



# Documento di ePolicy

BGIC88700C

VERDELLO "DON MILANI"

VIA DON GIAVAZZI 26 - 24049 - VERDELLO - BERGAMO (BG)

GUELI ANGELO

# Capitolo 1 - Introduzione al documento di ePolicy

---

## 1.1 - Scopo dell'ePolicy

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

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

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

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

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

## Argomenti del Documento

### 1. Presentazione dell'ePolicy

1. Scopo dell'ePolicy
2. Ruoli e responsabilità
3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
5. Gestione delle infrazioni alla ePolicy
6. Integrazione dell'ePolicy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

### 2. Formazione e curriculum

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

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

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

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

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

### 5. Segnalazione e gestione dei casi

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

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

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

all'uso di Internet.

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

L'Istituto Comprensivo di Verdello ha redatto nell'anno scolastico 2020-2021 la seguente epolicy in conformità con le "Le linee di orientamento per azioni di prevenzione e di contrasto al bullismo e Cyberbullismo" emanate dal MIUR in collaborazione con il Safer Internet Center (SIC) per l'Italia, progetto co-finanziato dalla Commissione Europea nell'ambito del programma "Connetting Europe Facility" ( CEF)- Telecom, con l'obiettivo di diffondere campagne di sensibilizzazione, promuovere azioni, risorse e servizi per un uso consapevole e responsabile delle tecnologie digitali e per la segnalazione delle problematiche connesse.

Il presente Documento è parte integrante del PTOF e le azioni sottoscritte costituiscono indicazioni e buone prassi di azione e prevenzione in materia di bullismo e cyberbullismo.

---

## ***1.2 - Ruoli e responsabilità***

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

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

### **IL DIRIGENTE SCOLASTICO**

- promuove iniziative atte alla diffusione delle competenze digitali nell'Istituto
- è garante della sicurezza, anche online, di tutti i membri della comunità scolastica
- promuove la cultura della sicurezza online attivando, con la collaborazione del Referente di Istituto per il bullismo /cyberbullismo, percorsi di formazione per la sicurezza e le problematiche connesse all'utilizzo della RETE sia online che offline
- garantisce l'esistenza di un sistema/protocollo per il monitoraggio della

sicurezza online

- gestisce e interviene nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali da parte degli studenti e delle studentesse.

### **L'ANIMATORE DIGITALE**

- supporta il personale scolastico da un punto di vista informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali
- promuove percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale"
- monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola

### **IL REFERENTE BULLISMO E CYBERBULLISMO**

- coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e cyberbullismo, avvalendosi anche delle Forze di Polizia, delle associazioni e degli enti territoriali
- promuove percorsi formativi per studenti, docenti e genitori sulle problematiche del bullismo e cyberbullismo

### **I DOCENTI**

- integrano parti del curricolo disciplinare con approfondimenti sull'uso responsabile delle TIC e della rete servendosi delle tecnologie digitali nella didattica (LIM o altri dispositivi tecnologici)
- sviluppano le competenze digitali degli allievi facendo sì che gli stessi conoscano e seguano le norme di sicurezza nell'utilizzo del web sia per attività in presenza sia per attività didattiche extracurricolari
- segnalano prontamente alle famiglie eventuali problematiche emerse in classe nell'utilizzo del digitale e stabiliscono linee comuni di intervento educativo
- segnalano al Dirigente scolastico e ai suoi collaboratori qualunque violazione, anche online, del Regolamento di Istituto secondo la procedura stabilita

### **IL PERSONALE ATA**

- svolge funzioni di tipo amministrativo, contabile, gestionale e di sorveglianza, connesse alle attività dell'Istituzione scolastica, in collaborazione con il Dirigente scolastico e con il personale docente tutto

- controlla che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti
- segnala al Dirigente scolastico e ai suoi collaboratori comportamenti non adeguati e/o episodi di bullismo/cyberbullismo
- collabora nel reperire, verificare e valutare informazioni inerenti possibili casi di bullismo/cyberbullismo

## **STUDENTI E STUDENTESSE**

- partecipano alle iniziative di sensibilizzazione e formazione organizzate dall'Istituto sull'uso consapevole delle TIC e della RETE
- adottano le regole di e-safety per evitare situazioni di rischio per sé e per gli altri
- rispettano le norme che disciplinano l'uso corretto e responsabile delle tecnologie digitali, come indicato nel Regolamento di Istituto.

## **I GENITORI**

- partecipano alle iniziative di sensibilizzazione e formazione organizzate dall'Istituto sull'uso consapevole delle TIC e della RETE, nonché sull'uso responsabile dei device personali
- condividono con i docenti le linee educative relative alle TIC e alla RETE, al Regolamento di Istituto e al patto di corresponsabilità educativa
- accettano e condividono il documento di e-Policy dell'Istituto
- collaborano con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite.

## **GLI ENTI EDUCATIVI ESTERNI E LE ASSOCIAZIONI**

- osservano le politiche interne sull'uso consapevole della Rete e delle TIC
- attivano procedure e comportamenti sicuri per la protezione degli studenti e delle studentesse durante le attività che vengono svolte all'interno della scuola o in cui sono impegnati gli stessi.

Per quanto non espressamente indicato sui ruoli e sulle responsabilità delle figure presenti all'interno dell'Istituzione scolastica, si rimanda: all'art. 21, comma 8, Legge 15 marzo 1997, n. 59; all'art. 25 della Legge 30 marzo 2001, n. 165; al CCNL in vigore; al D.P.R. 8 marzo 1999, n. 275; alla Legge 13 luglio 2015, n. 107; al Piano Nazionale Scuola Digitale; a quanto stabilito in materia di culpa in vigilando, culpa in organizzando, culpa in educando.

---

## ***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).

### **Ambiti di applicazione, attività e ruoli**

Le attività progettuali o di formazione a carattere seminariale, devono essere preventivamente autorizzate dal Dirigente scolastico, con modalità e tempi concordati; a tal proposito, al fine di verificare preventivamente il contenuto da somministrare o dibattere con la scolaresca, i soggetti esterni forniranno un programma delle attività con narrazione sintetica della scaletta al fine di essere autorizzato dalla Dirigenza.

Condivisione della E-policy d'istituto in forma sintetica dagli operatori ed associazioni esterne preliminarmente all'inizio delle attività con gli studenti e studentesse (per progetti semestrali/annuali che prevedano l'utilizzo delle TIC).

---

## ***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 del documento e-Policy alla Comunità scolastica ed ai genitori degli studenti e delle studentesse:**

Le norme adottate e sottoscritte dalla scuola in materia di sicurezza ed utilizzo delle tecnologie digitali, saranno rese note tramite pubblicazione del presente documento sul sito web della scuola.

### **CONDIVISIONE E COMUNICAZIONE DELLA E-POLICY AGLI STUDENTI E ALLE STUDENTESSE**

- all'inizio dell'anno, in occasione dell'illustrazione del Regolamento di Istituto agli alunni da parte dei docenti, verrà presentata la e-policy insieme ai regolamenti correlati e al patto di corresponsabilità con modalità diverse in base all'ordine di scuola
- tutti gli alunni saranno informati che la rete, l'uso di internet e di ogni dispositivo digitale saranno controllati dai docenti e utilizzati solo con la loro autorizzazione e supervisione
- 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, con specifico riferimento al contrasto di ogni forma di

cyberbullismo.

### **CONDIVISIONE E COMUNICAZIONE DELLA EPOLICY AL PERSONALE SCOLASTICO**

- le norme adottate dalla scuola in materia di sicurezza dell'uso del digitale saranno discusse dagli organi collegiali e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito istituzionale
- il personale scolastico riceverà un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso materiali resi disponibili anche sul sito istituzionale nonché mediante la partecipazione a incontri formativi organizzati dall'Istituto
- 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**

- sarà favorito un approccio collaborativo nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione di incontri scuola- famiglia assembleari, collegiali e individuali
- al fine di sensibilizzare le famiglie sui temi dell'uso delle TIC saranno organizzati incontri informativi per presentare e condividere la presente e-policy.

La ePolicy, redatta dalla Commissione bullismo/cyberbullismo e approvata dal collegio Docenti e dal Consiglio di Istituto, sarà inserita all'interno del PTOF.

---

## ***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.

### **DISCIPLINA DEGLI ALUNNI**

Le potenziali infrazioni in cui potrebbero incorrere gli alunni, relativamente alla fascia di età considerata, nell'utilizzo delle tecnologie digitali e di internet durante la didattica sono le seguenti:

- uso della RETE per giudicare, infastidire, offendere, denigrare, impedire a qualcuno di esprimersi o partecipare, esprimersi in modo volgare usando il turpiloquio
- invio incauto o senza permesso di foto o altri dati personali (indirizzo di casa, numero di telefono)
- condivisione online di immagini o video di compagni/e e del personale scolastico senza il loro esplicito consenso o che li ritraggono con intento offensivo e denigratorio
- condivisione di immagini intime e a sfondo sessuale
- invio di immagini o video volti all'esclusione di compagni/e comunicazione incauta e senza permesso con sconosciuti collegamenti a siti web non adeguati e non indicati dai docenti.

L'azione educativa prevista per gli alunni è rapportata alla fascia di età e al livello di sviluppo e maturazione personale. Infatti in alcuni casi i comportamenti sanzionabili sono 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.

Pertanto sono previsti interventi graduali in base all'età e alla gravità delle violazioni:

- richiamo verbale
- richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante)
- richiamo scritto con annotazione sul registro elettronico
- convocazione dei genitori da parte dell'insegnante
- convocazione dei genitori da parte del Dirigente Scolastico.

Contestualmente 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.

E' inoltre importante intervenire su tutto il contesto classe con attività specifiche educative e di sensibilizzazione.

Si fa riferimento al documento Integrazione-Regolamento Disciplinare-DAD pubblicato nell'area del sito web della scuola : Regolamenti d'Istituto.

## **DISCIPLINA DEL PERSONALE SCOLASTICO**

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 allievi:

- utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni,

non connesso alle attività di docenza o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiale non idoneo

- utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale
- trattamento dei dati personali e dei dati sensibili degli alunni non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi
- diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi
- carente istruzione preventiva degli alunni sull'uso corretto e responsabile delle TIC e di internet
- vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili rischi connessi
- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

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

## **DISCIPLINA DEI GENITORI**

In considerazione dell'età degli studenti e delle studentesse e della loro dipendenza dagli adulti, anche talune condizioni e condotte dei genitori medesimi possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli allievi a scuola, 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:

- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non corre rischi
- una posizione del computer in una stanza o in una posizione non visibile e controllabile dall'adulto
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'uso di cellulare o smartphone
- un utilizzo del pc in comune con gli adulti che possono conservare in memoria

materiali non idonei a minori

- un utilizzo di cellulari e smartphone in comune con gli adulti che possono conservare in memoria indirizzi di siti o contenuti non idonei a minori.

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sè 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.

La e-Policy è coerente con quanto stabilito nei Regolamenti vigenti e nel Patto di corresponsabilità.

---

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

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

Il monitoraggio e la revisione della e-Policy sarà svolta annualmente e /o qualora si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno dell'Istituto.

L'aggiornamento del documento di e-Policy sarà curato dal docente Referente di

Istituto per la prevenzione e il contrasto del bullismo e cyberbullismo, in qualità di coordinatore del gruppo di lavoro del presente documento e, ove possibile, con la partecipazione dell'Animatore digitale.

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

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

- Organizzare una o più attività volte alla raccolta di problematiche sull'utilizzo delle TIC da parte dei docenti e alunni per la stesura finale dell'ePolicy.
- Organizzare un evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti (collegio docenti unitario)

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

- Organizzare un'attività volta per l'aggiornamento dell'ePolicy con i docenti
- Pianificare incontri per la sensibilizzazione e la partecipazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Utilizzare le risorse del progetto Generazioni Connesse
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori con il contributo degli alunni.

# 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.

Le finalità formative delle TIC possono essere sintetizzate nei seguenti punti:

- Favorire la conoscenza dello strumento pc e/o tablet a scopo didattico.
- Sostenere l'alfabetizzazione informatica.
- Favorire la trasversalità delle discipline.
- Facilitare il processo di apprendimento.
- Favorire il processo di inclusione.
- Fornire nuovi strumenti a supporto dell'attività didattica.
- Promuovere situazioni collaborative di lavoro e di studio.

- Sviluppare creatività e capacità di lavorare in gruppo.
- Promuovere azioni di cittadinanza attiva.
- Utilizzare in modo critico, consapevole e collaborativo la tecnologia.

### **Competenze digitali declinate secondo le cinque aree del quadro di riferimento DIGCOM**

#### **(Quadro comune di riferimento europeo per le competenze digitali):**

1. **INFORMAZIONE:** identificare, localizzare, recuperare, conservare, organizzare e analizzare le informazioni digitali, giudicare la loro importanza e lo scopo;
2. **COMUNICAZIONE:** comunicare in ambienti digitali, condividere risorse attraverso strumenti on-line, collegarsi con gli altri e collaborare attraverso strumenti digitali, interagire e partecipare alle comunità e alle reti;
3. **CREAZIONE DI CONTENUTI:** creare e modificare nuovi contenuti (da elaborazione testi a immagini e video); integrare e rielaborare le conoscenze ed i contenuti; produrre espressioni creative, contenuti media e programmare; conoscere e applicare i diritti di proprietà intellettuale e le licenze;
4. **SICUREZZA:** protezione personale, protezione dei dati, protezione dell'identità digitale, misure di sicurezza, uso sicuro e sostenibile;
5. **PROBLEM-SOLVING:** identificare i bisogni e le risorse digitali, valutare appropriati strumenti digitali secondo lo scopo o necessità, risolvere problemi concettuali attraverso i mezzi digitali, utilizzare creativamente le tecnologie, risolvere problemi tecnici, aggiornare la propria competenza e quella altrui.

### **COMPETENZA DIGITALE**

#### **TRAGUARDI PER LO SVILUPPO DELLE COMPETENZE**

##### **Al termine della Scuola dell'Infanzia**

- Comunica e si esprime con una pluralità di linguaggi, avvalendosi anche della strumentazione tecnologica
- Orientarsi, con la guida dell'insegnante, nel mondo delle tecnologie.

##### **Al termine della Scuola Primaria**

- Si orienta tra i diversi mezzi di comunicazione ed è in grado di farne un uso

adeguato a seconda delle diverse situazioni.

- Produce semplici modelli o rappresentazioni grafiche del proprio operato utilizzando elementi del disegno tecnico o strumenti multimediali.
- Inizia a riconoscere in modo critico le caratteristiche, le funzioni e i limiti della tecnologia attuale.
- Sa affrontare e trovare soluzioni complesse attraverso l'identificazione di soluzioni più semplici.

### **Al termine della Scuola Secondaria di I grado**

- È in grado di cercare, selezionare e valutare le informazioni in rete, anche nel confronto con altre fonti.
- E' consapevole della distinzione tra identità digitale e identità reale
- E' in grado di applicare responsabilmente le regole sulla privacy tutelando la propria e quella altrui.
- È in grado di argomentare attraverso diversi sistemi di comunicazione.
- E' consapevole dei rischi della rete e utilizza gli strumenti necessari ad individuarli e limitarne gli effetti.
- E' responsabile nell'uso dei mezzi per non nuocere a se stesso e agli altri (netiquette).

## **COMPETENZE SPECIFICHE**

### **Scuola dell'Infanzia**

- primo approccio al coding unplugged
- utilizzare strumenti informatici in situazioni di gioco e/o come supporto didattico
- utilizzare le TIC per produrre, rivedere e documentare il proprio lavoro.

### **Scuola Primaria**

#### **Classe terza**

- utilizzare il computer in un contesto applicativo
- utilizzare strumenti informatici e di comunicazione in situazioni significative di gioco e come supporto didattico
- utilizzare le TIC in modo creativo e funzionale allo studio, alla collaborazione e alla comunicazione
- saper riferire algoritmi per spiegare un percorso

#### **Classe quinta**

- utilizzare le TIC come strumento per produrre, rivedere e documentare il proprio lavoro
- recuperare e analizzare informazioni da canali diversi e da diversi siti sicuri

- usare comandi/simboli/algoritmi e funzioni.

### **Scuola secondaria di I grado**

- Usare la rete Internet per reperire e selezionare informazioni utili
- Accostarsi a nuove applicazioni informatiche esplorandone le funzioni e le potenzialità
- Usare comandi/simboli/algoritmi e funzioni per programmare un comportamento desiderato, anche di robot.
- Conoscere le proprietà e le caratteristiche dei diversi mezzi di comunicazione ed essere in grado di farne un uso efficace e responsabile rispetto alle proprie necessità di studio e socializzazione collaborando con altri

### **ABILITA'**

#### **Scuola dell'Infanzia**

- utilizzare, con la supervisione dell'insegnante, alcune TIC per documentare un'esperienza vissuta, per fare ricerca, per conoscere
- utilizzare il reticolo del coding unplugged con l'ausilio di frecce direzionali per compiere percorsi, dare spiegazioni, dare indicazioni ai compagni e per raggiungere un obiettivo
- uso essenziale della piattaforma Google WS

#### **Scuola Primaria**

##### **Classe terza**

- usare in modo guidato i giochi didattici multimediali
- usare semplici programmi grafici per disegnare e colorare
- sapersi orientare tra gli elementi principali del computer o altri tipi di device e le loro funzioni
- saper utilizzare gli elementi per immettere dati, stampare e salvare un documento
- saper verbalizzare un percorso da compiere
- saper usare l'ambiente di Google WS

##### **Classe quinta**

- Saper utilizzare dispositivi per archiviare dati
- Archiviare documenti in cloud
- Saper usare programmi didattici presenti sui device
- Saper trovare informazioni su internet a scopi didattici
- Convertire movimenti in istruzioni simboliche
- Costruire ed elaborare tabelle di dati
- Formattare testi scritti inserendo elementi grafici
- Utilizzare la rete per inviare e-mail legate ad attività didattiche in ambiente Google WS

- Creare artefatti digitali utilizzando semplici applicativi
- Usare i principali applicativi di Google WS
- Utilizzare la rete in modo consapevole attuando comportamenti preventivi.

### **Scuola Secondaria di I grado**

- Utilizzare le tecnologie dell'Informazione e della Comunicazione per elaborare dati, testi, immagini, per produrre artefatti digitali in diversi contesti e per la comunicazione.
- Ricercare informazioni in rete per integrare gli apprendimenti.
- Utilizzare strumenti informatici per sviluppare abilità computazionale facendo ricorso anche al coding (programmazione di robot, app, rappresentazioni 3D)
- Comunicare attraverso strumenti online partecipando alle reti di comunità rispettando la netiquette
- Utilizzare modalità di comportamento consone ai regolamenti d'istituto.

## **CONOSCENZE**

### **Scuola dell'Infanzia**

- reticolo e frecce direzionali per progettare e realizzare percorsi di coding unplugged
- Alcune strumentazioni tecnologiche e loro utilizzo.

### **Scuola Primaria**

#### **classe terza**

- Giochi didattici multimediali
- Principi d'uso dei più noti programmi grafici per disegnare e colorare
- Principali parti e funzioni del computer
- Funzionalità di programmi di videoscrittura con inserimento di tabelle e immagini
- concetto di algoritmo
- funzionalità di programmi inseriti in Google WS.

#### **classe quinta**

- Funzioni principali dei software più conosciuti: word, excel, power point o simili in GWS
- Concetto di funzione e variabile
- Fondamentali forme di utilizzo della rete per la ricerca di informazioni
- Forme di comunicazione attraverso la rete
- Semplici applicativi per la collaborazione e la produzione e condivisione di informazioni e conoscenze
- Principali rischi dell'utilizzo della rete con i diversi device.

### **Scuola Secondaria di I grado**

- I diversi applicativi per la collaborazione e la produzione e condivisione di informazioni e conoscenze.
- Le applicazioni tecnologiche per risolvere problemi.
- Netiquette e regolamenti.
- Le procedure di utilizzo sicuro e legale di reti informatiche per ricavare informazioni e comunicare.
- I rischi collegati ad un uso scorretto del web.

---

## ***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 Collegio docenti riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola, sia quelle liberamente scelte dai docenti (anche online) purché restino coerenti con il piano di formazione, come meglio indicato nel PTOF.

L'attenzione all'uso delle TIC nella didattica rende gli apprendimenti più motivanti, coinvolgenti ed inclusivi, con una funzione di guida da parte del docente; inoltre, permette di sviluppare capacità che sono sempre più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza ed il confronto fra pari in modalità asincrona.

La competenza digitale -oggi- è imprescindibile sia per i docenti sia per gli studenti e per le studentesse, e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa ed in grado di venire incontro ai nuovi stili di apprendimento.

---

## ***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.

I momenti di formazione ed aggiornamento sono dunque formulati secondo un'analisi del fabbisogno formativo del corpo docente sull'utilizzo ed integrazione delle TIC nella didattica e in base a contenuti scelti anno per anno in riferimento principalmente alle piattaforme d'Istituto e ai loro applicativi ( Google Ws, RE Axios, Microsoft 365).

---

## ***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.

Gli studenti e le studentesse devono attenersi a quanto previsto dai Regolamenti scolastici e dalle Circolari interne emanate dal Dirigente scolastico, sulla base delle note ministeriali sull'utilizzo consapevole delle tecnologie digitali all'interno del contesto scolastico.

I genitori, nell'azione di corresponsabilità didattico-educativa, rappresentano un punto di forza per l'implementazione dei rapporti "scuola-famiglia", quale garanzia e rispetto degli impegni, di natura anche pedagogica, sottoscritti e condivisi nello stesso Patto di corresponsabilità che andranno ripetutamente richiamati durante le assemblee di classe.

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

### **AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021)**

- 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 (classi quinte) 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.

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

- 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 consapevole e sicuro di Internet e delle tecnologie 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.

Nel nostro Istituto per adempiere alla normativa vigente in materia di esplicita autorizzazione all'atto di iscrizione alla suddetta scuola ai genitori viene consegnata l' INFORMATIVA PRIVACY AGLI ALLIEVI Redatta ai sensi degli Artt. da 13 a 15 del Regolamento U.E. 2016/679 (G.D.P.R.) con RICHIESTE DI MANIFESTAZIONE DEL CONSENSO AI SENSI DELL'ART. 7 DEL REGOLAMENTO U.E.

Il genitore deve sottoscrivere inoltre i suddetti documenti:

-RICHIESTE DI MANIFESTAZIONE DEL CONSENSO AI SENSI DELL'ART. 7 DEL  
REGOLAMENTO U.E. - INFORMATIVA PRIVACY AGLI ALLIEVI USO DI IMMAGINI

-RICHIESTE DI MANIFESTAZIONE DEL CONSENSO AI SENSI DELL'ART. 7 DEL  
REGOLAMENTO U.E. - INFORMATIVA PRIVACY AGLI ALLIEVI PER I SERVIZI A  
SUPPORTO DELL'INCLUSIONE SCOLASTICA

---

## **3.2 - Accesso ad Internet**

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

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre

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

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

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

L’accesso a Internet è possibile e consentito per la didattica in tutti i plessi attraverso la rete LAN e WiFi. L’accesso a Internet, attraverso i dispositivi della scuola o con dispositivo proprio da parte degli studenti, avviene solo in presenza dell’insegnante ed è consentito mediante registrazione del mac address del dispositivo.

I docenti possono accedere alla propria sezione del registro elettronico con credenziali personali. I computer presenti nelle aule non richiedono una password di accesso per l’accensione.

Tutti i docenti dell’Istituto e gli studenti della scuola primaria e secondaria di I grado, oltre che la sezione dei grandi della scuola dell’infanzia, possiedono un account generato dalla scuola per consentire loro l’accesso a piattaforme didattiche per la DID.

La famiglia si impegna a

1. promuovere comportamenti di cittadinanza consapevole improntati alla legalità, al senso critico e allo sviluppo della persona umana anche nell’ottica dello sviluppo sostenibile, al fine di prevenire azioni in contrasto con le regole del vivere civile, dell’ambiente ed in modo particolare in contrasto al cyberbullismo e alla violazione della privacy e alle varie forme di discriminazione;
2. condividere con gli insegnanti il rispetto delle norme indicate nei regolamenti d’uso dei dispositivi digitali (regolamento byod, netiquette, ...)

3. intraprendere azioni educative e formative tese alla promozione da parte dei propri figli di comportamenti consapevoli improntati alla legalità, al senso critico e allo sviluppo della persona umana, al fine di prevenire azioni in contrasto con le regole del vivere civile, del vivere a scuola, del rispetto della diversità, della Legge ed in modo particolare, azioni che rientrano nel cyberbullismo e tese alla violazione della privacy.

L'alunno/a si impegna a

1. mettere in atto comportamenti rispettosi delle regole del vivere civile, del vivere in situazione di emergenza sanitaria e, in particolare, del vivere a scuola, - anche nelle attività in didattica digitale integrata (DiD) (ad esempio, evitare comportamenti colposi o dolosi anche in merito all'esecuzione di verifiche, al rispetto del diritto d'autore, all'uso dello smartphone ecc.) come da Regolamento d'Istituto;

2. utilizzare i dispositivi elettronici a supporto della didattica, in comodato o personali, in modo corretto nel rispetto della Legge evitando azioni lesive della privacy e della dignità dell'altro riconducibili al cyberbullismo ed al bullismo in generale.

---

## ***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.

Il sito dell'Istituto Comprensivo è raggiungibile all'indirizzo <https://icverdello.edu.it>. La gestione del sito della scuola e la rispondenza alle normative per quanto concerne i contenuti (accuratezza, appropriatezza, aggiornamento) e le tecniche di realizzazione e progettazione è a cura del Dirigente Scolastico e dei docenti referenti del sito web. Sul sito è possibile trovare il Regolamento d'Istituto, pubblicizzazione di eventi, avvisi ai genitori, documentazione di attività curricolari ed extracurricolari svolte; pulsanti attivi permettono l'accesso a link di interesse, tra cui il registro elettronico. Docenti, personale ATA e genitori possono accedere all'area riservata del sito attraverso credenziali personali. La scuola, in qualità di ente pubblico, pubblicherà sul proprio sito web i contenuti che saranno valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative.

## INDICAZIONI SUL REGISTRO ELETTRONICO UTILIZZATO DALL'ISTITUTO COMPRENSIVO

Il portale Axios è una piattaforma che permette di interagire in tempo reale con tutti i dati che la scuola vuole rendere disponibili ai destinatari (segreteria, docenti, famiglia).

La sicurezza e la privacy, nonché le prerogative di accesso, sono controllati da Axios mediante password individuali, generate da un'apposita procedura interna e comunicate ai destinatari a mezzo posta elettronica o cartacea, in presenza.

L'app "Axios RE famiglia" permette di verificare in tempo reale alcuni dati sulla carriera scolastica del/la proprio/a figlio/a, tra cui: dati anagrafici, curriculum scolastico, assenze/ritardi/permessi e giustificazioni ed è possibile visionare i compiti assegnati e gli argomenti trattati; comunicazioni appositamente indirizzate alle rispettive famiglie; le valutazioni ed altre funzionalità specifiche, se debitamente attivate.

L'utilizzo della piattaforma è riservata esclusivamente a fini didattici, nel rispetto di quanto indicato dal gestore e sulla base di quanto stabilito dalla normativa vigente.

### PIATTAFORMA GSUITE WS

Nell'istituto è in dotazione la piattaforma digitale G WS con applicativi utilizzati dagli insegnanti dell'IC per integrare le attività didattiche e per la DAD. Per l'utilizzo viene richiesta ai genitori una informativa e una liberatoria.

Nel regolamento DDI del 3-09-2020 inserito nel PTOF si cita:

#### Art. 13 - Aspetti riguardanti la privacy

1. Gli insegnanti dell'Istituto sono nominati dal Dirigente scolastico quali incaricati del trattamento dei dati personali degli alunni e delle loro famiglie ai fini dello svolgimento delle proprie funzioni istituzionali e nel rispetto della normativa vigente. 2. Gli alunni e chi ne esercita la responsabilità genitoriale

a) Prendono visione dell'Informativa sulla privacy dell'Istituto per le studentesse, gli studenti e le loro famiglie ai sensi dell'art. 13 del Regolamento UE 2016/679 (GDPR);

b) Sottoscrivono la dichiarazione liberatoria sull'utilizzo della Google Suite for Education, comprendente anche l'accettazione della Netiquette ovvero dell'insieme di regole che disciplinano il comportamento delle studentesse e degli studenti in rapporto all'utilizzo degli strumenti digitali;

c) Sottoscrivono il Patto educativo di corresponsabilità che comprende impegni specifici per prevenire e contrastare eventuali fenomeni di bullismo e cyber bullismo, e impegni riguardanti la DDI.

---

## 3.4 - *Strumentazione personale*

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente **ePolicy** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

L'IC ha un regolamento per il BYOD inserito nel PTOF nel quale si cita:

1. Sono ammessi a scuola i seguenti dispositivi: computer portatile, tablet, e reader
2. Non sono ammessi a scuola i seguenti dispositivi: cellulari, smartphone, videogiochi in genere.

---

## *Il nostro piano d'azioni*

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

- 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
- informativa agli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per alcune classi per la presentazione ai genitori di indicazioni/regolamenti sull'uso delle piattaforme digitali in uso nella scuola
- Organizzare attività volte a formare gli studenti e le studentesse

dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

- Organizzare attività volte 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
- 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.

I comportamenti a rischio possono essere molteplici ma afferiscono, in base alla fascia di età, a uno sviluppo cognitivo, affettivo e morale incompleto oppure a fasi critiche transitorie o alla capacità di gestione di dinamiche complesse, mediante confronto/relazione con il Sé e l'altro, mediante la dimensione dell'empatia, della socialità, dell'affettività e della sessualità, e -ancora- mediante il riconoscimento di un

limite tra dimensione di legalità ed utilizzo sicuro delle tecnologie digitali. Anche per questo motivo nel nostro Istituto è stato istituito uno sportello psicopedagogico d'ascolto dedicato a tutte le componenti della realtà scolastica per fornire gli strumenti necessari e prioritari in vista della necessità di sensibilizzare ad un uso positivo e consapevole delle TIC gli studenti e le studentesse, sia in un'ottica di tutela dai rischi potenziali sia di valorizzazione delle opportunità esistenti, ponendo la scuola ed i genitori di fronte alla sfida di riconsiderare la propria identità, il proprio ruolo educativo e le proprie risorse, oltre allo stato dei rapporti reciproci per un patto educativo da rinnovare costantemente.

---

## ***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).

Gli atti di cyberbullismo possono essere suddivisi in due gruppi:

- **diretto**: il bullo utilizza strumenti di messaggistica istantanea come SMS o MMS, che hanno un effetto immediato sulla vittima poiché diretti esclusivamente alla persona;
- **indiretto**: il bullo fa uso di spazi pubblici della Rete, come Social network, blog o forum, per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima, anche dal punto di vista psicologico.

**Indicatori di segnali che può manifestare una potenziale vittima di cyberbullismo sono:**

- Appare nervosa quando riceve un messaggio o una notifica;
- Sembra a disagio nell'andare a scuola o finge di essere malata (ha spesso mal di stomaco o mal di testa);
- Cambia comportamento ed atteggiamento in modo repentino;
- Mostra ritrosia nel dare informazioni su ciò che fa online;
- Soprattutto dopo essere stata online, mostra rabbia o si sente depressa;
- Inizia ad utilizzare sempre meno PC e telefono (arrivando ad evitarli);
- Perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;
- Il suo rendimento scolastico peggiora.

Finalità condivisa tra scuola e famiglia è intervenire preventivamente, efficacemente e tempestivamente al fine di evitare, arginare ed eliminare possibili manifestazioni di comportamenti antisociali. Valutare i comportamenti che sfociano in disagio sociale è precursore di un lavoro in rete, con il coinvolgimento dello Sportello d'Ascolto quale supporto e/o forme di mediazione.

L'azione deve trovare una sinergia in tutte le componenti della Scuola che " è chiamata a realizzare azioni preventive" con azioni di "formazione e prevenzione in rete anche con professionisti esterni" come definito dall'AGGIORNAMENTO DELLE LINEE GUIDA DI ORIENTAMENTO E PREVENZIONE DEL BULLISMO E CYBERBULLISMO del Marzo 2021 e dalla legge del 20 Agosto 2019 n°92 *Introduzione dell'insegnamento scolastico dell'educazione civica* che prevede nell'ambito dell'insegnamento trasversale dell'educazione civica uno specifico approfondimento sull'educazione alla cittadinanza

digitale. Come strumenti di rilevamento e prevenzione si utilizzeranno quelli forniti dalla Piattaforma Elisa sia con i corsi per DS che con i corsi per i referenti.

---

## ***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.

Occorre valorizzare la dimensione relazionale dei più giovani, sensibilizzandoli verso capacità di analisi e discernimento, per fornire strumenti idonei tanto comunicativi quanto educativi sotto l'aspetto civico e morale:

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

La corresponsabilità con la famiglia è un precursore fondamentale nell'azione didattica-educativa della scuola, anche per attivare progettazioni complementari con finalità socio-educative.

---

## **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?*

La formazione del personale è una priorità che la scuola si prefigge di attivare, coerentemente ai criteri enunciati nel PTOF per fornire di strumenti adeguati atti al riconoscimento delle problematiche e per un tempestivo intervento.

Le tecnologie digitali rappresentano una possibilità di espressione dell'identità individuale prima impensabile, ma d'altra parte rappresentano anche un potenziale rischio.

La RETE produce comunità di conoscenza e questo permette ai giovani di confrontarsi con un sapere digitalizzato. Il bilanciamento tra opportunità e rischi negli ambienti mediali e in relazione ai più giovani, richiede una costante e attenta negoziazione tra opportunità e rischi.

Si ribadisce la necessità di una linea condivisa con la famiglia per stabilire mezzi e modalità durante lo studio domestico, con tempi stabiliti e controllo attivo durante la navigazione in Rete.

---

## **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.

La Legge 19 luglio 2019 n. 69, all'articolo 10, ha introdotto in Italia il reato di

"revenge porn", ossia la diffusione illecita di immagini o di video sessualmente espliciti.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psico-sessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro e depressione.

Una informativa precoce serve a sensibilizzare a questa tematica spesso ignorata nel percorso educativo stabilito.

---

## 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.

Per riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli segnali che possono essere indicatori importanti, per valutare un cambiamento improvviso nel comportamento di un minore:

- Il minore ha conoscenze sessuali non adeguate alla sua età
- Venite a conoscenza di un certo video o di una foto che circola online o - ancora- il minore ha ricevuto un contenuto (o filmato), ma c'è imbarazzo e preoccupazione nel raccontarvi di più...
- Il minore si isola totalmente e sembra preso solo da una relazione online
- Ci sono prese in giro e allusioni sessuali verso un bambino/ragazzo in

particolare

Il nostro Istituto attiva percorsi di Educazione all'affettività e alla sessualità, al fine di informare ed accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) su queste tematiche; ciò per aiutarli ad essere più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri.

Inoltre, all'interno dell'Istituto è attivo lo Sportello di Ascolto, al fine di supportare psicologicamente gli studenti e le studentesse in difficoltà.

---

## 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](#).**

Qualora l'Istituto ricevesse una segnalazione, i referenti procederanno a coinvolgere le autorità competenti in materia. L'intento è quello di facilitare il processo di rimozione del materiale stesso dalla Rete e allo stesso tempo consentire le opportune attività investigative finalizzate ad identificare chi possiede quel materiale, chi lo diffonde e chi lo produce, ma, soprattutto e primariamente, ad identificare i minori abusati presenti nelle immagini e video, assicurando la fine di un abuso che potrebbe essere ancora in corso e il supporto necessario. Parallelamente, per salvaguardare il benessere psicofisico degli alunni coinvolti nella visione di questi contenuti, sarà opportuno ricorrere a un supporto psicologico. Se si è a conoscenza di tale tipologia di reato è possibile far riferimento alla: Polizia di Stato - Compartimento di Polizia postale e delle Comunicazioni; Polizia di Stato - Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri - Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato - Commissariato online. Studi in materia dimostrano come l'utilizzo di materiale pedopornografico possa essere propedeutico all'abuso sessuale agito ed è quindi fondamentale, in termini preventivi, intervenire per ridurre l'incidenza di tale possibilità. L'abuso sessuale online rappresenta una particolare declinazione dell'abuso sessuale su bambini/e, ragazzi/e, la cui caratteristica fondante è il ruolo ricoperto dalle tecnologie digitali, le quali diventano il mezzo principale attraverso cui l'abuso viene perpetrato, documentato e diffuso in Rete con immagini e/o video. Le dinamiche attraverso cui l'abuso sessuale online si manifesta producono effetti sulle vittime che si aggiungono e moltiplicano a quelli associati all'abuso sessuale.

Il nostro Istituto è dotato di un sistema di filtro della navigazione, firewall, per evitare consultazioni di siti impropri durante la permanenza a scuola e tutelare i minori dalla visione di contenuti inappropriati alla loro età.

Inoltre aderisce ad iniziative volte alla prevenzione del rischio promosse da enti specifici (Polizia di Stato, Unicef,...)

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

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

- Organizzare attività 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 attività e laboratori per studenti e studentesse dedicati all'Educazione Civica nell'ambito della Cittadinanza Digitale.
- Organizzare attività 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.

### **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/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 attività per studenti e studentesse dedicati all'Educazione Civica nell'Ambito della Cittadinanza 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 (Educazione all'affettività e alla sessualità).

# 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).

**In relazione al CASO A**, è opportuno il coinvolgimento del Referente d'Istituto per il contrasto del bullismo e del cyberbullismo, al fine di raccogliere le segnalazioni sia in forma cartacea ( modulo reperibile in un luogo ben contrassegnato di ciascun Plesso) sia attraverso il modulo online sul sito d'Istituto nella sezione dedicata a scadenza mensile e di valutare le possibili strategie d'intervento. Se si ravvisano gli estremi, viene informato il Dirigente scolastico unitamente al Consiglio di classe.

Uno strumento utile per raccogliere e sistematizzare le segnalazioni può essere il diario di bordo, una scheda riepilogativa delle situazioni gestate nell'Istituto (allegato alla presente e-Policy). Il docente incaricato inserisce gli episodi segnalati, le azioni intraprese e i soggetti coinvolti.

Operativamente è fondamentale coinvolgere tutti gli studenti e le studentesse, informandoli sui fenomeni e sulle caratteristiche degli stessi, suggerendo di chiedere aiuto se pensano di vivere situazioni, di subire atti identificabili come bullismo o cyberbullismo.

**In relazione al CASO B**, il docente deve condividere immediatamente quanto osservato con il Referente per il bullismo e il cyberbullismo, al fine di valutare insieme le possibili strategie di intervento. Il Referente stende la "Scheda di valutazione Approfondita dei casi di bullismo e vittimizzazione (vedasi allegato). Si avvisa anche il Dirigente Scolastico che convoca il Consiglio di classe. Se non si ravvisano fattispecie di reato, è opportuno:

- informare i genitori (o chi esercita la responsabilità genitoriale) degli/delle studenti/studentesse direttamente coinvolti/e (qualsiasi ruolo abbiano avuto), se possibile con la presenza di professionisti dell'aiuto, per strategie condivise e modalità di supporto;
- creare momenti di confronto costruttivo in classe, con la presenza di figure specialistiche territoriali;
- informare i genitori degli/delle studentesse infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o Social (o successivamente, in caso di non risposta, al garante della Privacy);
- convocare il Consiglio di classe
- valutare come coinvolgere gli operatori scolastici su quello che sta accadendo.

A seconda della situazione e delle valutazioni effettuate con Referente, Dirigente e genitori, si potrebbe poi segnalare alla Polizia Postale -ove necessario ai sensi di legge-:

1. contenuto del materiale online offensivo;
2. fattispecie di reato eventuale.
3. modalità di diffusione.

Se è opportuno, richiedere un sostegno ai servizi e alle associazioni territoriali o ad altre autorità competenti (pensiamo al cyberbullismo, con il suo impatto sulla vita quotidiana della vittima, la quale sa che i contenuti lesivi sono online, diffusi fra molte persone conosciute e non, in un circuito temporale senza fine e senza barriere spaziali).

E' bene sempre dialogare con la classe, attraverso interventi educativi specifici, cercando di sensibilizzare studenti e studentesse sulla necessità di non diffondere online i materiali dannosi, ma anzi di segnalarli e bloccarli. Ciò è utile anche per capire il livello di diffusione dell'episodio all'interno dell'Istituto.

---

### **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.

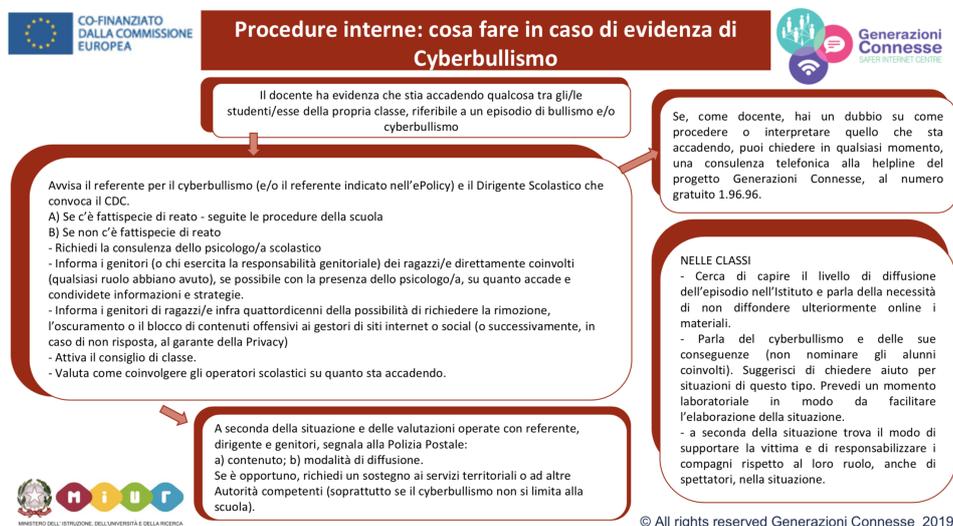
- **Aziende Sanitarie Locali:** forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni 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.

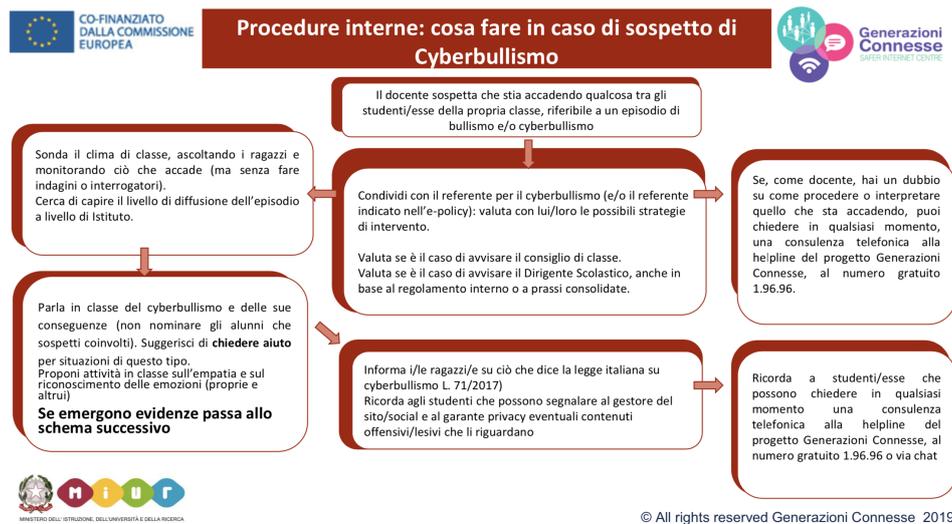
Si ritiene utile adottare un modulo (vedasi allegato) di sintesi contenente i contatti per Interventi di rete con il territorio contenente:

1. SE AVESSIMO BISOGNO DI...
2. CHI
3. CONTATTI
4. POSSIBILI REFERENTI.

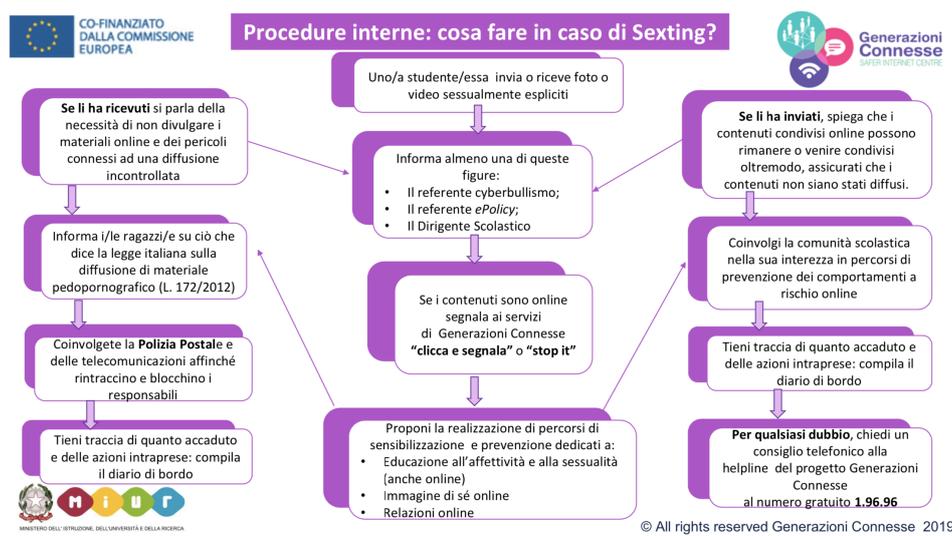
## 5.4. - Allegati con le procedure

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

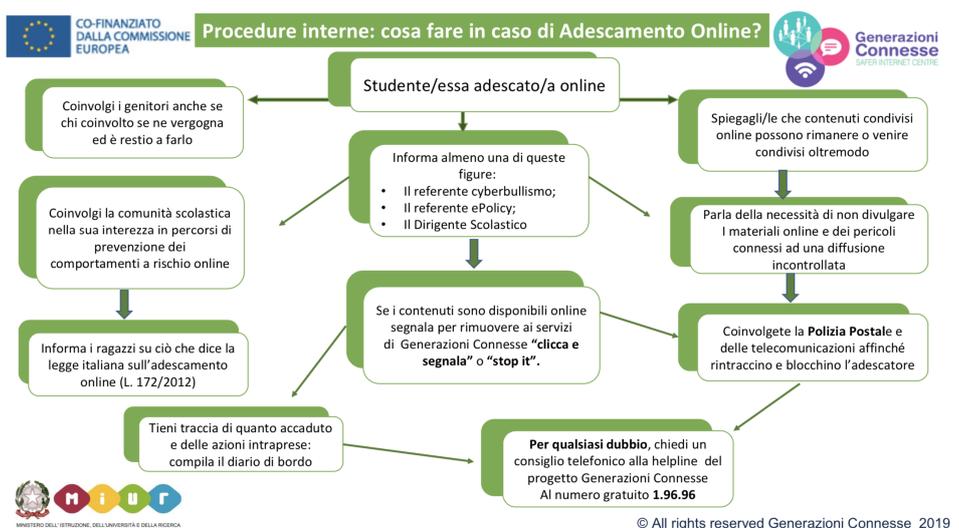




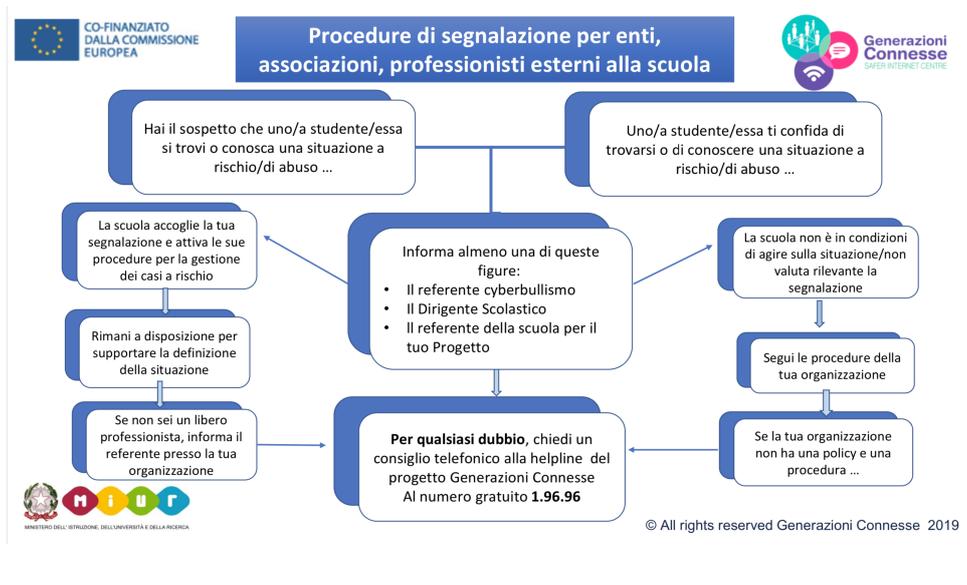
## Procedure interne: cosa fare in caso di sexting?



## 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***

---

### IL NOSTRO PIANO DI AZIONI

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

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

