



# Documento di ePolicy

**GRIS01200Q** 

POLO BIANCIARDI GROSSETO

PIAZZA DE MARIA 31 - 58100 - GROSSETO - GROSSETO (GR)

BARBARA ROSINI

# 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 <u>Quadro di riferimento</u> <u>Europeo delle Competenze per l'apprendimento permanente</u> 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 curricolo

- 1. Curricolo 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 Polo Bianciardi ritiene opportuno dotarsi di un e-policy vista la diffusione dell'ICT nell'intera comunità educante, nelle attività didattiche e negli ambienti scolastici. Questo documento può rappresentare un valido aiuto nel sensibilizzare il personale docente e non docente, gli studenti e le famiglie ad un uso consapevole e sicuro delle TIC.

Nel corso degli anni l'uso della dotazione tecnologica è aumentato, numerosi sono gli strumenti messi a disposizione delle classi, degli studenti e dei docenti rendendo necessaria una specifica regolamentazione.

Internet offre moltissime opportunità, ma presenta anche molti rischi: non è sufficiente saper usare procedure e tecniche ma bisogna imparare ad utilizzarle con consapevolezza, per essere oltre che nativi digitali anche cittadini digitali.

I cittadini digitali, poiché vivono ed operano nella società digitale, hanno diritti, doveri e regole da rispettare.

La nostra Scuola nel suo curricolo, promuove l'adozione di strategie che favoriscano l'acquisizione da parte degli alunni del DigComp (digital competence), al fine di poter usare in modo responsabile le opportunità offerte dal web, navigare in sicurezza ed avere una condotta civile che non danneggi se stessi e gli altri.

## 1.2 - Ruoli e responsabilità

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

#### Il DIRIGENTE SCOLASTICO

Il Dirigente Scolastico garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica. Interviene sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIUR. Insieme al docente referente sulle tematiche del bullismo/cyberbullismo promuove la cultura della sicurezza online anche attraverso corsi di formazione specifici sull'utilizzo

positivo e responsabile delle TIC. Gestisce ed interviene nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

#### L'ANIMATORE DIGITALE E IL TEAM DELL'INNOVAZIONE

L'Animatore coadiuvato dal Team supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento alla prevenzione dei rischi online, alla protezione e gestione dei dati personali. Promuove percorsi di formazione, interna all'Istituto, nell'ambitio di sviluppo delle competenze digitali. Promuove l'adesione ai bandi relativi allo sviluppo delle competenze digitali e alle TIC.

#### IL REFERENTE BULLISMO E CYBERBULLISMO

Il referente per il bullismo-cyberbullismo ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo avvalendosi anche della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola. Svolge un importante compito di supporto al Dirigente per la stesura di regolamenti e documenti. Segnala tempestivamente situazioni di rischio online o casi di bullismo-cyberbullismo

#### I DOCENTI

Tutto il personale docente ha il compito di diffondere la cultura dell'uso responsabile delle TIC e della rete integrando nella propria disciplina approfondimenti utilizzando le tecnologie digitali. Provvede alla propria formazione-aggiornamento sull'utilizzo delle TIC (in particolare: il rispetto dei diritti intellettuali dei materiali ricercati in rete, tutela della privacy ....) Ha, inoltre, il dovere di monitorare ed eventualmente segnalare al Dirigente Scolastico, all'animatore digitale o al referente del bullismo-cyberbullismo qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse avviando le procedure previste in caso di violazioni. Supporta e indirizza gli studenti/studentesse coinvolti in problematiche relative alla rete.

#### IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il Dirigente Scolastico e con tutto il personale docente. Oltre a svolgere attività di formazione e autoformazione in tema di bullismo e cyberbullismo è coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo. il personale ATA è chiamato al trattamento dei dati sensibili nel rispetto della privacy.

#### GLI STUDENTI E LE STUDENTESSE

Gli studenti e le studentesse, in relazione al proprio grado di maturità e consapevolezza raggiunta, devono impegnarsi ad avvalersi al meglio delle tecnologie

digitali rispettando le norme indicate per il loro utilizzo in coerenza con quanto richiesto dai docenti e dal documento e-Policy. Possono partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della rete facendosi promotori di quanto appreso con percorsi di peer education. Supportati dai loro docenti imparano a tutelare se stessi e i propri compagni dai rischi online.

#### I GENITORI

I Genitori e i tutori rivestono un ruolo importante affinché gli studenti/studentesse abbiano piena consapevolezza nell'utilizzo sicuro ed appropriato dei device personali o forniti dalla scuola partecipando attivamente alle attività di promozione ed educazione sull'uso consapevole delle TIC e della rete. È importante che si relazionino con gli studenti/studentesse e il personale della scuola in maniera costruttiva nella prevenzione dei rischi e nell'accettazione e condivisione delle procedure previste in caso di violazione delle regole stabilite.

#### GLI ENTI EDUCATIVI ESTERNI E LE ASSOCIAZIONI

Gli Enti educativi esterni e le associazioni che entrano in relazione con il Polo Bianciardi si conformano all'uso consapevole della rete e delle TIC promuovendo comportamenti sicuri, la sicurezza online e assicurando la protezione degli studenti e delle studentesse durante le attività che svolgono all'interno del Polo o presso le loro strutture.

# 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).

Per tutelare gli studenti e le studentesse le organizzazioni/associazioni extrascolastiche e gli esperti, chiamati a vario titolo alla realizzazione di progetti ed attività educative nel breve e/o lungo periodo, prenderanno visione del documento e-Policy con un'informativa sintetica comprensiva delle procedure di segnalazione.

È importante che anche i soggetti esterni siano sensibilizzati e responsabilizzati sui rischi online in cui possono incorrere gli studenti e le studentesse e dei comportamenti corretti che devono seguire nello svolgimento delle loro attività contrastando condotte non professionali.

L'informativa permetterà una piena conoscenza delle azioni e delle procedure di segnalazione valide per tutto il personale esterno che si interfaccerà con gli studenti/studentesse per rilevare e gestire eventuali problematiche connesse ad un uso improprio delle tecnologie digitali. Questo documento sintetico garantisce la diffusione delle procedure distinguendo i ruoli e le azioni da compiere in base alla tipologia dei casi, i passi per la segnalazione alle autorità competenti in collaborazione con i servizi del territorio, in un'ottica di condivisione degli interventi potenziando ll rapporto fiduciario fra scuola e famiglia.

L'informativa sarà condivisa e sottoscritta nella stipula di eventuali contratti con personale e associazioni esterne. Le figure professionali e le organizzazioni coinvolte in progetti, laboratori e attività prenderanno visione di tutti i documenti proposti dall'Istituto e li sottoscriveranno preliminarmente all'avvio delle attività con gli studenti e le studentesse, in classe o fuori. L'istituto valuterà se richiedere eventualmente anche il casellario giudiziale come fattore ulteriormente protettivo verso i minori per verificare l'eventuale esistenza o meno di condanne per alcuni reati previsti dal Codice Penale.

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

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

studenti/esse) si faccia a sua volta promotore del documento.

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

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

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

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

Il presente documento di e-Policy viene condiviso con tutta la comunità educante, al fine di promuovere competenze digitali diffuse. Al tempo stesso ogni attore scolastico è chiamato a diventare promotore del documento.

A tal fine si prevede:

- 1. Condivisione e comunicazione della Policy agli alunni:
- all'inizio dell'anno scolastico, i docenti, in occasione dell'illustrazione del regolamento d'istituto alle studentesse e agli studenti, presenteranno il documento di e-policy della scuola
- nel corso dell'anno ciascun docente darà spazio alla diffusione delle buone pratiche con specifici richiami al documento per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e al contrasto ai fenomeni di bullismo e di cyberbullismo.
- 2. Condivisione e comunicazione della Policy al personale:
- Le norme adottate dalla scuola in materia di sicurezza nell'utilizzo del digitale saranno discusse in occasione degli incontri degli organi collegiali (collegio docenti, riunioni di dipartimento,.....) e rese note all'intera comunità scolastica tramite pubblicazione sul sito web della scuola
- Il personale riceverà un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso diffusione di materiali rdedicati
- 3. Condivisione e comunicazione della Policy ai genitori:
- le famiglie saranno informate in merito alla linea di condotta adottata dalla scuola per un uso sicuro e responsabile delle tecnologie digitali e di internet attraverso la

condivisione del presente documento e di materiali informativi specifici attraverso canali istituzionali quali il sito web della scuola, il registro elettronico, ecc....

# 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.

Il Polo Bianciardi ritiene che le condotte da sanzionare relative all'uso improprio delle tecnologie digitali siano:

- Realizzazione e/o condivisione online di immagini o video di compagni/e senza il loro consenso o che li ritraggono in pose offensive e denigratorie
- Realizzazione e/o condivisione di scatti intimi e a sfondo sessuale
- Condivisione di dati personali dei compagni, dei docenti e del personale ATA senza il loro consenso
- Invio di immagini o video volti all'esclusione di compagni/e
- Condivisione in rete di comunicazioni ufficiali interne del Polo: compiti in classe, circolari, comunicazioni, valutazioni
- Registrazioni e diffusione di audio delle lezioni senza un preventivo assenso del docente
- Utilizzare la rete per giudicare, denigrare, offendere infastidire o impedire a qualcuno di esprimersi o partecipare
- Connettersi a siti proibiti o comunque non autorizzati
- Scaricare file per finalità personali

Tutte le infrazioni alla presente e-Policy andranno tempestivamente segnalate al Dirigente Scolastico, che avrà cura di convocare le parti interessate onde valutare le possibili azioni da intraprendere.

In merito ai provvedimenti disciplinari da adottare da parte del Consiglio di classe nei confronti dello studente/essa che ha commesso un'infrazione alla e-policy (in proporzione sia all'età dello studente sia alla gravità dell'infrazione commessa), si prediligeranno interventi di tipo educativo e non punitivo, sanzioni disciplinari di tipo riparativo, convertibili quando possibile in attività a favore della comunità.

Più precisamente:

a. colloquio con lo/a studente/essa coinvolto/a;

- b. eventuale confronto con i genitori;
- c. ripristino delle regole di convivenza all'interno della classe;
- d. interventi di educazione tra pari (peer education);
- e. incontri con esperti esterni e con il CIC della scuola;
- f. provvedimenti disciplinari educativi (eventuale sospensione con obbligo di frequenza presso strutture convenzionate dove svolgere mansioni di pubblica utilità sociale);

g.eventuale segnalazione alle autorità (polizia postale, Garante per la protezione dei dati personali, Garante dell'Infanzia e dell'Adolescenza, servizi minorili dell'amministrazione della Giustizia, richiesta di ammonimento da parte del Questore).

Le infrazioni compiute dal personale scolastico saranno gestite dal Dirigente Scolastico secondo quanto previsto dal Codice di comportamento dei dipendenti pubblici (GU n.129 del 4-6-2013), dal CCNL (29 novembre 2007), dal DPCM (28 novembre 2000) e dal Codice disciplinare pubblicato tramite il sito istituzionale e dalla normativa in vigore inerente alla privacy.

## 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.

I regolamenti dell'Istituto verranno integrati in linea con la policy con l'inserimento delle sequenti norme:

- Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.
- Le postazioni informatiche dell'istituto possono essere utilizzate esclusivamente per attività didattiche, funzionali all'insegnamento e di formazione del personale docente e non docente.
- In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al tecnico responsabile.

Disposizioni sull'uso dei software:

1. I software installati sono ad esclusivo uso didattico

2. E' fatto divieto di usare software non conformi alle leggi sul copyright.

#### Accesso a internet:

- 1. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante.
- 2. Internet non può essere usato per scopi vietati dalla legislazione vigente.
- 3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet.
- 4. E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza.

Utilizzo dello smartphone e dei vari dispositivi tecnologici:

- 1. è vietato l'uso dello smartphone e dei dispositivi tecnologici da parte degli studenti e delle studentesse, durante lo svolgimento delle attività didattiche, salvo preventivo accordo con il docente per lo svolgimento di attività didattiche. Il divieto deriva dai doveri sanciti dallo Statuto degli studenti e delle studentesse (D.P.R. n. 249/1988). La violazione di tale divieto configura una infrazione disciplinare rispetto ai quali la scuola è tenuta ad applicare apposite sanzioni. I suddetti dispositivi devono essere tenuti spenti e opportunamente custoditi e depositati nei borsoni, zaini, giacconi, né sul banco né tra le mani. In caso di accordi con i docenti e per lo svolgimento di compiti e/o verifiche gli smartphone e altri dispositivi tecnologici possono essere depositati presso la cattedra.
- 2. Considerato che gli smartphone e altri dispositivi tecnologici possono essere utilizzati anche per scattare foto, effettuare riprese filmate, condividere contenuti con i social media, la scuola informa che, il verificarsi di tali eventi in orario scolastico, qualora configuri un'ipotesi di reato, verrà segnalato agli organi competenti.
- 3. In ogni caso, i genitori tengano conto che le comunicazioni urgenti ed improcrastinabili possono essere trasmesse ai loro figli durante l'orario scolastico rivolgendosi telefonicamente alle singole sedi scolastiche.

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

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

Il monitoraggio dell'implementazione del documento di e-Policy e del suo eventuale aggiornamento sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore digitale, del Referente del bullismo e del cyberbullismo e del Gruppo di lavoro della policy. Sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle TIC e della Rete.

Il monitoraggio sarà rivolto anche ai docenti, al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti.

## Il nostro piano d'azioni

# Azioni da svolgere entro un'annualità scolastica:

• Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti

### Azioni da svolgere nei prossimi 3 anni:

- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

# Capitolo 2 - Formazione e curricolo

# 2.1. Curricolo 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 curricolo digitale.

La formazione digitale è parte integrante della formazione della persona in chiave di cittadinanza consapevole.

La scuola progetta un curriculum digitale tenendo ben presenti ed integrando le tre dimensioni richiamate nella definizione di "competenze digitali" delle Raccomandazioni Europee:

- dimensione tecnologica: per far riflettere i giovani sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana e guidarli verso un'adeguata comprensione della "grammatica" dello strumento per evitare automatismi.
- dimensione cognitiva: si riferisce alla capacità di ricerca, utilizzo e creazione delle informazioni in rete in modo consapevole e critico e di saperne valutare credibilità e affidabilità.

 dimensione etico-sociale: si riferisce alla capacità di gestire in modo attento e sicuro i propri dati personali e quelli degli altri e di usare le tecnologie digitali nell'ottica del rispetto verso tutti. La dimensione sociale, invece, riguarda in particolar modo le pratiche sociali e lo sviluppo di abilità socio-comunicative e partecipative, per far prendere coscienza di quali sono i nostri doveri nei confronti delle persone con le quali abbiamo scambi comunicativi e confronti in rete.

Pertanto il percorso, partendo dalle prime classi, affronta i vari aspetti in maniera sempre più approfondita, anche avvalendosi dell'aiuto di esperti, affinché gli studenti prendano consapevolezza di rischi ed opportunità legati all'uso delle tecnologie.

Punto di partenza nell'elaborazione di un curriculum digitale deve essere la dimensione etico-sociale, che richiama l'attenzione degli studenti su una gestione attenta e sicura dei propri dati personali e di quelli altrui ed una corretta comunicazione on line, rispettosa della netiquette. Tale aspetto, di fondamentale importanza per formare cittadini digitali consapevoli e informati, deve essere integrato, negli anni, con le altre due dimensioni; quella legata alla ricerca e all'uso corretto delle informazioni in rete e della tecnologia nella vita quotidiana e nel lavoro.

La progettazione e attuazione del curriculum digitale deve coinvolgere tutta la comunità educante supportata da esperti al fine di creare un percorso completo ed efficace.

# 2.2 - Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

La formazione dei docenti è funzionale ad una concreta armonizzazione degli apprendimenti in chiave di cittadinanza consapevole.

La scuola sollecita l'uso delle TIC nella didattica e per tale motivo offre ed ha offerto

diverse opportunità formative per i docenti sulle tematiche legate al digitale e alle nuove tecnologie per una didattica efficace ed inclusiva.

Tali metodologie sono ormai fondamentali per una didattica attiva, dinamica e adeguata ai diversi stili di apprendimento, in quanto gli studenti si sentono maggiormente coinvolti e a loro agio con una didattica che va incontro al loro modo di vivere, di studiare e di informarsi. Per questo è fondamentale che i docenti abbiano una formazione sulle tecnologie digitali e sul loro uso nella didattica e che tale formazione sia permanente, per offrire agli insegnanti sempre nuovi spunti metodologici e occasioni di aggiornamento sulle nuove opportunità offerte dalle tecnologie.

L'istituto si impegna a mettere in atto ulteriori interventi allo scopo di formare i docenti sulle TIC e sulle metodologie per una didattica digitale.

Gli interventi da mettere in atto sono:

- fornire opportunità formative partendo dall'analisi dei fabbisogni formativi dei docenti
- elaborare una serie di percorsi formativi strutturati anche su base pluriennale per implementare di anno in anno le competenze digitali dei docenti legate alla didattica, anche tenendo conto delle caratteristiche e peculiarità dei diversi indirizzi di studio
- promuovere momenti di confronto fra docenti sulle metodologie digitali più efficaci nella didattica

## 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 si impegna ad attivare percorsi formativi in collaborazione con gli enti del territorio per promuovere un uso sicuro di Internet in un'ottica di prevenzione e

contrasto alle discriminazioni, offese, denigrazioni e lesioni della dignità dell'altro contrastando fenomeni di bullismo e cyberbullismo.

L'uso consapevole delle tecnologie è importante non soltanto a livello didattico ma anche per educare gli studenti/studentesse alle emozioni in contesto onlife modulando e gestendo i propri comportamenti nel rispetto reciproco per una convivenza civile.

È necessario formare in maniera adeguata e permanente i docenti su questi aspetti affinché siano preparati ad affrontare l'argomento nelle classi e a far fronte a problematiche ed esigenze in maniera opportuna e tempestiva.

Punto di partenza per realizzare azioni mirate ed efficaci sarà l'analisi delle esigenze e dei fabbisogni formativi dei docenti. Dopo questa prima fase l'istituto si impegnerà a fornire e promuovere opportunità formative e di approfondimento, utilizzando le risorse interne.

Inoltre sarà messo in evidenza il progetto di "Generazioni connesse" e diffuso attraverso i canali istituzionali, come il sito della scuola, nel quale saranno inseriti materiali e link di riferimento ad uso dei docenti, studenti e famiglie.

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

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

Scuola e famiglia collaborano, come da patto educativo di corresponsabilità, per accompagnare gli studenti nel percorso scolastico fino al mondo del lavoro con una formazione in itinere.

In questo percorso di accompagnamento è importante tenere presente la formazione digitale che deve coinvolgere tutta la comunità educante e le famiglie anche attraverso il "Patto di corresponsabilità" che sarà integrato con riferimenti relativi all'educazione digitale e all'ePolicy.

Oggigiorno, infatti, insegnare ai ragazzi l'uso corretto e consapevole delle tecnologie e della rete rientra tra i compiti e le responsabilità di scuola e famiglia, tanto quanto la trasmissione di valori fondamentali come il rispetto per se stessi e per gli altri.

Pertanto è opportuno stabilire un percorso condiviso con le famiglie su tali tematiche.

Una prima azione sarà messa in atto utilizzando il sito istituzionale per fornire materiali, consigli ed informazioni.

Saranno realizzate iniziative, momenti di incontro e di confronto ed occasioni formative da proporre ai genitori sui vari aspetti legati alle tecnologie e all'educazione digitale, anche con il coinvolgimento degli alunni.

Sfruttando le peculiarità dei diversi indirizzi di studio presenti nell'istituto, verrà promossa la realizzazione di materiale divulgativo da parte degli studenti.

## Il nostro piano d'azioni

# AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023)

#### Scegliere almeno 1 di queste azioni

• Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.

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

#### Scegliere almeno 1 di queste azioni

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

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

### 3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

Il Polo Bianciardi tratta i dati personali per gli scopi istituzionali e richiede il permesso nei casi particolari a margine di questa funzione. Sul sito istituzionale del Polo è caricato un modello di permesso che la scuola richiede alle famiglie (TRATTAMENTO DATI PERSONALI consenso riprese video/foto per lavori in classe).

Il trattamento dei dati viene svolto secondo le indicazioni di legge e secondo buone pratiche consigliate dal DPO della scuola. I dati personali vengono trattati dagli uffici della segreteria e conservati all'interno di una rete informatica separata da quella dedicata alla didattica. Anche la gestione e la manutenzione delle due reti è affidata a soggetti diversi.

Il Polo Bianciardi utilizza Il registro Elettronico "Nuvola" della Madisoft e la piattaforma educativa Google Workspace per le attività didattiche con gli studenti e per il lavoro di progettazione e rendicontazione delle attività didattiche degli insegnanti.

La piattaforma contiene gli account degli studenti ed è gestita, in materia di dati personali dei minori, secondo le seguenti regole:

- gli account degli studenti non contengono dati sensibili a loro riferiti
- nessun dato o informazione circa l'esistenza, l'accesso, le credenziali degli
  account viene inviato ad account privati non gestiti dalla scuola; tali dati
  personali riguardanti l'account o la sua attività vengono inviati solo brevi manu
  agli interessati oppure in digitale attraverso il registro elettronico.

Il Polo provvede con cadenza regolare all'analisi del sito web istituzionale con azioni e proposte volte a migliorare la sicurezza e la protezione dei dati trattati.

#### In particolare:

- ha progettato il sito web in base ai concetti di privacy by default e by design
- ha effettuato la migrazione del sito al suffisso edu.it
- utilizza il protocollo HTTPS (protocollo per la comunicazione su Internet che protegge l'integrità e la riservatezza dei dati scambiati online)
- il template utilizzato è ItaliaPA, template ufficiale delle pubbliche amministrazioni
- quando il trattamento di dati lo richiede, utilizza un sistema di cifratura oscurando il dato per evitare di renderlo comprensibile a coloro che non hanno titolo di accedervi
- utilizza un sistema di backup per salvare regolarmente i dati, ripristinare

- eventuali file modificati o rimossi per errore dalla rete, garantire una copia di sicurezza di tutti i file rilevanti
- utilizza un piano di disaster recovery con misure che permettono agli apparati di Information technology di superare situazioni di emergenza, o impedire che situazioni accidentali o incidenti possano compromettere il funzionamento delle strutture.

### 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.
- 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.
- 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.

La rete della segreteria è separata dalla rete didattica e, grazie ad un diverso firewall e ad un server dedicato, gestisce in modo autonomo e con regole differenti la sicurezza.

Il Dirigente Scolastico, il Direttore dei Servizi Generali e Amministrativi ed il personale degli uffici della segreteria sono profilati con account personalizzati e accedono ai servizi tramite procedura di autenticazione personale che prevede l'utilizzo di password con specifiche caratteristiche.

L'assistenza tecnica del server e delle apparecchiature informatiche è affidata a ditte specializzate nel settore, che provvede al controllo sul backup dei dati, all'aggiornamento dei sistemi operativi e degli antivirus installati sulle macchine e al controllo del funzionamento del firewall.

L'accesso alla rete è garantito in tutti i plessi della scuola.

Ogni plesso ha:

- una connessione ad internet protetta da firewall hardware
- una rete di pc connessi via cavo alla rete
- una rete Wifi protetta da password per la connessione dei dispositivi mobili.

I firewall sono programmati per la selezione dei contenuti. In alcuni plessi è stata aggiunta una seconda rete wifi protetta da password specifica per la connessione alla rete internet di ospiti e studenti.

La password per l'accesso alla rete wifi viene comunicata agli studenti e agli ospiti che necessitano di utilizzare dispositivi mobili durante le attività didattiche curricolari ed extracurricolari.

# 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 Polo Bianciardi ha in uso diversi strumenti di comunicazione attivi tra le varie parti che compongono la comunità scolastica:

- Posta elettronica ..@istruzione.it, usata dalla segreteria per le comunicazioni con le famiglie e con personale docente per contenuti amministrativi e divulgativi di realtà esterne alla scuola
- 2. Posta elettronica ...@polobianciardigrosseto.it, usata da tutto il personale per le attività che riguardano il funzionamento e l'organizzazione della scuola.
- 3. Registro Elettronico "Nuvola", strumento prevalente per la comunicazione con studenti e famiglie su contenuti legati alle attività didattiche
- 4. Piattaforma educativa Google WorkSpace, ambiente di apprendimento digitale che affianca quello in presenza
  - facilitando il reperimento dei materiali e semplificando la fruizione delle lezioni.
- 5. Sito internet della scuola, utilizzato come strumento di divulgazione delle informazioni e delle attività; rappresenta il canale prioritario per far conoscere la scuola alle famiglie e agli altri attori presenti nel territorio.

## 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'utilizzo dei dispositivi mobili personali è permesso all'interno della scuola a:

 adulti, impiegati, docenti e collaboratori che hanno la possibilità di utilizzare l'accesso alla rete wifi di ogni plesso. Ogni lavoratore si assume in pieno la responsabilità dell'utilizzo dei propri device personali.

2. gli studenti possono utilizzare i dispositivi personali con il permesso e sotto la responsabilità del docente, soltanto per scopi didattici

### Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).

#### Scegliere almeno 1 di queste azioni:

 Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

#### Scegliere almeno 1 di queste azioni:

• Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity).

# 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 gueste 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 scuola propone corsi di formazione per sensibilizzare la prevenzione al rischio on line. In alcuni indirizzi di studio, all'interno del curriculo scolastico, viene affrontata, nello specifico, la tematica della tutela della privacy nell'utilizzo dei sistemi informatici. La sensibilizzazione degli adulti e degli studenti viene attuata anche tramite la collaborazione con le autorità ed enti locali (polizia postale, ASL) attraverso

la partecipazione ai corsi e/o progetti dagli stessi promossi ed attivati al fine di realizzare la massima prevenzione dai rischi legati all'utilizzo errato di internet nelle scuole

- Sensibilizzazione (acquisire informazioni e possibili soluzioni)
- Attraverso il progetto generazioni connesse e il suo portale, la scuola potrà
  fornire al personale docente il materiale divulgativo creato ad hoc, molto
  efficace per i ragazzi, e potrà essere mostrato e fornire interessanti spunti di
  riflessione per il dibattito. I video di sensibilizzazione non sono specifici per una
  materia in particolare, quindi possono essere utilizzati da tutti i docenti in
  modo trasversale facilitando il dibattito.
- Prevenzione (attivare interventi)

Alcuni docenti nelle ore di educazione civica si possono occupare di fare creare ai ragazzi/ragazze un vademecum, una cartellonistica, una campagna di informazione, ecc.. per diffondere consapevolezza e proporre percorsi di soluzione.

# 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 <u>cyberbullismo</u> 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 <u>cyberbullismo</u>. 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).

La scuola propone corsi di formazione per prevenire il cyberbullismo.

I percorsi formativi intrapresi dall'istituto sono volti ad una riflessione e analisi approfondita del fenomeno, anche con l'aiuto di esperti, per far prendere coscienza agli studenti di tutti i rischi ad esso connessi.

L'orientamento della scuola è quello di concentrarsi, ogni anno, nella formazione specifica delle classi del biennio per raggiungere nel tempo la situazione ideale di avere tutte le classi di tutti gli indirizzi adeguatamente formate sulla tematica.

Il cyberbullismo è un fenomeno molto pericoloso che difficilmente riesce ad essere bloccato una volta che l'azione è iniziata poichè, su internet, tutto diventa virale entro pochi minuti. Riveste quindi un ruolo essenziale la prevenzione che la scuola cerca di attuare accompagnando gli studenti verso la comprensione, in primo luogo, di ciò che può essere considerato cyberbullismo. Interventi specifici in classe da parte del referente bullismo della scuola mirano a stimolare un dialogo con gli alunni, a dare informazioni sulla tematica ma anche ad evidenziare situazioni e casistiche che possono coinvolgere i giovani e che sono valutate come cyberbullismo. L'utilizzo delle strumentazioni (smartphone, tablet, pc, telecamere e macchine fotografiche) e delle applicazioni più comuni come whatsapp, tik tok, facebook o istagram sono, per i giovani, veicoli semplici di trasmissione e "nuova" socializzazione ma possono rivelarsi anche strumento, più o meno consapevole, di attuazione del cyberbullismo. La prevenzione raggiunge il suo fine quando lo studente prende coscienza del fatto che anche una foto scattata senza autorizzazione e poi trasmessa può comportare per chi ne è protagonista un disagio, grande o piccolo che sia.

La scuola promuove la diffusione, non una tantum ma costantemente, di materiale informativo sul bullismo/cyberbullismo che aiuti a riconoscere il fenomeno e a trovare soccorso nel caso in cui ci si riconosca vittima.

Tale materiale informativo deve essere il più possibile chiaro affinché i ragazzi/ragazze "vittime" possano avere indicazioni specifiche, figure di riferimento con nomi e cognomi o ruoli fissi, azioni da compiere schematizzate... e non si sentano soli "in preda al branco".

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

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

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

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

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

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale con appositi corsi di formazione.

È importante lavorare in maniera incisiva su questo tema, con azioni formative, supportate dalla pratica didattica quotidiana, volta ad eliminare qualsiasi tipo di discriminazione.

La scuola, attraverso l'attività di alcuni docenti principalmente di materie umanistiche, deve promuovere la lettura collettiva di quotidiani o siti internet e portare all'attenzione dei ragazzi quanto l'Hate speech sia presente quotidianamente senza che questo susciti la dovuta indignazione da parte dell'opinione pubblica. Un linguaggio quotidiano volgare, brutale e offensivo, discriminante che ha preso piede grazie ai social e si è diffuso ovunque, abbassa i livelli di accettazione e assottiglia la

linea di confine tra lecito e illecito, giusto e ingiusto, buono e cattivo, quindi va ad incidere direttamente e fortemente nella dimensione etica e valoriale degli individui, specialmente "in formazione".

E' doveroso per la scuola occuparsi di insegnare "da capo" un linguaggio RISPETTOSO anche della diversità.

# 4.4 - Dipendenza da Internet e gioco online

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

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

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale con appositi corsi di formazione.

A scuola, durante le lezioni, l'utilizzo di apparecchiature informatiche è regolamentato e gli studenti possono servirsi di computer e/o smartphone solo su autorizzazione del docente ed esclusivamente per fini didattici.

Nei momenti di pausa o fuori dalla scuola i ragazzi utilizzano liberamente le loro strumentazioni informatiche ed il rischio di abuso di internet risulta essere molto reale. La prevenzione riveste quindi un ruolo essenziale per evitare di essere attratti dal luccichio di facili guadagni attraverso giochi online e falsi investimenti.

L'Istituto ha negli anni aderito a progetti di formazione per la prevenzione del gioco d'azzardo che utilizzavano approcci innovativi e coinvolgenti, facendo giocare gli alunni e mettendo nel contempo in evidenza le percentuali di vincita e di perdita di varie tipologie di gioco d'azzardo. La consapevolezza della statistica percentuale di perdita aveva quindi il fine di disincentivare il giocatore.

La scuola intende predisporre un questionario ad hoc ANONIMO, per raccogliere dati sul gioco on line, le tipologie, le ore trascorse davanti allo schermo, per comprendere la portata del fenomeno nella nostra realtà. In base alla dimensione del problema, in collaborazione con gli enti e le istituzioni presenti sul territorio (esempio: Coeso

Società della Salute Grosseto), l'Istituto intende attivarsi per individuare soluzioni.

## 4.5 - Sexting

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

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale con appositi corsi di formazione.

È importante lavorare con i ragazzi e con le ragazze sul rispetto per gli altri e per se stessi

Il fenomeno è molto più diffuso di quanto gli adulti possano pensare perché va di pari passo con l'uso di internet che sostituisce le relazioni personali acuito dalla recente pandemia.

Uno dei modi per contribuire a limitare il problema, oltre a diffondere consapevolezza sui rischi connessi al cyberbullismo, grooming, revenge porn ecc.. , è quello di favorire il più possibile incontri dal vivo, relazioni live interpersonali, gite, uscite didattiche, cene di gruppo... attività che qualche anno fa occupavano naturalmente il tempo libero dei ragazzi arricchendo la loro sfera affettiva, ma che oggi risultano talmente ridotte da rendere necessario l'intervento delle istituzioni (come scuola, associazioni sportive, associazioni parrocchiali, ecc...) per ricreare occasioni di incontro.

### 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.

La scuola deve diffondere conoscenza e consapevolezza sui rischi che si corrono, specialmente da adolescenti e a tal fine intende coinvolgere gli studenti/esse:

- Partecipando ad eventi ed incontri con esperti della Polizia postale
- Organizzando cicli di incontri con la Polizia di Stato, per le classi del biennio e con l'Arma dei Carabinieri per le classi quinte per la prevenzione e la sensibilizzazione sui reati legati all'utilizzo di internet e delle piattaforme online
- Attivare uno sportello d'ascolto

## 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 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 <u>Telefono Azzurro</u> e "STOP-IT" di Save the Children.

La scuola intende diffondere conoscenza e consapevolezza sul REATO di pedopornografia per questo intende, con l'aiuto e il sostegno delle forze dell'Ordine, pianificare incontri e/o eventi coinvolgendo il maggior numero di classi.

## Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).

Scegliere almeno 1 di queste azioni:

□ Organizzare uno o più incontri per la promozione del rispetto della

diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

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

#### 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.

# 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 minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting**: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

segnalare la presenza di materiale pedopornografico online.

L'attività di prevenzione della scuola parte dal creare un rapporto di fiducia con gli alunni che li renda liberi di esprimersi manifestando sentimenti di gioia ma anche, eventualmente, di paura/insofferenza/disagio. Occorre considerare che spesso atteggiamenti sbagliati verso compagni o l'utilizzo errato di internet avviene con device propri e quindi difficilmente controllabili.

Per questo motivo oltre alla formazione, il rapporto di fiducia docente-discente è essenziale. Lo studente deve avere consapevolezza del fatto che può contare sui docenti, può rifersi a loro per segnalare situazioni che creano a lui o ad altri compagni disagio. Il docente dovrà essere formato per riconoscere il problema e attivare la procedura corretta in base alla gravità della situazione mettendosi in contatto con il team della prevenzione coordinato dal referente bullismo.

La formazione intrapresa dalla scuola è indirizzata ai vari ambiti di rischio che possono coinvolgere l'adolescente. I docenti possono frequentare diversi corsi tematici attivati da enti territoriali locali od enti esterni, sia in presenza che on line. Formarsi è di estrema importanza poiché crea nel soggetto formato un bagaglio di parole chiave e la conoscenza di possibili situazioni tipiche che lo rendono in grado di riconoscere campanelli d'allarme ai quali prestare maggior attenzione.

L'istituto può contare su una procedura di segnalazione precisa per i casi di bullismo e cyberbullismo. Le fasi di tale procedura, in base alle linee guida della Legge del 2017, prevedono il coinvolgimento per step di vari soggetti a partire da docenti, personale ATA, referente bullismo, Dirigente Scolastico, genitori e per i casi più gravi Autorità esterne predisposte.

# 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.

Nella nostra scuola la prevenzione ai rischi legati al bullismo ed al cyberbullismo è attuata attraverso la partecipazione a progetti di enti esterni promossi dal referente per il bullismo ed il cyberbullismo che forma ogni anno gli studenti di ogni indirizzo. Nelle giornate di formazione il referente comunica agli studenti le procedure di segnalazione e li invita, in caso di necessità, a scrivere direttamente alla sua email o comunque a segnalare ancor più rapidamente il disagio al coordinatore di classe che poi si metterà a sua volta in contatto con lui.

Nel sito della scuola è inoltre presente in evidenza un'area dedicata nella quale è possibile leggere la normativa di riferimento e reperire i contatti da poter utilizzare per le segnalazioni.

Gli studenti, attraverso le apposite procedure, sono invitati a segnalare episodi che possono potenzialmente rientrare nell'ambito della fattispecie dei fenomeni di

bullismo, cyberbullismo, uso inappropriato della rete come navigazione in siti che inneggiano all'odio e/o con contenuti inappropriati per l'età degli alunni.

Il referente bullismo, informato di tali fatti direttamente dallo studente o dai colleghi, provvede ad informare la Dirigente.

Delle attività dirette ad acquisire maggiori informazioni su di uno specifico evento segnalato viene sempre redatto apposito verbale.

### 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.

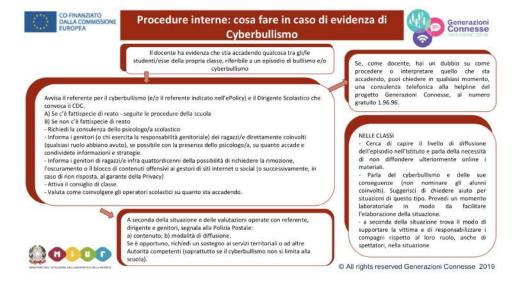
La scuola collabora con diversi enti territoriali ai fini della prevenzione.

A cadenza annuale vengono organizzati interventi della polizia postale o del nucleo carabinieri di Grosseto diretti alla formazione degli studenti e corsi di formazione per i docenti promossi dalla Asl Toscana sud est.

Con L'Ufficio scolastico provinciale e con le scuole del territorio è stata istituita dal 2022 una Rete con finalità di prevenzione al bullismo ed al cyberbullismo della quale la nostra scuola è Capofila.

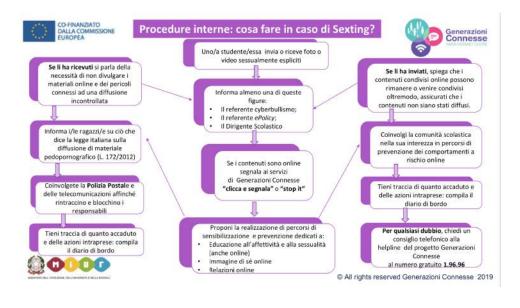
## 5.4. - Allegati con le procedure

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

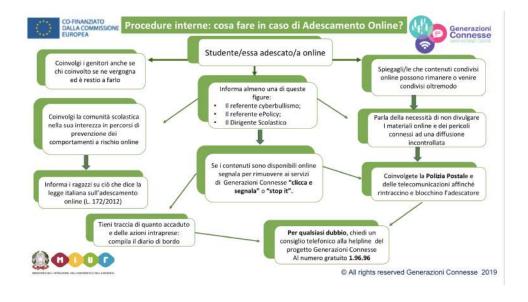




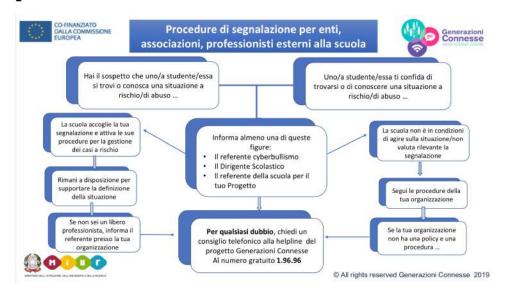
#### Procedure interne: cosa fare in caso di sexting?



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



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



### Altri allegati

- Scheda di segnalazione
- <u>Diario di bordo</u>
- iGloss@ 1.0 l'ABC dei comportamenti devianti online
- Elenco reati procedibili d'ufficio

All'interno dell'Istituto tra gli studenti non si sono ravvisati eventi riconducibili a rischi quali sexting, adescamento on line, pedopornografia o hate speech. Situazioni legate ad un iniziale abuso dell'utilizzo di internet e/o gioco d'azzardo on line che potessero creare dipendenza sono state trattate con progetti mirati alla prevenzione ed alla formazione che la scuola ha attivato in passato e cerca, se possibile, ogni anno di riproporre. In caso di necessità e per gestire al meglio eventuali casi che si dovessero verificare l'Istituto tiene in considerazione le procedure messe a disposizione da Generazioni Connesse nello schema allegato.

La scuola ha un codice interno per la prevenzione del bullismo e cyberbullismo nel quale, oltre ad informative per docenti, studenti e genitori vengono indicati i comportamenti da tenere nella circostanza in cui sia ravvisabile una situazione riconducibile al fenomeno.

Il docente che assiste oppure viene a conoscenza in altro modo di un fatto che potenzialmente può configurare ipotesi di bullismo o cyberbullismo, tenendo a mente la tabella indicata nel Codice per l'analisi dei fatti, deve:

- 1. Annotare nel registro di classe in modo dettagliato lo svolgimento dei fatti qualora gli stessi siano avvenuti in sua presenza oppure, in caso contrario, accertarsi dell'accaduto cercando di comprendere meglio la dinamica degli eventi, ascoltando testimonianze e dichiarazioni, tutelando al contempo la privacy dei soggetti coinvolti
- 2. Qualora dall'analisi dei fatti il docente ravvisi un caso anche solo sospetto di bullismo o cyberbullismo dovrà contattare il coordinatore di classe che avrà cura di informare tempestivamente il Referente Bullismo. A seguito di tale confronto, qualora l'evento venga valutato rientrare in una delle casistiche di bullismo o cyberbullismo, si procederà come segue:
- Confronto tra alunni coinvolti alla presenza del Referente Bullismo, del coordinatore di classe e di almeno un altro docente della classe.
- Comunicazione e richiesta colloquio con le famiglie degli alunni coinvolti al fine di chiarire la dinamica dei fatti, condividere opzioni di intervento in seno alla scuola e/o ulteriori eventuali forme di intervento esterne all'Istituzione.
- Richiesta al DS di convocazione del consiglio di classe straordinario per stabilire strategie di primo intervento individuali e per il gruppo classe alla presenza del Referente Bullismo che dovrà darne esito al Dirigente Scolastico.
- 3. Qualora le strategie di primo intervento attuate dalla scuola non avessero esito positivo si procederà, per cercare di risolvere la situazione, ad un secondo colloquio alla presenza del DS o suo delegato, delle famiglie degli studenti coinvolti, di almeno due docenti del CdC e degli stessi alunni.

Il codice interno della scuola è strutturato per raggiungere, ove possibile, una naturale conciliazione delle controversie che si sono verificate qualora vi sia volontà unanime in

tal senso delle famiglie e degli alunni coinvolti. Nei casi più complessi i docenti del team per la prevenzione si avvalgono anche del parere della psicologa se tale servizio è attivato. Qualora i tentativi di composizione non producono risultati positivi o l'azione commessa è grave la scuola segnalerà la situazione alle Autorità competenti.

## Il nostro piano d'azioni

Non è prevista nessuna azione.