigli di Classe secondo il criterio di proporzionalità: sono, pertanto, commisurati alla particolare gravità dei comportamenti tenuti dagli studenti.

I percorsi di recupero sociale e culturale di seguito elencati possono prevedere attività sia antimeridiane, sia pomeridiane per una durata massima di quindici giorni:

- Riordino del materiale didattico e delle aule.
- Piccoli lavori di manutenzione.
- Svolgimento di attività di utile collaborazione nell'ambito della comunità scolastica.
- Attività didattiche che inducano lo studente alla riflessione e alla rielaborazione dell'episodio verificatosi.

Nei casi in cui si riscontrino persistente disinteresse e trascuratezza, da parte della famiglia, nei confronti del minore, della situazione, su segnalazione dei docenti,

vengono formalmente informati i servizi sociali o l'autorità preposta.

Tutto il personale è tenuto a collaborare con il Dirigente scolastico e con l'Animatore digitale, con la funzione strumentale e il referente per il cyberbullismo e a fornire ogni informazione utile per la risoluzione di eventuali situazioni problematiche connesse all'uso delle TIC e Internet.

### **Impugnazioni**

Contro le sanzioni disciplinari è ammesso ricorso da parte dei genitori, entro quindici giorni dalla comunicazione, ad un apposito organo di garanzia interno alla scuola previsto dall'art. 5 del DPR n. 249 del 24-6-1998. L'organo di garanzia ha durata biennale ed è costituito dai seguenti membri:

- Dirigente Scolastico
- Due genitori
- Due docenti designati dal Collegio unitario dei docenti

Denunce di cyberbullismo saranno trattate in conformità alla normativa vigente e reclami relativi alla protezione dei bambini saranno trattati in conformità alle procedure di protezione dell'infanzia.

## **2. Disciplina del personale scolastico**

Eventuali infrazioni nell'uso del device o della Rete compiute dal personale scolastico saranno gestite dal Dirigente Scolastico, secondo quanto previsto dal Codice di comportamento dei dipendenti pubblici, dal CCNL, dal DPCM 28 novembre 2000 e dalla normativa in vigore inerente alla privacy.

Le possibili infrazioni in cui è possibile che il personale scolastico incorra, relativamente all'utilizzo delle tecnologie digitali e di internet, riguardano l'incidenza che le stesse possono avere sull'uso delle TIC da parte degli allievi:

- utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non compatibile con le attività di docenza, ad esempio salvataggio di materiale non idoneo, uso di social network etc.
- utilizzo delle comunicazioni elettroniche con i genitori e gli alunni mediante canali non ufficiali
- trattamento dei dati personali e dei dati sensibili degli alunni non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi
- diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi
- non adeguata istruzione preventiva degli alunni sull'uso corretto e responsabile delle TIC e di internet
- mancata vigilanza che può favorire un utilizzo non autorizzato delle TIC da parte degli alunni e può generare possibili rischi connessi
- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o

di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale, al referente Cyberbullismo.

Il Dirigente scolastico può disporre il controllo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola; può disporre la cancellazione di materiali non adeguati o non autorizzati dal sistema informatico della scuola, e se necessario ne conserva una copia per eventuali approfondimenti successivi.

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

### **3. Disciplina dei genitori**

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

Gli atteggiamenti da parte della famiglia meno favorevoli sono:

- credere che se il proprio figlio rimane a casa ad usare il computer sia al sicuro e non corra alcun tipo di rischio
- posizionare il computer in un luogo non visibile e controllabile dall'adulto
- una piena e completa autonomia concessa al proprio figlio nella navigazione sul web e nell'uso di cellulare o smartphone
- un utilizzo del pc/tablet/smartphone condiviso, nei quali gli adulti possono conservare in memoria materiali non idonei a minori.

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 altri (culpa in educando e in vigilando).

---

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

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

Il presente documento si integra pienamente per obiettivi e contenuti con il PTOF, incluso il piano per l'attuazione del PNSD e con i regolamenti già in vigore nel nostro Istituto.

---

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

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

All'interno del nostro Istituto è costituita una Commissione E-Policy, nominata dal Dirigente Scolastico, avente il preciso compito di revisionare, aggiornare e monitorare l'implementazione del presente documento. Tutte le modifiche della Policy saranno discusse ed approvate dal Collegio dei Docenti e dal Consiglio d'Istituto.

---

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

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

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per l'aggiornamento dell'ePolicy.

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

- Organizzare 1 o più eventi di presentazione e conoscenza dell'ePolicy rivolto ai nuovi studenti, docenti e 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.

Attualmente nel profilo finale delle competenze digitali (14 anni), contenute nelle Indicazioni Nazionali per il primo ciclo di istruzione si legge che "lo studente ha buone competenze digitali, usa con consapevolezza le tecnologie della comunicazione per ricercare ed analizzare dati e informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo".

È riportato infine che la competenza digitale "arricchisce la possibilità di accesso ai saperi, consente la realizzazione di percorsi individuali di apprendimento, la comunicazione interattiva e la personale espressione creativa".

La scuola, pertanto, tenuto conto anche del quadro di riferimento per le competenze digitali dei cittadini - DigComp 2.1 - si impegna a sviluppare, a seconda del grado di maturità degli alunni, le seguenti competenze:



**Area delle competenze 1: Alfabetizzazione su informazioni e dati**

- 1 Saper navigare, ricercare e filtrare dati, informazioni e i contenuti digitali
- 2 Saper valutare e gestire dati, informazioni e contenuti digitali
- 3 Saper riconoscere e sapersi difendere da contenuti dannosi e pericolosi in Rete (es. app, giochi online, siti non adatti ai minori, ...)

**Area delle competenze 2: Comunicazione e collaborazione**

- 1 Saper interagire con gli altri attraverso le tecnologie digitali
- 2 Saper condividere informazioni attraverso le tecnologie digitali
- 3 Saper esercitare la cittadinanza attraverso le tecnologie digitali
- 4 Saper collaborare attraverso le tecnologie digitali
- 5 Conoscere le Netiquette, ossia le norme di comportamento online
- 6 Saper gestire la propria identità digitale

**Area delle competenze 3: Creazione di contenuti digitali**

- 1 Saper creare e modificare contenuti digitali per esprimersi attraverso mezzi digitali
- 2 Saper modificare, affinare, integrare e rielaborare contenuti digitali per crearne di nuovi originali e rilevanti
- 3 Capire come il copyright e licenze si applicano ai dati, alle informazioni e ai contenuti digitali
- 4 Saper pianificare e sviluppare una sequenza di istruzioni comprensibili da parte di un sistema informatico per risolvere un determinato problema o svolgere un compito specifico

**Area delle competenze 4: Sicurezza**

- 1 Saper proteggere i dispositivi e i contenuti digitali e comprendere i rischi e le minacce presenti negli ambienti digitali. Conoscere le misure di sicurezza e protezione e tenere in debita considerazione l'affidabilità e la privacy
- 2 Proteggere i dati personali e la privacy negli ambienti digitali. Capire come utilizzare e condividere informazioni personali proteggendo se stessi e gli altri dai danni. Comprendere che i servizi digitali hanno un "regolamento sulla privacy" per informare gli utenti sull'utilizzo dei dati personali raccolti
- 3 Saper evitare rischi per la salute e minacce al benessere psico-fisico quando si utilizzano le tecnologie digitali. Essere in grado di proteggere se stessi e gli altri da possibili pericoli negli ambienti digitali (ad es. cyberbullismo). Essere a conoscenza

delle tecnologie digitali per il benessere e l'inclusione sociale

4 Essere consapevoli dell'impatto ambientale delle tecnologie digitali e del loro utilizzo

#### **Area delle competenze 5: Risolvere problemi**

1 Individuare problemi tecnici nell'utilizzo dei dispositivi e degli ambienti digitali e risolverli

2 Saper adeguare e personalizzare gli ambienti digitali in base alle esigenze personali

3 Utilizzare gli strumenti e le tecnologie digitali per creare conoscenza e innovare processi e prodotti. Partecipare individualmente e collettivamente ai processi cognitivi per comprendere e risolvere problemi concettuali e situazioni problematiche negli ambienti digitali.

4 Capire dove occorre migliorare o aggiornare i propri fabbisogni di competenze digitali. Essere in grado di supportare gli altri nello sviluppo delle proprie competenze digitali. Ricercare opportunità di crescita personale e tenersi al passo con l'evoluzione digitale.

Nella nostra scuola le aree tematiche del DigComp 2.1 vengono affrontate anche trasversalmente con la disciplina "Ed. Civica". L'alfabetizzazione informatica è presente nel Piano dell'Offerta Formativa come principale obiettivo da raggiungere nel nostro percorso formativo.

---

## ***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.

Il nostro Istituto, in linea con le azioni del PNSD, nel corso degli ultimi anni, ha consolidato le competenze digitali del personale docente, utilizzando e valorizzando risorse interne adeguatamente formate.

Al fine di promuovere la condivisione di buone pratiche per un uso consapevole delle risorse digitali, prevenendo e contrastando "ogni forma di discriminazione e del bullismo, anche informatico" (Legge 107/2015, art. 1, c. 7, l), il nostro Istituto ha aderito già nel corso dell'anno 2018 al progetto "Generazioni Connesse".

Alcuni docenti, oltre al docente referente del Bullismo e Cyberbullismo, hanno proseguito la formazione anche mediante la piattaforma Elisa ed altri canali.

L' Animatore Digitale ha predisposto corsi di formazione, progettati sulla base dei bisogni formativi dei docenti, relativi all'uso del registro elettronico, all'utilizzo di metodologie multimediali nella didattica quotidiana e soluzioni alternative di didattica a distanza, anche al fine di affinare le competenze richieste dalla DaD e dalla DDI.

Nell'ottica di una formazione continua in linea con i progressi e le innovazioni tecnologiche, il nostro Istituto riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola, dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti, anche online, purché restino coerenti con il piano di formazione.

---

## ***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.

La scuola, in realtà, ha già individuato e formato un gruppo di docenti tra i quali l'Animatore Digitale che accompagna il Dirigente Scolastico e il DSGA nell'attuazione degli obiettivi e delle innovazioni previste dal PNSD.

Anche attraverso il già presente Gruppo Digitale, pertanto:

- attua la formazione dei docenti all'uso corretto del registro elettronico e dello scrutinio elettronico
- attua la formazione volta allo sviluppo e alla diffusione del pensiero

computazionale

- attua la formazione sull'uso delle tecnologie nella didattica
  - si assicura che il personale conosca la normativa sulla privacy
  - offre una formazione/aggiornamento in materia di sicurezza on-line
  - realizza la ricognizione e messa a punto delle dotazioni digitali
  - monitora il piano digitale d'Istituto ed i risultati conseguiti.
- 

## ***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.

L'Istituto, secondo quanto disposto dall'art. 5 - comma 2 - della legge 29 maggio 2017 n. 71, integra il Regolamento d'Istituto e il Patto di Corresponsabilità Educativa con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti, al fine di meglio regolamentare l'insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione al fenomeno.

Il Patto di corresponsabilità ((DPR 24 giugno 1998, n. 249, modificato dal DPR n. 235 del 21 novembre 2007-art. 5-bis) è aggiornato secondo le Linee di indirizzo "Partecipazione dei genitori e corresponsabilità educativa" al fine di informare e rendere partecipi le famiglie sul percorso intrapreso con il documento e-policy e il piano d'azione. A tal fine vengono anche:

- elaborate regole sull'uso delle tecnologie digitali da parte dei genitori nelle comunicazioni con la scuola e con i docenti,
- forniti consigli e/o linee guida sull'uso delle tecnologie digitali nella comunicazione

con i figli.

Mediante incontri periodici (Consigli di Classe/Interclasse):

- comunica alle famiglie l'attivazione di progetti/laboratori intrapresi per la formazione degli alunni

- diffonde informazioni sui siti nazionali di sostegno, tra i quali il sito [www.generazioniconnesse.it](http://www.generazioniconnesse.it)

Il nostro istituto, inoltre, in questi ultimi anni ha organizzato incontri con enti esterni, come la Polizia Postale, per sensibilizzare docenti, alunni e genitori sui temi della sicurezza online.

Altresì con l'uso diffuso del registro elettronico e della piattaforma Gsuite for education, sono stati elaborati e diffusi i regolamenti concernenti l'utilizzo dei dispositivi digitali e i regolamenti disciplinari con le sanzioni ammesse.

Per i prossimi anni prevede ulteriori incontri con esperti esterni (polizia, associazioni, ...) e l'organizzazione di percorsi di sensibilizzazione e formazione dei genitori su un uso responsabile e costruttivo della Rete in famiglia e a scuola.

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

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

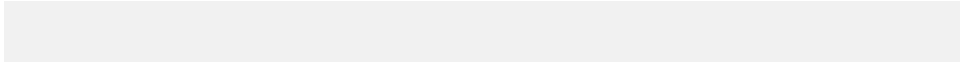
**Scegliere almeno 1 di queste azioni**

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica, sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

### **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
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'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.

Il nostro Istituto, avvalendosi anche della figura del Responsabile della protezione dei dati (R.P.D./D.P.O.), redige l'Informativa Generale sul trattamento dei dati personali ai sensi degli Artt. 13 e 14 del Regolamento UE 2016/679 (GDPR) e fornisce a ciascun utente informazioni relative alle modalità con le quali vengono trattati i dati e quali diritti può esercitare l'interessato rispetto ad ogni trattamento.

Ciascuna Informativa Generale viene integrata, caso per caso, da altre Informative Specifiche.

I dati personali vengono trattati ispirandosi ai seguenti principi generali: necessità, finalità, liceità, correttezza e lealtà, sicurezza e protezione.

A garanzia della riservatezza dei dati sono applicate misure adeguate di sicurezza organizzativa ed informatica evidenziate nel "Documento delle misure a tutela dei dati delle persone" elaborato dall'Istituto Scolastico con riferimento esplicito alle regole tecniche in materia di conservazione digitale degli atti, definite dall'Agenzia per l'Italia Digitale (Ag.I.D.).

Tra i punti da soddisfare per rendere compliant ogni Istituto Scolastico al Regolamento UE 2016/679, la nostra scuola:

- redige un registro dei trattamenti dei dati, depositato in segreteria, sia per il titolare che per il responsabile dei trattamenti,
- predispone una lettera di incarico per il trattamento dei dati al personale ATA, ai collaboratori scolastici e ai docenti all'inizio del rapporto di lavoro,
- adotta misure tecniche ed organizzative per garantire la sicurezza dei trattamenti:
  - ha effettuato la migrazione del sito da suffissi gov.it a suffissi edu.it
  - utilizza il protocollo HTTPS per la comunicazione su Internet
  - possiede un sistema di backup e un piano di disaster recovery
  - ha realizzato un sito web secondo i protocolli di privacy by default e by design.

Relativamente alla sicurezza della intranet scolastica, l'Istituto si avvale di un gestore della rete, AFA System, che si occupa - attraverso il proprio sistema Majornet - di controllare il traffico con sistemi di controllo e limitazioni di accesso alla rete tramite una blacklist, firewall e registro dei log di accesso.



## 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.

Per garantire il diritto di accesso a Internet in tutte le sezioni e classi, dalla scuola dell'infanzia alla scuola secondaria di primo grado, il nostro Istituto è provvisto di una rete Wi-fi adeguata al numero di studenti e in grado di supportare il traffico dati generato dal numero di utenti. Dispone, inoltre, di fibra ottica, soluzioni cloud e cablaggio LAN.

La scuola, per le attività da svolgere nel contesto extra-scolastico, mette anche a

disposizione degli alunni della scuola primaria e secondaria di primo grado, che ne avessero reali necessità, tablet e notebook per la didattica a distanza in regime di comodato d'uso gratuito.

In riferimento alla sicurezza dell'ambiente digitale ed alla manutenzione del sistema di accesso, si avvale di un gestore della rete, AFA System, che si occupa - attraverso il proprio sistema Majornet - di controllare il traffico con sistemi di controllo e limitazioni di accesso alla rete tramite una blacklist, firewall e registro dei log di accesso; relativamente agli aspetti legali, in relazione prevalentemente alla privacy, si avvale della figura del Responsabile della protezione dei dati (R.P.D./D.P.O.)

L'Istituto, inoltre, dispone di un Regolamento sull'uso delle TIC.

---

## ***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.

La scuola utilizza diversi strumenti di comunicazione sia per valorizzare e promuovere le attività portate avanti dall'Istituto, sia per far circolare al suo interno informazioni di servizio o contenuti importanti tra i diversi attori scolastici (docenti, studenti, genitori, ...).

Tra gli strumenti di comunicazione esterna c'è in primis il sito web, tramite il quale l'Istituto trasmette la sua identità, i suoi valori, le sue azioni, i progetti e l'idea di educazione che porta avanti.

Tra gli strumenti di comunicazione interna, invece, ci sono l'e-mail istituzionale, una piattaforma web professionale di comunicazione, le piattaforme di lavoro condiviso e collaborativo come classroom, google doc con gli strumenti di google workspace e, non ultimo, il registro elettronico - che permette di gestire la comunicazione con le famiglie in merito all'andamento scolastico, ai risultati scolastici, a comunicazioni varie.

---

## **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.

Come da Regolamento d'Istituto è vietato l'uso del cellulare all'interno della scuola. Altri strumenti possono essere utilizzati solo ed esclusivamente per uso didattico/scolastico.

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

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

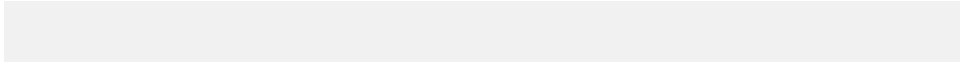
##### **Scegliere almeno 1 di queste azioni:**

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

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

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

- Organizzare uno o più eventi o attività volti a formare il personale dell'Istituto, gli studenti e le studentesse 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.

La nostra scuola già da qualche anno attua interventi di sensibilizzazione e prevenzione universale mediante il progetto d'Istituto "GENERAZIONI CONNESSE: Bullismo e Cyberbullismo" che integra l'offerta formativa. Per suo tramite essa forma e consolida le competenze educative di base necessarie per poter gestire le situazioni di vita che i ragazzi sperimentano online: li informa sui vari rischi online cui possono

incorrere e su quali sono i comportamenti più corretti da adottare. In particolare il progetto vuole rendere i ragazzi consapevoli circa un determinato problema che potrebbe presentarsi nel gruppo, incoraggiarli ad adottare comportamenti più funzionali, favorire la diffusione di informazioni utili alla collettività. Nel contempo promuove competenze digitali al fine di ridurre i rischi per la loro sicurezza.

Non sono previsti ancora interventi di prevenzione selettiva e prevenzione indicata poiché, al momento, non risultano gruppi di studenti in cui è presente il rischio on-line o casi specifici.

---

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

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

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

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

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

del [cyberbullismo](#). A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.

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

Il nostro Istituto, mediante il progetto "GENERAZIONI CONNESSE: Bullismo e Cyberbullismo" tratta ampiamente il problema, rendendo gli alunni consapevoli in merito a cos'è il cyberbullismo, quali sono le sue caratteristiche, la suddivisione nei due grandi gruppi, come riconoscerlo, le responsabilità civili e penali di chi compie atti di bullismo e cyberbullismo, le responsabilità che ricadono su ragazzi e ragazze, genitori e docenti. Destinatari del progetto sono gli alunni di tutte le classi della scuola primaria e secondaria di primo grado, con declinazione diversa delle priorità tra i diversi cicli. Gli obiettivi del progetto vengono raggiunti mediante una serie di attività/azioni che vanno dalla semplice conversazione, alla visione e analisi di filmati - compresi i video di Generazioni Connesse, alla lettura di testi, a giochi di ruolo, agli incontri con la Polizia Postale.

Nel contempo la scuola promuove lo sviluppo di competenze digitali e l'assunzione di ruolo attivo degli studenti, la formazione del personale scolastico.

L'Istituto ha provveduto dall'anno scolastico 2017/18 alla nomina del Referente per le iniziative di prevenzione e contrasto, a munirsi di un documento e-policy, ad integrare il Regolamento d'Istituto ed il Patto di Corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari.

---

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

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

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

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui

spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;

- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

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

La prevenzione dell'hate speech è legata indissolubilmente all'educazione e alla sensibilizzazione alla diversità, da attuarsi all'interno della comunità educante.

Il PTOF della nostra scuola prevede anche l'Educazione alle pari opportunità e prevenzione della violenza di genere. Nella macro area dei Bisogni Educativi Speciali si cita: "L'Istituto si propone di potenziare la cultura dell'inclusione per rispondere in modo efficace alle necessità di ogni alunno ... Obiettivo principale è la riduzione delle barriere che limitano l'apprendimento e la partecipazione sociale ... Obiettivo dell'integrazione è la progettazione per acquisire non solo gli obiettivi didattici, ma anche, e soprattutto, abilità che migliorino, in modo reale, le azioni quotidiane e la qualità della vita attraverso un costante utilizzo di ecosistemi relazionali.

Vengono privilegiate attività formative per favorire l'acquisizione della conoscenza di sé, per la costruzione di una propria identità e per favorire rapporti relazionali positivi.

A tal fine la scuola si organizza per creare un ambiente accogliente e inclusivo, ..., promuovere l'attiva partecipazione di tutti gli alunni al processo di apprendimento, ..., favorire l'acquisizione di competenze collaborative, promuovere culture e pratiche inclusive attraverso una più stretta collaborazione fra tutte le componenti della comunità educante ...".

Per quanto sopraesposto, il progetto d'Istituto "Generazioni connesse: bullismo e cyberbullismo" si prefigge, tra le altre, le seguenti finalità:

- Promuovere il benessere a scuola.
- Educare i ragazzi a modalità relazionali sane e serene.
- Promuovere lo sviluppo di comportamenti positivi ispirati all'utilizzo di buone pratiche legate al rispetto delle regole, di se stessi e del prossimo, con particolare riferimento all'inclusione scolastica degli alunni con disabilità, all'Intercultura, alla dispersione scolastica.
- Prevenire comportamenti di prepotenza e di vittimismo tra i bambini.
- Prevenire ogni forma di discriminazione e del bullismo, anche informatico.
- Educare alla cittadinanza digitale riflettendo sulla propria identità e sulla partecipazione responsabile nella comunità ampia del web.



## **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?*

Le tecnologie digitali rappresentano una possibilità di espressione dell'identità individuale ma anche un potenziale rischio, per questo si rende necessaria una formazione - per il loro uso corretto - attinente non solo ai contenuti ma anche ai tempi e all'utilizzo.

La nostra scuola promuove azioni di prevenzione alla dipendenza da Internet e gioco online mediante:

- l'integrazione della tecnologia nella didattica, al fine di evidenziarne il suo utilizzo funzionale e rendere, così, i ragazzi più consapevoli delle proprie abitudini online,
- momenti di riflessione comune che mettono in risalto la tecnologia come strumento per raggiungere i propri obiettivi e non solo come strumento di distrazione o addirittura di ostacolo,
- lo sviluppo di conoscenze e competenze riferite al mondo del web e della comprensione dei rischi personali legati al suo utilizzo scorretto.

---

## **4.5 - Sexting**

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

Oltre a quanto detto relativamente alle altre problematiche connesse all'uso scorretto delle tecnologie digitali: integrazione nella didattica, sviluppo di conoscenze e competenze, ..., nel curriculum della nostra scuola sono previste attività trasversali, relative all'educazione all'affettività e alle differenze di genere, che vengono realizzate

anche mediante progetti diversificati.

---

## **4.6 - Adescamento online**

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

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

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

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

Al fine di rendere i ragazzi più sicuri e pronti ad affrontare eventuali situazioni a rischio, la nostra scuola si prefigge di accompagnarli in due percorsi paralleli: da un lato un percorso di educazione all'affettività e alla sessualità affinché imparino a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri; dall'altro un percorso di educazione digitale che comprenda lo sviluppo di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online. Importante è il ruolo degli adulti - genitori e/o insegnanti - che devono essere un punto di riferimento, ispirare fiducia, affinché i ragazzi si sentano ascoltati, compresi, non giudicati. Trattandosi di una problematica molto delicata da gestire e con possibili ripercussioni psicologiche significative, l'esistenza di casi reali comporterebbe l'intervento della Polizia Postale e di un Servizio territoriale.

---

## 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.**

Anche relativamente al problema della pedopornografia, la scuola evidenzia l'importanza:

- di un percorso di educazione all'affettività, a modalità relazionali sane e serene, alla cittadinanza digitale che consenta riflessioni sulla propria identità e sulla partecipazione responsabile nella comunità del web,
- del ruolo dell'adulto quale punto di riferimento.

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

**AZIONI (da sviluppare nell'arco dell'anno scolastico).****Scegliere almeno 1 di queste azioni:**

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

**AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).****Scegliere almeno 1 di queste azioni:**

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

# Capitolo 5 - Segnalazione e gestione dei casi

---

## 5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

segnalare la presenza di materiale pedopornografico online.

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

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

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

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

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

Per tutti i dettagli 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).

### **5.3. - Gli attori sul territorio**

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

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

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

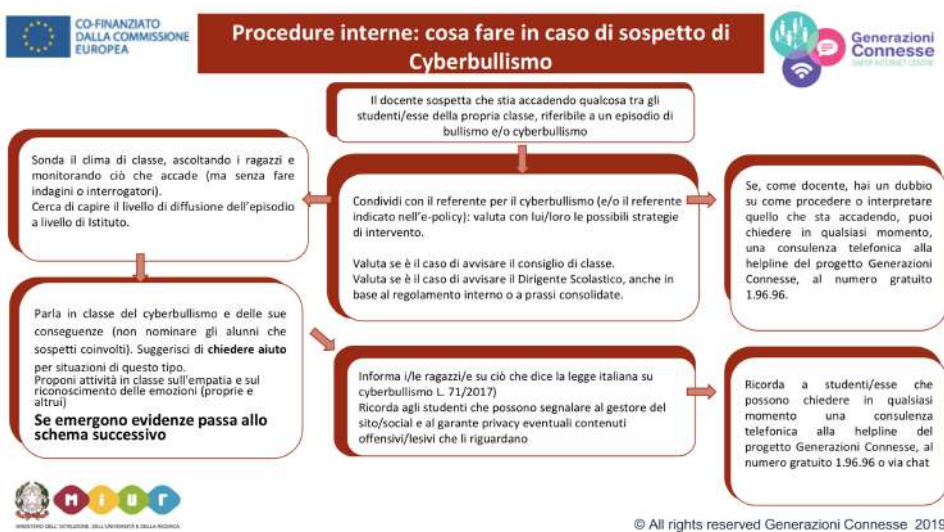
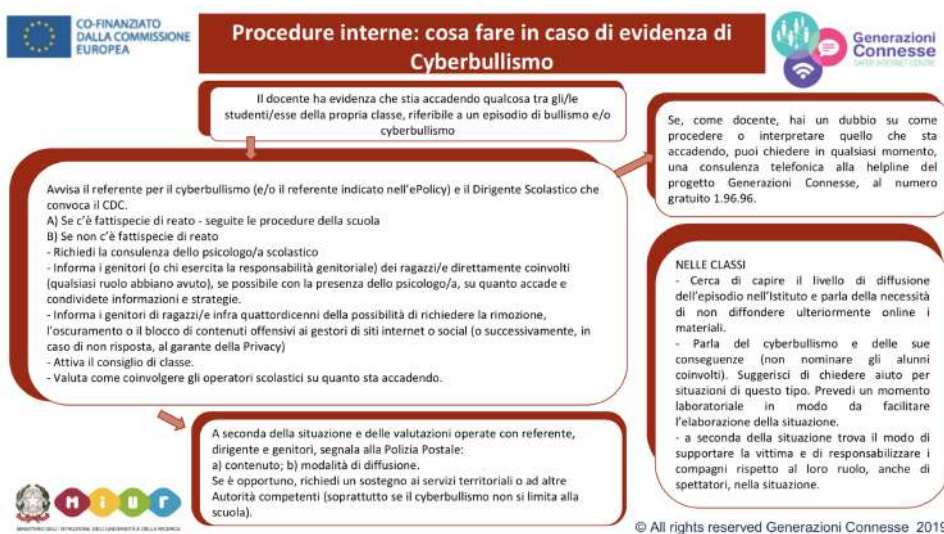
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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



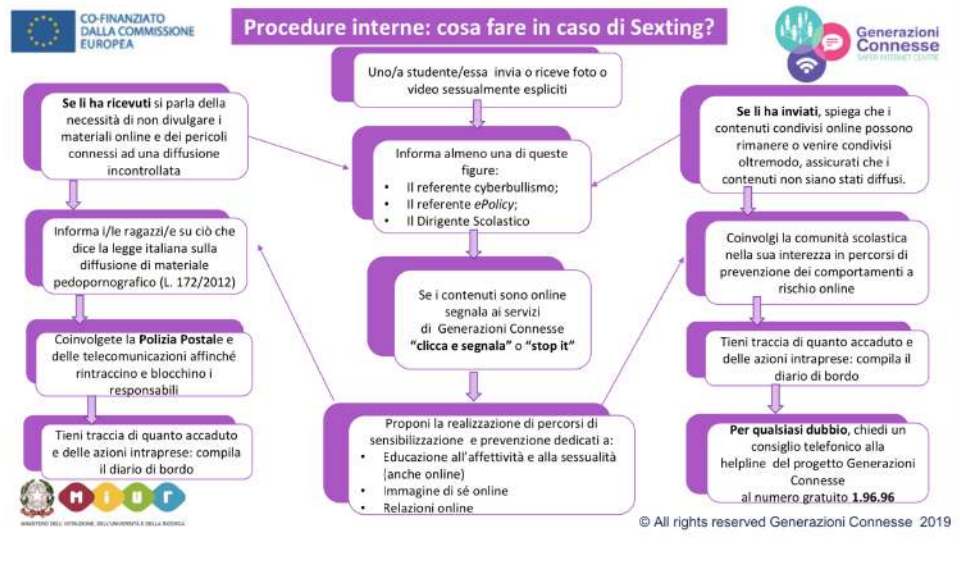
- **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

## 5.4. - Allegati con le procedure

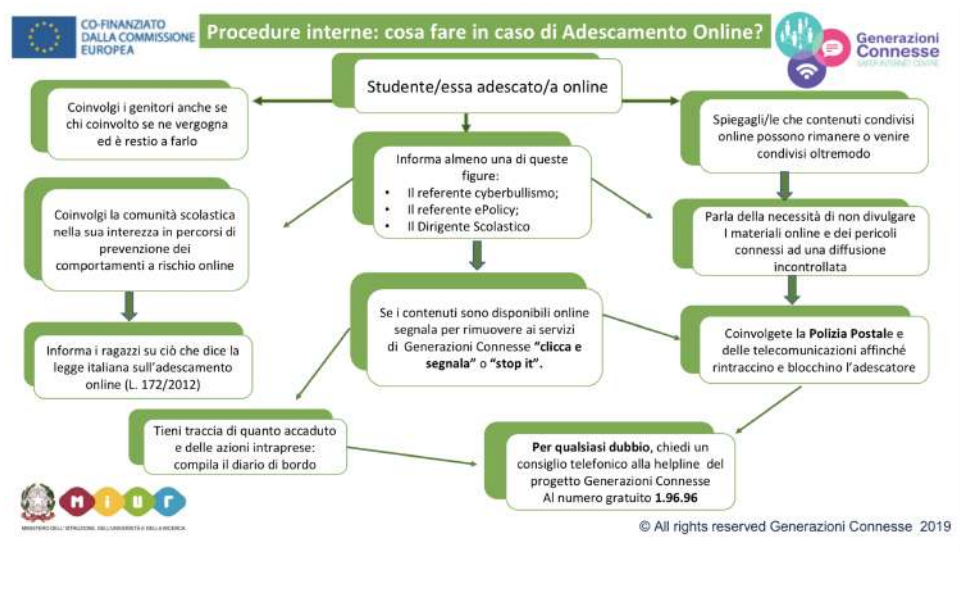
### Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



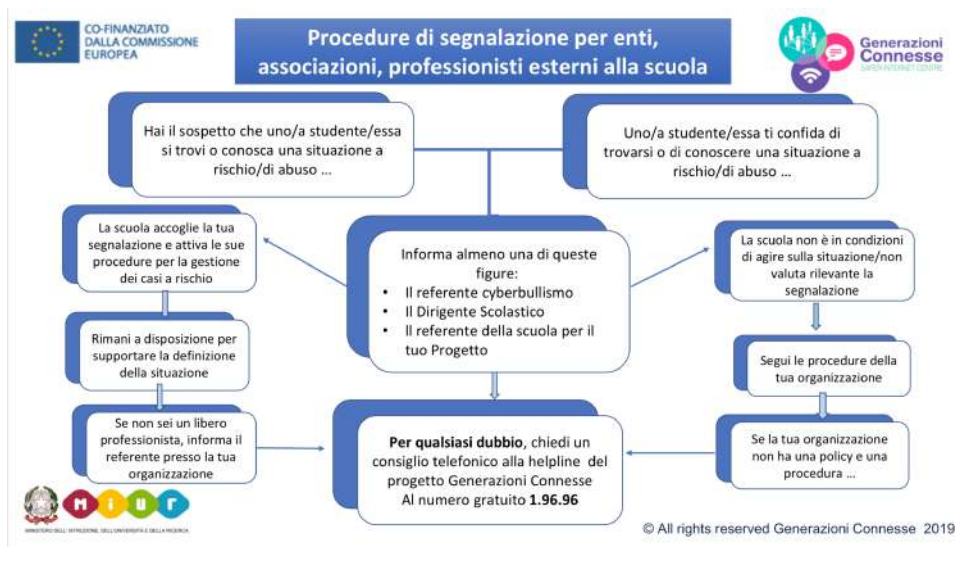
### Procedure interne: cosa fare in caso di sexting?



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



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



## Altri allegati

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

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

**Non è prevista nessuna azione.**

