Istituto Comprensivo GROSSETO 2

Presidenza - Segreteria Piazza F.lli Rosselli, n. 14 - 58100 Grosseto
Centralino: tel. 0564/22132 - Fax 0564/21871 Cod. fisc. 80002140533
E-mail: gric829001@istruzione.it **Posta certificata:** gric829001@pec.istruzione.it**Sito web:** www.comprensivo2.gr.it

Documento di ePolicy

I.C. Grosseto 2

INDICE

Capitolo 1 - Introduzione al documento di ePolicy

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 ePolicy, 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'ePolicy, 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'ePolicy 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 sicurezzaonline 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 noncorretto delle tecnologie digitali.

Perché è importante dotarsi di una ePolicy?
Attraverso l'ePolicy 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, criticoed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

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

Il documento vuole presentare in maniera chiara ed esaustiva le **linee guida dell'Istituto Comprensivo Grosseto 2** in materia di:

- utilizzo consapevole delle TIC nella didattica e negli ambienti scolastici;
- prevenzione/gestione di situazioni problematiche relative all'uso delle tecnologie digitali.

Lo **scopo del presente documento**, che potrà essere revisionato annualmente, è quello di informare l'utenza per un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente.

La Scuola opererà:

– descrivendo le norme comportamentali e le procedure atte a facilitare e a promuovere l'uso delle TIC nelladidattica e negli ambienti scolastici;

- stabilendo le misure per la prevenzione e per la rilevazione e la gestione delle problematiche connesse a unuso non consapevole e/o scorretto delle tecnologie digitali;
- dando disposizioni per la segnalazione di casi di uso scorretto e/o non consapevole;
- fornendo indicazioni per la gestione dei suddetti casi;
- attivando misure a supporto delle famiglie e degli studenti che sono stati vittime o spettatori attivi e/o passividi quanto avvenuto.

2. Ruoli e responsabilità

Affinché l'ePolicy 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 presente documento è condiviso da tutte le componenti educative che operano nella scuola ed in esso sono individuati ruoli e responsabilità correlate, così come di seguito indicati.

1) **Dirigente Scolastico** dovrà:

- garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- garantire ai propri docenti una formazione di base sulle Tecnologie dell'Informazione e della Comunicazione (ICT) tale da consentire loro il possesso delle competenze necessarie all'utilizzo di tali risorse;
- garantire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on line.

2) **Animatore Digitale**, come da PNSD, dovrà:

- stimolare la formazione interna alla scuola negli ambiti del PNSD, attraverso l'organizzazione di laboratori formativi, favorendo l'animazione e la partecipazione di tutta la comunità scolastica alle attività formative;
- favorire la partecipazione e stimolare il protagonismo degli studenti nell'organizzazione di workshop e altre attività, anche strutturate, sui temi del PNSD, con momenti formativi aperti alle famiglie e ad altri attori delterritorio, per la realizzazione di una cultura digitale condivisa;
- individuare soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno degli ambienti della scuola (es. uso di particolari strumenti per la didattica di cui la scuola si è dotata; adozione di metodologie comuni; informazione su innovazioni esistenti in altre scuole; laboratorio di coding per tutti gli studenti), coerenti con l'analisi dei fabbisogni della scuola stessa, anche in sinergia con attività di assistenza tecnica condotta da altre figure.

3) **Direttore dei Servizi Generali e Amministrativi** dovrà:

- assicurare, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione richiesti da cattivo funzionamento e/o danneggiamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate;
- facilitare la trasmissione di comunicazioni relative alle tecnologie digitali tra le varie componenti della scuola(Dirigente scolastico, Animatore digitale, docenti e famiglie degli alunni);
- curare la registrazione dei disservizi e delle problematiche relative alla rete e all'uso del digitale segnalate dai docenti, provvedendo all'intervento del personale tecnico di assistenza.

4) **Docenti di tutte le discipline** dovranno:

- provvedere alla propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti dei materiali reperiti in Internet e dell'immagine degli altri, lotta al cyberbullismo);
- sviluppare le competenze digitali degli alunni e fare così in modo che conoscano e seguano le norme di sicurezza nell'utilizzo del web e utilizzino correttamente le tecnologie digitali sia a scuola sia nelle attività didattiche extracurricolari;
- segnalare prontamente alle famiglie eventuali problematiche emerse in classe nell'utilizzo del digitale e

stabilire comuni linee di intervento educativo per affrontarle;

- segnalare al/lla Dirigente Scolastico/a e ai/alle suoi/sue collaboratori/trici eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazioni.

5) **Alunne e alunni** dovranno:

- ascoltare e seguire le indicazioni fornite dai/lle docenti per un uso corretto e responsabile delle tecnologiedigitali, attuando le regole di *e-safety* per evitare situazioni di rischio;
- chiedere l'intervento dell'insegnante, o dei genitori/tutori a casa, nello svolgimento dei compiti per mezzo del digitale, qualora insorgano difficoltà o dubbi nel suo utilizzo.

6) **Genitori/tutori** dovranno:

- contribuire, in sinergia con il personale scolastico, alla sensibilizzazione dei/lle proprie figlie sul tema della sicurezza in rete;
- incoraggiare l'impiego delle TIC da parte delle alunne e degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza;
- agire in modo concorde con la Scuola per la prevenzione dei rischi e l'attuazione delle procedure previste incaso di violazione delle regole stabilite;
- supportare le azioni intraprese dalla Scuola.

3. - Un'informativa per i soggetti esterni che erogano attività 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/lla minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri delle/dei minori, soprattutto se preoccupati/e o allertati/e 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 studentie 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/llDirigente Scolastico/a, con modalità e tempi concordati con il/la Referente d'Istituto per il contrasto del Bullismo e Cyberbullismo; a tal proposito, al fine di verificare preventivamente il contenuto da somministrare o dibattere con la scolaresca, i soggetti esterni forniranno un dettagliato programma delle attività con narrazione sintetica della scaletta, al fine di essere autorizzato dalla Dirigenza.

4. - Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

Il documento di ePolicy 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/lle docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.

L'ePolicy 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'iniziodell'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/e sul fatto che sono monitorati/e e supportati/e nella navigazione online, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

Allo scopo di condividere regole comuni per l'utilizzo sicuro di Internet sia a casa che a scuola, si invitano tutti i genitori a prestare la massima attenzione ai principi e alle regole contenute nel presente documento.

Si richiede che ogni genitore e/o tutore si impegni a farle rispettare ai propri figli e alle proprie figlie anche in ambito domestico, primariamente assistendo i/le minori nel momento dell'utilizzo della rete e poi ponendo in atto tutti i sistemi di sicurezza che aiutino a diminuire il rischio di imbattersi in materiale indesiderato.

La scuola promuove eventi e dibattiti informativi e formativi, in momenti diversi dell'anno, rivolti a tutto il personale, agli alunni e alle alunne e ai loro genitori, con il coinvolgimento di esperte/i, sui temi oggetto di questo documento.

Tra le misure di prevenzione che la scuola mette in atto vi sono, inoltre, azioni finalizzate a promuovere una cultura dell'inclusione, del rispetto dell'altro e delle differenze così che l'utilizzo di Internet e dei cellulari, oltre che collocarci all'interno di un sistema di relazioni, ci renda consapevoli di gestire con un certo grado di trasparenza i rapporti che si sviluppano in tale ambiente, giungendo a riconoscere e gestire le proprie emozioni.

5. - Gestione delle infrazioni alla ePolicy

La scuola gestirà le infrazioni all'ePolicy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni (si veda il ***Regolamento della disciplina***).

Tutte le infrazioni alla presente ePolicy andranno tempestivamente segnalate al/lla Dirigente Scolastico/a, che avrà cura di convocare le parti interessate onde valutare le possibili azioni da intraprendere. Il/la Dirigente Scolastico/a ha, altresì, la facoltà di revocare l'accessibilità temporanea o permanente ai laboratori e all'utilizzo di strumenti tecnologici (pc, tablet, notebook, smartphone, ecc.) a chi non si attiene alle regole stabilite.

6. - Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico assume integralmente, facendosene garante, i contenuti dell'ePolicy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temiin oggetto.

Il presente documento si integra pienamente con obiettivi e contenuti dei seguenti documenti, che specificanoil contesto di attuazione delle politiche dell'Istituto Comprensivo per un uso efficace e consapevole del digitalenella didattica:

- PTOF
- Regolamento d'Istituto
- Regolamento della disciplina.
- Regolamento per l'utilizzo dei laboratori.

7. - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'ePolicy deve essere aggiornata periodicamente e ogni qualvolta si verifichino 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.

Le regole relative all'accesso ad Internet vengono approvate dal Collegio dei Docenti e dal Consiglio di Istitutoe pubblicate sul sito della scuola.

I genitori/tutori sono invitati a rilasciare il consenso per l'accesso ad Internet e la dichiarazione liberatoria per

la pubblicazione di elaborati, nomi, voci, immagini, materiale audiovisivo sul sito della scuola. (cfr. Allegato 1 al Documento di eSafety Policy).

Le alunne e gli alunni vengono informate/i del fatto che l'utilizzo di Internet è monitorato e vengono date loro istruzioni per un uso responsabile e sicuro.

Tutto il personale scolastico è coinvolto nel monitoraggio dell'utilizzo di Internet, nello sviluppo delle linee guida e nell'applicazione delle istruzioni sull'uso corretto della rete (cfr. Allegato 2 al Documento di eSafety Policy).

Il nostro piano d'azioni

AZIONI da svolgere entro un'annualità scolastica:

- Organizzare 1 evento di presentazione e conoscenza del documento ePolicy rivolto ai docenti.

AZIONI da svolgere nei prossimi 3 anni:

- Monitorare il tipo di utilizzo di Internet da parte degli studenti.
- Sviluppare moduli didattici per lo svolgimento di attività di ricerca, utilizzo critico delle fonti online e rielaborazione dei contenuti.
- Creare moduli didattici per la promozione del rispetto della diversità.
- Organizzare uno o più incontri dedicati alla prevenzione dei rischi associati all'utilizzo di Internet e delletecnologie digitali, rivolti agli studenti, ai docenti e ai genitori con il coinvolgimento di esperte/i.

Capitolo 2 - Formazione e curricolo

1. - Curricolo sulle competenze digitali per gli studenti

I ragazzi e le ragazze usano la Rete quotidianamente, talvolta in modo più "intuitivo" e "agile" rispetto agli adulti, ma non per questo sono dotati/e 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" ("Raccomandazionedel 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.

Le Indicazioni Nazionali del 2012 in raccordo con le Raccomandazioni del Consiglio Europeo relativamente alle Competenze chiave per l'apprendimento permanente prevedono che al termine del primo ciclo di istruzione lo studente e la studentessa posseggano buone competenze digitali e sappiano usare con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo. In questo senso le TIC (Tecnologie dell'Informazione e della Comunicazione) preparano le studentesse e gli studenti a un'attiva e consapevole partecipazione a un mondo in rapida evoluzione e nel quale è necessario acquisire abilità e competenze in grado di facilitare l'adattamento dell'individuo ai continui cambiamenti.

Si rende quindi necessario lo sviluppo e la diffusione di una mentalità tecnologica diffusa e precoce, intesa come alfabetizzazione al senso, all'utilizzabilità in contesti dati e per scopi definiti, da un lato ed acquisizione sempre più consapevole di strategie efficaci per il dominio di una macchina complessa che impiega e genera oggetti immateriali, dall'altro.

Gli alunni dovrebbero quindi imparare ad utilizzare le TIC per cercare, esplorare, scambiare e presentare informazioni in modo responsabile, creativo e con senso critico, essere in grado di avere un rapido accesso a idee ed esperienze provenienti da persone, comunità e culture diverse. Alla scuola spetta quindi anche il compito di trovare raccordi efficaci tra la crescente dimestichezza degli alunni con le Tecnologie dell'Informazione e della Comunicazione e l'azione didattica quotidiana. Le TIC possono infatti offrire significative occasioni per sviluppare le competenze di comunicazione, collaborazione e problem solving.

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 e della DAD;

-promuovere situazioni collaborative di lavoro e di studio;

-sviluppare creatività e capacità di lavorare in gruppo e in modalità sincrona e asincrona;

-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 creativamentele tecnologie, risolvere problemi tecnici, aggiornare la propria competenza e quella altrui.

Obiettivi:

1. migliorare l'apprendimento;

2. favorire l'acquisizione della competenza digitale;

3. servirsi di strumenti in maniera interattiva;

4. interagire in gruppi eterogenei;

5. imparare ad imparare.

Competenze:

- Utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall'attività di studio;

- essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto produttivo, culturale e sociale in cui vengono applicate;

- saper gestire la propria eSafety;

- saper utilizzare la tecnologia per sviluppare il pensiero computazionale e per realizzare simulazioni, test, esercizi, etc.

Conoscenze:

- Le applicazioni tecnologiche e le relative modalità di funzionamento;

- i dispositivi informatici di input e output;

- il sistema operativo, i software e le app, applicativi (residenti e/o cloud), con particolare riferimento ai prodotti anche Open Source;

- procedure per la produzione/elaborazione di testi, dati e immagini, prodotti multimediali;

- procedure di utilizzo delle Reti per la ricerca di informazioni, per la comunicazione, la collaborazione e lacondivisione;

- procedure di utilizzo sicuro e legale della Rete per la ricerca e la condivisione di dati (motori di ricerca, sistemi di comunicazione mobile, e-mail, chat, Social network, cloud, protezione degli account, download, diritto d'autore, etc.). Fonti di pericolo e procedure di sicurezza: e-safety;

- concetti base del coding.

Abilità:

- Utilizzare le Tecnologie dell'Informazione e della Comunicazione per elaborare dati, testi, immagini, video, per produrre artefatti digitali in diversi contesti e per la comunicazione;

- conoscere gli elementi base che compongono un computer e le relazioni essenziali fra di essi;

- collegare le modalità di funzionamento dei dispositivi elettronici con le conoscenze scientifiche e tecniche acquisite;

- utilizzare materiali digitali per l'apprendimento;

- utilizzare il PC, periferiche e programmi applicativi;

- riconoscere potenzialità e rischi connessi all'uso delle tecnologie e della Rete, saper gestire i propri account in funzione della eSafety;

- utilizzare software offline e online per attività di Coding.

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

È fondamentale che le/i docenti tutte/i siano formate/i ed aggiornate/i 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 personale docente partecipa a corsi di formazione anche nell'ambito di piani nazionali, PNSD, oltre che a iniziative organizzate dall'istituzione o dalle scuole associate in rete e possiede generalmente una discreta basedi competenze e, nel caso di alcune figure di sistema, anche di carattere specialistico.

È inoltre disponibile ad aggiornarsi per mantenere al passo la propria formazione, in rapporto al rinnovo della dotazione multimediale.

L'attenzione all'uso delle TIC nella didattica rende gli apprendimenti più motivanti, coinvolgenti ed inclusivi, con una funzione di guida da parte del/lla 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 sincrona e asincrona.

La competenza digitale - oggi - è imprescindibile per i/le docenti, così come per le studentesse e gli studenti, 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.

Il percorso complesso della formazione specifica dei/lle docenti sull'utilizzo delle TIC nella didattica in presenza e/o a distanza non esauribile nell'arco di un anno scolastico, può, pertanto, prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva anche all'interno dell'Istituto, con la condivisione delle conoscenze dei singoli ed il supporto dell'Animatore digitale e del Team per l'innovazione.

3. - Formazione dei/lle docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

La scuola si impegna a promuovere percorsi formativi per le/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.

Anche il percorso della formazione specifica dei/lle docenti sull'utilizzo consapevole e sicuro di Internet, può prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere

permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche le/i ragazze/i.

I momenti di formazione e aggiornamento sono formulati secondo un'analisi del fabbisogno formativo del corpo docente sull'utilizzo ed integrazione delle TIC nella didattica in presenza e a distanza DAD.

Sarà predisposta una sezione online per la messa a disposizione e la condivisione di materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di internet, collegata alla homepage del sito scolastico (https://comprensivo2gr.edu.it). Qui sarà possibile trovare materiali informativi sulla sicurezza in Internet per l'approfondimento personale, per le attività con le studentesse e gli studenti e gli incontri con i genitori/tutori, link a siti specializzati.

4. - Sensibilizzazione delle famiglie/legali tutori e integrazioni al Patto di Corresponsabilità

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

L'Istituto attiverà iniziative per sensibilizzare le famiglie o i legali tutori all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine sono previsti incontri fra docenti e genitori per la diffusione del materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati e dalle forze dell'ordine.

Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo.

Sul sito scolastico, dal quale si potrà accedere a "Generazioni connesse" saranno messi in condivisione materiali dedicati agli/alle alunni/e e alle famiglie/tutori che possono fornire spunti di approfondimento e confronto. La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento di ePolicy e eSafety per portare a conoscenza delle famiglie/tutori il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'Istituto e prevenire i rischi legati a un utilizzo non corretto di Internet.

Gli studenti e le studentesse devono attenersi a quanto previsto dai Regolamenti scolastici e dalle Circolari interne emanate dal/lla Dirigente Scolastico/a, sulla base delle note ministeriali, sull'utilizzo consapevole delle tecnologie digitali all'interno del contesto scolastico. I genitori/tutori nell'azione di corresponsabilità didattico-educativa, rappresentano un punto di forza per l'implementazione dei rapporti "scuola- famiglia", quale garanzia e rispetto degli impegnisottoscritti e condivisi nello stesso Patto di corresponsabilità, di natura anche pedagogica.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024)

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TICnella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro diInternet e delle tecnologie digitali.

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

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TICnella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti/e per i/le docenti sulle competenze digitali.
- Organizzare incontri con esperti/e per i genitori/tutori sull'educazione alla cittadinanza digitale.

Capitolo 3 - Gestione dell'infrastruttura e della strumentazione TIC della e nellascuola

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 comunicazionequesto 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 sulle studentesse e 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 edel Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento deidati personali, nonché alla libera circolazione di tali dati).

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/lle minori. A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare, conformi alla normativa vigente, in materia di protezione dei dati personali.

L'Istituto Comprensivo Grosseto 2 rispetta la privacy dei/lle propri/e utenti e si impegna a proteggere i dati personali che gli/le stessi/e conferiscono all'Istituto.

In generale, l'utente può navigare sul sito web della scuola senza fornire alcun tipo di informazione personale.

Il personale scolastico è "incaricato del trattamento" dei dati personali (delle alunne e degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione).

L'istituto tratta i dati personali forniti dagli/lle utenti in conformità alla normativa vigente.

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 sostanzialie non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi eapplicazioni 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 20022/22/CE relativa al servizio universale e ai diritti degli/lle 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/lle studenti/esse 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 in tutte le aule e nei laboratori d'informatica.

Le impostazioni sono definite dal responsabile dei laboratori e dall'Animatore digitale ed è in carico a ciascun/a docente la segnalazione di malfunzionamenti e disservizi, al fine di richiedere, ove necessario, l'intervento di tecnici esterni.

I/le docenti hanno piena autonomia nel collegamento ai siti web nelle postazioni a loro riservate.

Relativamente alle alunne e agli alunni che accedono a Internet durante l'attività didattica, sono consentiti la navigazione guidata da parte dell'insegnante e la stesura di documenti collaborativi purché sotto il controllo dell'insegnante e nel caso in cui tale attività faccia parte di un progetto di lavoro precedentemente autorizzato.

3. - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

La Scuola è dotata di un sito istituzionale con estensione "edu.it" (https://comprensivo2gr.edu.it) sul quale diversi siti tematici rimandano al contenuto di interesse (pubblicità legale, circolari, ecc).

Pulsanti attivi permettono l'accesso a link di interesse tra cui il registro elettronico.

Il sito prevede un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali, avvisi dicarattere generale e un'area riservata, accessibile solo dopo autenticazione.

Il personale che è in possesso delle credenziali per la gestione dei contenuti sul portale si assumerà la responsabilità editoriale di garantire che il contenuto inserito sia accurato e appropriato.

4. - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei/lle docenti (oltre che di tutte le figure professionali che a vario titolo sono inserite nel mondo della scuola), e 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 piùampio PNSD.

La presente ***ePolicy*** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'utilizzo 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 aspettipositivi ed eventuali criticità nella e per la didattica.

Come meglio indicato nel D.M. 15 marzo 2007, n. 30 "la scuola è una risorsa fondamentale in quanto assume il ruolo di luogo di crescita civile e culturale per una piena valorizzazione della persona, rafforzando l'esistenzadi una comunità educante in cui ragazze/i e adulte/i, docenti e genitori/tutori, vengano coinvolti in un'alleanza educativa che contribuisca ad individuare non solo contenuti e competenze da acquisire ma anche obiettivi e valori da trasmettere per costruire insieme identità, appartenenza, e responsabilità.

Si rende, comunque, necessario rispettare quanto stabilito dal Regolamento di Istituto in merito all'utilizzo di dispositivi elettronici personali da parte di tutti gli attori scolastici durante le attività didattiche ed educative.

Ai sensi del Regolamento d'Istituto è vietato l'utilizzo del telefono cellulare e di altri dispositivi elettronici durante tutte le attività scolastiche, sia per comunicare che per effettuare riprese video e/o sonore (C.M. del 15 marzo 2007). Come stabilito dalla Nota MIM 107190 del 19/12/2022, è consentito l'utilizzo di tali dispositivi in classe, quali strumenti compensativi di cui alla normativa vigente, nonché, in conformità al Regolamento d'istituto, con il consenso del docente, per finalità inclusive, didattiche e formative, anche nel quadro del Piano Nazionale Scuola Digitale e degli obiettivi della c.d. "cittadinanza digitale" di cui all'art. 5 L. 25 agosto 2019, n. 92.
Riguardo alle alunne e agli alunni con disturbi specifici di apprendimento, i genitori/tutori sono tenuti a concordare con le/i docenti le modalità di impiego di strumenti compensativi quali tablet e computer portatili.

Ai sensi della Direttiva Ministeriale n. 30 del 15 marzo 2007, con la condivisione della presente Policy, "le famiglie si assumono l'impegno di rispondere direttamente dell'operato dei propri figli e delle proprie figlie nel caso in cui, ad esempio, gli/le stessi/e arrechino danni ad altre persone" a seguito di violazioni del presente regolamento.

Ai sensi del Regolamento d'Istituto il divieto di utilizzare il cellulare è da intendersi rivolto a tutto il personale della scuola, salvo diverse autorizzazioni disposte dal/lla Dirigente Scolastico/a per necessità motivate. Durante le ore delle lezioni, quindi, non è consentito l'utilizzo del cellulare, mentre è consentito l'uso di altri dispositivi elettronici personali solo a scopo didattico e integrativo rispetto a quelli scolastici disponibili, se autorizzato dai/lle docenti.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024)

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola.
- Organizzare 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).

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

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrareindicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola.
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delletecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologiedigitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accessoad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity).

Capitolo 4 - Rischi online: conoscere, prevenire e rilevare

1. - Sensibilizzazione e prevenzione

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

- commettere azioni online che possano danneggiare se stessi o altre/i;
- essere una vittima di queste azioni;
- osservare altri/e 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 le ragazze e 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/a 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.*

Al personale che opera nella scuola, e in modo particolare alle/agli insegnanti, viene oggi offerta la possibilità di essere promotori e garanti della costruzione dialogica di un percorso formativo partecipato.

La prima responsabilità delle/gli insegnanti consiste, dunque, nell'imparare a riconoscere i rischi più comuni che le ragazze e i ragazzi possono correre sul web, per potere poi intervenire adeguatamente.

Come sappiamo, le dimensioni che il fenomeno può determinare sono molteplici e riconducono alla capacità di gestione di dinamiche complesse, mediante confronto/relazione con il sé e l'altro, dimensioni dell'affettività e, ancora, mediante il riconoscimento di un limite tra dimensione di legalità ed utilizzo sicuro delle tecnologiedigitali.

Per questo motivo la scuola intende perseguire azioni per rispondere ai bisogni dell'utenza, attraverso una risposta integrata con la rete dei servizi territoriali locali (tra cui ASL, Polizia postale, etc.).

Si pone dunque la necessità di sensibilizzare ad un uso positivo e consapevole delle TIC le studentesse e gli studenti, non solo in un'ottica di tutela dai rischi potenziali ma anche della valorizzazione delle opportunità esistenti. Tutto ciò, pone la scuola e i genitori di fronte alla sfida di riconsiderare il proprio ruolo educativo e le proprie risorse, oltre allo stato dei rapporti reciproci per un patto educativo da rinnovare costantemente.

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 diminorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche unoo 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/a proprio/a referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo delle studentesse e degli studenti (ed ex studenti/sse) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei/lle minori coinvolti;
- integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte dicyberbullismo 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, delle associazioni e dei centri di aggregazione giovanile del territorio.
  - potrà svolgere un importante compito di supporto al/lla Dirigente Scolastico/a per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Si definiscono ***bullismo*** tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o a volte un piccolo gruppo). Si tratta, pertanto, di una serie di comportamenti portati avanti ripetutamente nel tempo. Si parla di cyberbullismo quando queste forme di prevaricazione reiterate nel tempo si estendono anche alla vita online. Tale specifica forma di bullismo ha caratteristiche peculiari:

1) è pervasivo: il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo;

2) è un fenomeno persistente: il materiale messo online vi può rimanere per molto tempo;

3) spettatori e cyberbulli sono potenzialmente infiniti: le persone che possono assistere agli atti di cyberbullismo sono potenzialmente illimitate.

Occorre tenere presente che il cyberbullo non è mai del tutto consapevole della gravità dei suoi comportamentise non viene aiutato ad esserne consapevole.

Qualora ci si trovi di fronte ad un caso di cyberbullismo si dovrà:

- informare i genitori/tutori degli/lle alunni/e coinvolti/e;
- coinvolgere il/la referente di istituto dell'eSafety e gli/le operatori/trici scolastici/che su quanto sta accadendo;
- coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online;
- tenere traccia di quanto successo e delle azioni intraprese, compilando un "diario di bordo" perconsentire ulteriori indagini se necessarie.

Azioni condivise tra scuola e famiglia al fine di intervenire preventivamente ed efficacemente, per 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 la possibilità di coinvolgere anche un servizio specialistico socio-sanitario (Consultorio familiare, Servizi di Neuropsichiatria,etc.), quale supporto e/o forme di mediazione.

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 è estremamente importante affrontarlo anche a livelloeducativo e scolastico con l'obiettivo di:

- fornire alle studentesse e 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.

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

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

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?

Al personale che opera nella scuola, e in modo particolare alle/agli insegnanti, viene oggi offerta la possibilità di essere promotori e garanti della costruzione dialogica di un percorso formativo partecipato, ma il loro ruolo diventa spesso inevitabilmente quello di confidenti delle alunne e degli alunni e delle loro esperienze.

Le/gli insegnanti dovranno imparare a riconoscere i rischi più comuni che le/i ragazze/i possono correre sul web, per potere poi intervenire adeguatamente. Se è vero che le tecnologie digitali sono un valido strumento compensativo per qualsivoglia bisogno educativo speciale delle studentesse e degli studenti, è anche vero che occorre 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.

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 le/i giovanissime/i 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 le/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 emotivoche si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro e depressione.

Qualora ci si trovi di fronte a un caso di sexting (con cui si intende l'invio e/o la ricezione e/o la condivisionedi testi, video o immagini sessualmente esplicite via cellulare o tramite internet) si dovrà:

- coinvolgere la classe e confrontarsi con esperte/i, facendo appello, per esempio, a eventuali sportellid'ascolto per capire come approfondire e affrontare il fenomeno;
- coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti riconducibili alsexting;
- intraprendere con la classe attività mirate a riflettere sulla fiducia che ciascuno/a ripone negli/lle altri/e e sul fenomeno del sexting.

6. - Adescamento online

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

Le tecnologie digitali consentono ai/lle giovani di ampliare la propria rete di amicizie in modo quasi smisurato: non di rado gli/le adolescenti "concedono" la loro amicizia non solo a persone che conoscono direttamente, ma anche ad "amici/che di amici/che". Questo li/le espone a rischi notevoli, come quello di dare accesso a sconosciuti/e al loro mondo online e quindi a informazioni personali.

È bene che anche le/gli insegnanti aiutino le proprie alunne e i propri alunni a tutelarsi, scegliendo con cura chi frequentare online, per evitare che una condotta imprudente possa comportare ripercussioni non banali nella loro vita reale. Una volta riconosciuti alcuni segni che possono rinviare a una situazione di adescamento online, quali un improvviso calo nel rendimento scolastico, un aumento del tempo trascorso dall'alunna/o online congiunto ad una particolare riservatezza al riguardo, allusioni da parte dell'alunna/o alla frequentazione di una persona più grande, o a regali ricevuti, ecc., è bene:

- approfondire la situazione coinvolgendo la classe e l'intera comunità scolastica;
- avviare dei percorsi di riflessione in classe sul concetto di fiducia;
- farsi affiancare da esperte/i, ricorrendo anche ad eventuali sportelli d'ascolto per offrire alle/ai minori, qualora lo desiderino, il supporto necessario.

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 messo 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 e 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 possonocondividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se sivogliono 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 Telefono Azzurro e "STOP-IT" di Save the Children.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024)

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

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 ai genitori/tutori e alle/ai docenti, con il coinvolgimento di esperte/i.
- 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 delle studentesse e degli studenti.
- Organizzare uno o più eventi e/o dibattitti in momenti extra-scolastici sui temi della diversità e sull'inclusione rivolti a genitori/tutori, studenti/studentesse e personale della scuola.
- Pianificare e realizzare progetti di peer-education sui temi della sicurezza online nella scuola.

Capitolo 5 - Segnalazione e gestione dei casi

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 gestionedel caso**;
- le modalità di coinvolgimento del/lla referente per il contrasto del bullismo e del cyberbullismo, oltre al/lla Dirigente Scolastico/a.

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 esulino 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/tutori e a tutti/e 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 coinvolgano i genitori/tutori, 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 allavittima? 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 a 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/lle minori e il rischio che corrono. Si ricorda 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/la 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 avràprovveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

La diffusione capillare dei social network tra i/le bambini/e e ancor più tra gli/le adolescenti li/le espone sempre più spesso al rischio di inviare o condividere senza alcuna protezione materiali personali o riservati. Discutendo in classe dei rischi del web e confrontandosi sulle esperienze personali o dei/delle propri/e coetanei/e, emergono spessofatti che "allarmano" l'insegnante. Tuttavia, mentre l'insegnante ha la possibilità, anzi il dovere, di intervenire sui dispositivi digitali in uso a scuola, non può intervenire direttamente sui telefoni cellulari dei/delle bambini/e senza un'esplicita autorizzazione delle famiglie o dei legali tutori.

Tra i contenuti andranno opportunamente segnalati:

- contenuti afferenti la violazione della privacy: foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici e amiche, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.;
- contenuti afferenti all'aggressività o alla violenza: messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano alsuicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.;
- contenuti riconducibili alla sfera sessuale: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche e pedopornografia, ecc.

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 deicontenuti 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/la 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/la 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 visibiledella 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.

Il personale della scuola, anche con l'ausilio del personale di assistenza tecnica e dell'Animatore digitale, dovrà provvedere a conservare le eventuali tracce di una navigazione non consentita su Internet o del passaggiodi materiali inidonei sui pc della scuola; la data e l'ora consentiranno di condurre più approfondite indagini; nel caso di messaggi, si cercherà di risalire al mittente attraverso i dati del suo profilo. Sia nel caso di chat chedi messaggi di posta elettronica, l'insegnante dovrà copiare e stampare i messaggi per fornire le eventuali prove dell'indagine sugli abusi commessi.

Tali prove saranno utili anche a informare la famiglia o i tutori dell'alunno/a vittima di abuso, il/la Dirigente Scolastico/a e, ove si configurino reati, la Polizia Postale.

In ogni caso, sarà opportuna una tempestiva informazione delle famiglie o dei tutori legali in merito all'accaduto, anche per consentire ulteriori indagini e, in assenza di prove oggettive, di raccogliere testimonianze sui fatti da riferire al/lla Dirigente Scolastico/a e, eventualmente, alla Polizia Postale.

Qualora siano coinvolti/e più alunni/e, in qualità di vittime o di responsabili della condotta scorretta, le famiglie/tutori degli/lle alunni/e in questione saranno informate tempestivamente per un confronto.

In base all'entità dei fatti si provvederà:

1) a una comunicazione scritta tramite diario alle famiglie o ai legali tutori;
2) a una nota disciplinare sul registro di classe;
3) a una convocazione formale dei genitori/tutori degli/lle alunni/e, tramite segreteria;
4) a una convocazione delle famiglie/tutori da parte del/lla Dirigente Scolastico/a.

Per i reati più gravi le operatrici e gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti).

Inoltre ci si potrà avvalere dei due servizi messi a disposizione dal Safer Internet Center il "Clicca e Segnala"di Telefono Azzurro e "STOP-IT" di Save the Children. Una volta ricevuta la segnalazione, infatti, gli operatori e le operatrici procederanno a coinvolgere le autorità competenti in materia.

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).

È bene sempre dialogare con la classe, attraverso interventi educativi specifici, cercando di sensibilizzare le studentesse e gli studenti sulla necessità di non diffondere ulteriormente online i materiali dannosi, ma anzi di segnalarli e bloccarli.

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 dallecompetenze e possibilità della scuola.

Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse

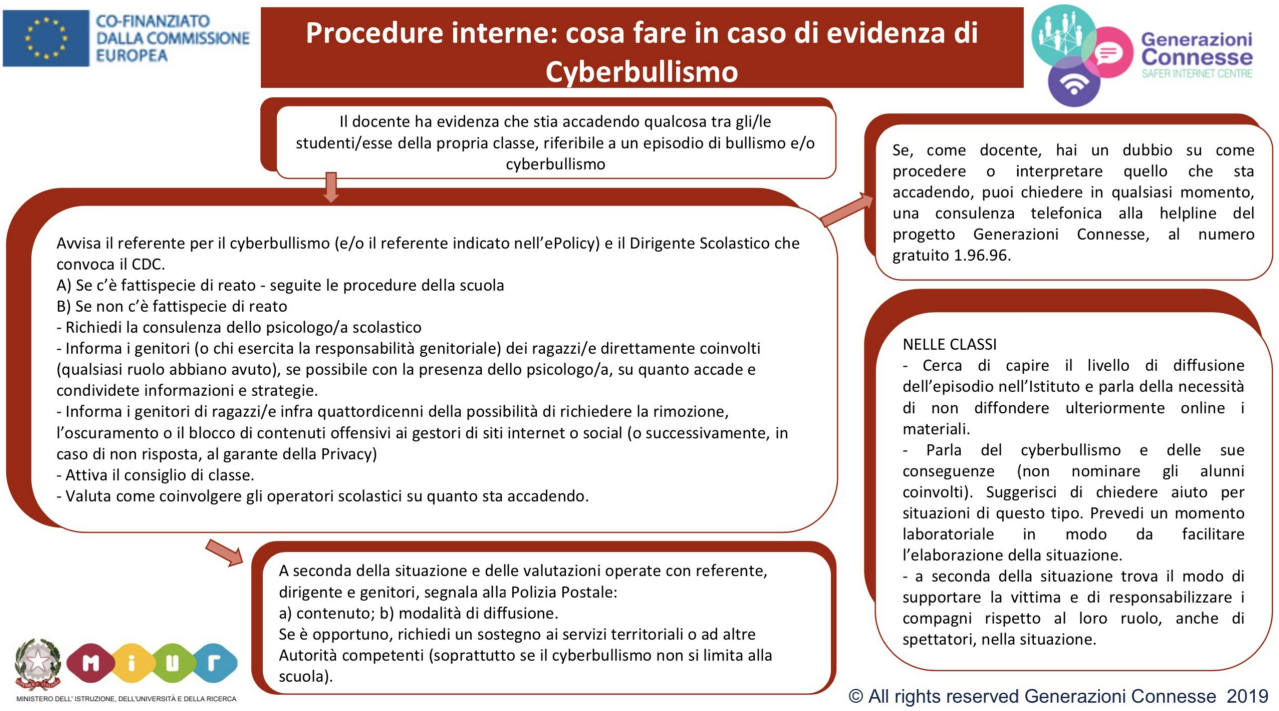
"Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente e un supporto 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.

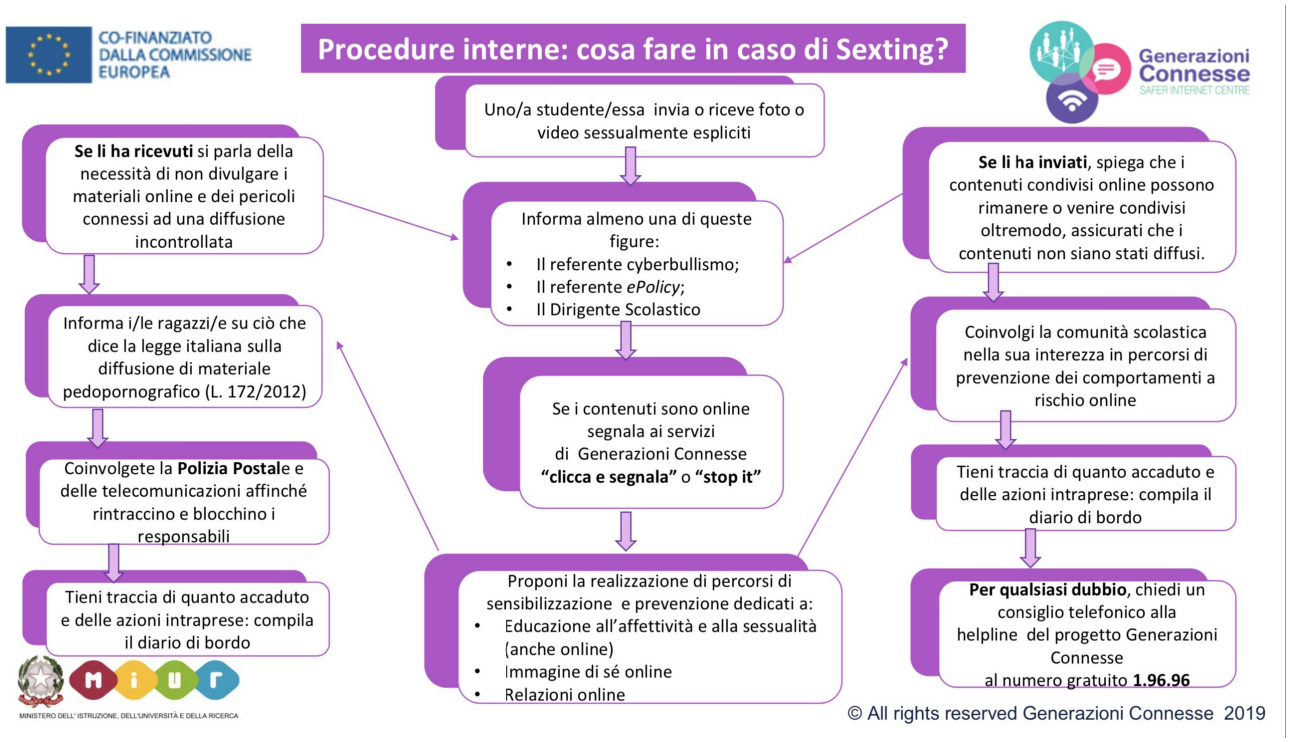
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei/lle minori.
- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione e 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/lle 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/lle minori.

4. – Suggerimenti per le procedure da seguire

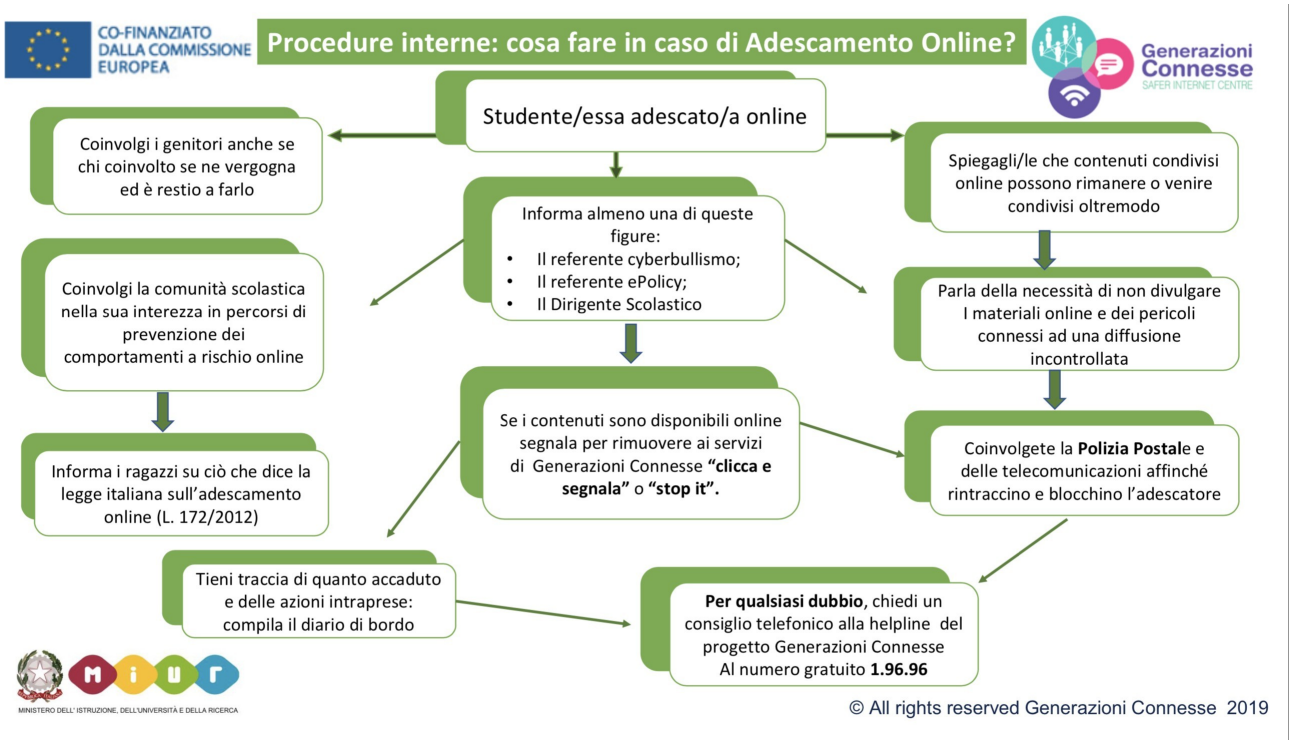
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



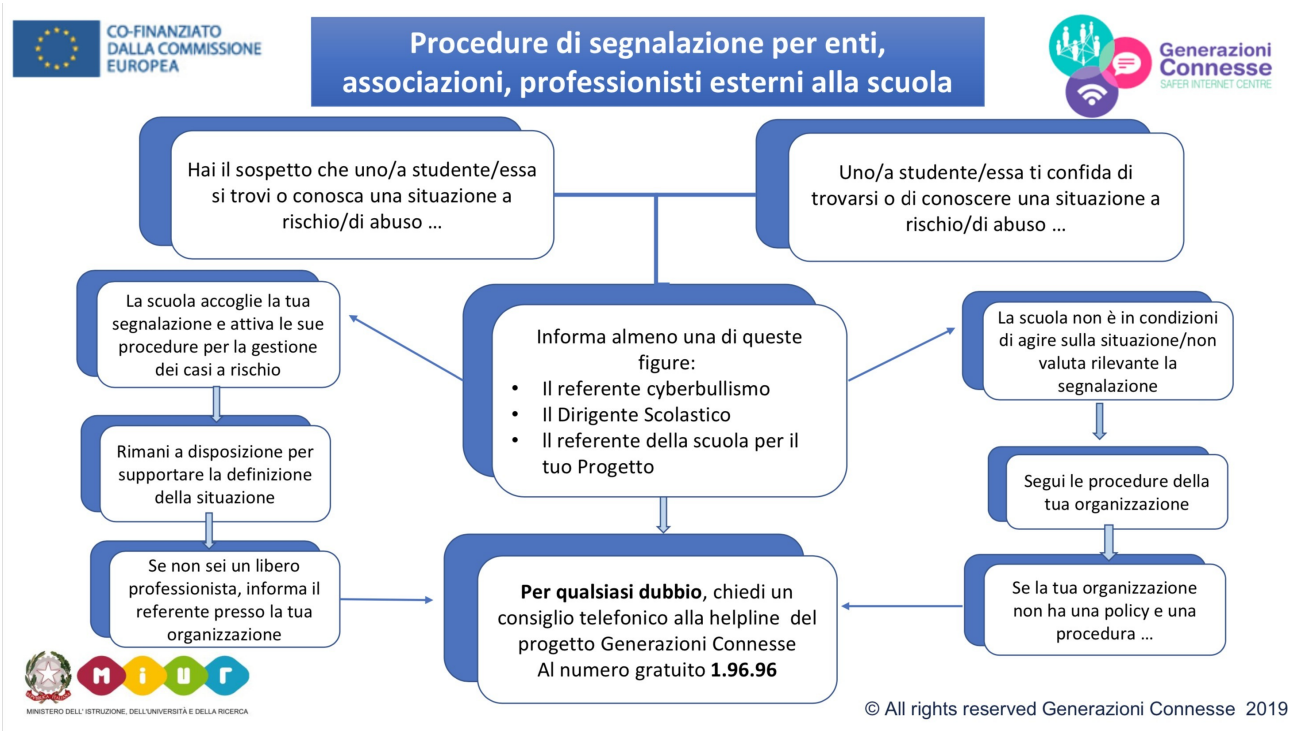
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Il nostro piano d'azioni

L'obiettivo che l'insegnante deve proporsi dopo aver riconosciuto il pericolo è agire di conseguenza, con azionidi contrasto efficaci e mirate, rispetto ai rischi sopra elencati.

Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte deglistudenti e delle studentesse in orario scolastico, vi sono le seguenti:

- diffondere un'informazione capillare rivolta al personale scolastico, agli/lle studenti/sse e alle famiglie o ai tutori, sui rischi che i/le minori possono correre sul web, condividendo materiali prodotti dalla scuola o reperibili su siti specializzati (vedi "Generazioni connesse");
- far rispettare il divieto di utilizzo di dispositivi digitali propri, quali cellulare e smartphone, alle studentesse e agli studenti in orario scolastico;
- dotare i dispositivi della scuola di filtri che impediscano l'accesso a siti web non adatti ai minori (black list);
- bloccare l'accesso a un sito o a un insieme di pagine impedendone la consultazione;
- controllare periodicamente i siti visitati dalle alunne e dagli alunni;
- utilizzare un software in grado di intercettare le richieste di collegamento e di respingere quelle non conformi alle regole stabilite dall'amministratore;
- affidare a un gruppo di docenti scelto le regole di filtraggio.

A tal proposito, la scuola proporrà incontri formativi atti a favorire momenti di riflessione e attività laboratoriali.

Altri allegati

Allegato 1- *Documento di ePolicy: Consenso dei genitori/tutori per l'accesso a Internet e dichiarazione liberatoria per la pubblicazione di elaborati, nomi, voci, immagini, materiale audiovisivo sul sito della scuola.*

Allegato 2 - *Documento di ePolicy: Assunzione di responsabilità da parte di Docenti e altro Personale della Scuola.*

Allegato 1 Documento di ePolicy

CONSENSO DEI GENITORI/TUTORI PER L'ACCESSO A INTERNET E DICHIARAZIONE LIBERATORIA PER LA PUBBLICAZIONE DI ELABORATI, NOMI, VOCI, IMMAGINI, MATERIALE AUDIOVISIVO

Alla Dirigente dell'Istituto Comprensivo Grosseto 2

I sottoscritti ..... e .....,

genitori/tutori dell'alunno/a ..... iscritto/a alla classe ..... sez. .....

della scuola dell'infanzia/primaria/secondaria di primo grado .....

Dichiarano

- di aver letto e compreso il **Documento di ePolicy**;
- di essere al corrente che la Scuola mette in atto tutte le precauzioni necessarie per garantire al massimoche le/gli alunne/i usino correttamente la rete e non accedano a materiale inadeguato;
- di essere consapevoli che, in considerazione delle precauzioni prese per ridurre al massimo i rischi della navigazione sul WEB, la Scuola non è responsabile di eventuali usi impropri della rete e delle Tecnologie dell'Informazione e della Comunicazione (TIC) né della natura e dei contenuti del materiale che il/la proprio/a figlio/a, aggirando per volontà propria le barriere predisposte dalla scuola, potrebbero reperire in Internet;
- di essere consapevoli della responsabilità individuale del/la proprio/a figlio/a per le eventuali violazioni delle norme e/o per gli eventuali danni provocati da un uso improprio degli strumenti informatici;
- di essere consapevoli che, qualora non venissero rispettate le regole, la scuola adotterà sanzioni disciplinari rapportate alla gravità degli episodi e saranno altresì possibili azioni civili per eventuali danni,nonché l'eventuale denuncia all'autorità giudiziaria qualora la violazione si configuri come reato.

Pertanto, i sottoscritti

- **acconsentono/non acconsentono** (*barrare la voce che non interessa*) che il/la proprio/a figlio/a utilizzi a scuola l'accesso Internet;
- **autorizzano/non autorizzano** *(barrare la voce che non interessa)* l'I.C Grosseto 2 a realizzare e a utilizzare, a scopo didattico e/o di documentazione e/o di informazione e senza finidi lucro, fotografie, video o altri materiali audiovisivi contenenti l'immagine, il nome, la voce, gli elaborati (scritti, disegni,...) del/la proprio/a figlio/a anche, se del caso, mediante riduzioni e/o adattamenti;
- **dichiarano** di essere informati che detto materiale potrà essere utilizzato per documentare e divulgare le attività della scuola tramite il sito Internet di Istituto, pubblicazioni, cd-rom, mostre, seminari, convegni e altre iniziative promosse dalla scuola anche in collaborazione con altri soggetti;
- **dichiarano** di non aver nulla a pretendere in ragione di quanto sopra indicato e di rinunciare irrevocabilmente ad ogni diritto, azione o pretesa derivante da quanto sopra autorizzato.

Allegato:
Fotocopie dei documenti di identità

Firma ..... Firma .....

Grosseto, ...

Allegato 2 Documento di ePolicy

ASSUNZIONE DI RESPONSABILITÀ DA PARTE DI DOCENTI E ALTRO PERSONALE DELLA SCUOLA

Alla Dirigente dell'Istituto Comprensivo Grosseto 2

Il/La sottoscritto/a....., dipendente dell'Istituto Comprensivo Grosseto 2, in qualità di .....

Dichiara:

- di aver letto e compreso il **Documento di ePolicy**;
- di essere consapevole delle responsabilità connesse all'uso delle Tecnologie o dell'Informazione e dellaComunicazione (TIC) nella scuola.

Pertanto, il/la sottoscritto/a

si impegna a:

- tenere riservate le credenziali di accesso al sistema;
- modificare la password periodicamente;
- segnalare tempestivamente eventuali perdite di riservatezza;
- utilizzare i computer e gli accessi esclusivamente per attività inerenti il proprio servizio e o l'aggiornamento professionale;
- segnalare eventuali anomalie;
- vigilare sul corretto utilizzo degli strumenti informatici e della navigazione in rete da parte delle alunne e degli alunni.

Firma

.....

Grosseto, ...