Documento di ePolicy

Argomenti del Documento

1. **Presentazione dell'ePolicy**
   1.1 Scopo dell'ePolicy
   1.2 Ruoli e responsabilità
   1.3 Informativa per i soggetti esterni che erogano attività educative nell'Istituto
   1.4 Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
   1.5 Gestione delle infrazioni alla ePolicy
   1.6 Integrazione dell'ePolicy con regolamenti esistenti
   1.7 Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

2. Formazione e curricolo

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

3. Gestione dell'infrastruttura e della strumentazione TIC (Tecnologie dell'Informazione e della Comunicazione) della e nella scuola

- Protezione dei dati personali
- Accesso ad Internet
- Strumenti di comunicazione online
- Strumentazione personale

4. Rischi on line: conoscere, prevenire e rilevare

- Sensibilizzazione e prevenzione
- Cyberbullismo: che cos'è e come prevenirlo
- Hate speech: che cos'è e come prevenirlo
- Dipendenza da Internet e gioco online
- Sexting
- Adescamento online
- Pedopornografia

5. Segnalazione e gestione dei casi

- Cosa segnalare
- Come segnalare: quali strumenti e a chi
- Gli attori sul territorio per intervenire
- Allegati con le procedure

1. Presentazione dell'ePolicy

1. Introduzione al documento di ePolicy

1.1 Scopo dell'ePolicy

Le TIC (Tecnologie dell'Informazione e della Comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.
Le "competenze digitali" sono fra le abilità chiave all'interno del *Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente* e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).
In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una 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 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 (TIC) 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.

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, critico ed 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 ed educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

1.2 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 Dirigente Scolastico
Garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica. Promuove la cultura della sicurezza online, e contribuisce, ove possibile, insieme al Referente per il bullismo e cyberbullismo, corsi di formazione per tutta la comunità scolastica sull'utilizzo positivo e responsabile delle TIC.

Interviene in casi di gravi episodi di bullismo e cyberbullismo e sull'uso improprio delle tecnologie digitali.

L'animatore Digitale
Coordina, promuove e diffonde nella scuola l'attuazione dei progetti e delle indicazioni contenute nel Piano Nazionale Scuola Digitale.

Supporta il personale scolastico in riferimento ai rischi online, alla protezione e gestione dei dati personali.

Monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola. Controlla che gli utenti autorizzati accedano alla rete della scuola con apposita password per scopi istituzionali e consentiti.

Il referente Bullismo e Cyberbullismo
Coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo.

Può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio.

I docenti
Diffondono la cultura dell'uso responsabile delle TIC e della Rete, integrandole nelle parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, l'uso delle tecnologie digitali nella didattica.

Accompagnano e supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete.

Hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

Il personale amministrativo, tecnico e ausiliario (ATA)
<u>Il Direttore dei Servizi Generali</u>
Assicura, nei limiti delle risorse finanziarie, la manutenzione delle strutture informatiche ai fini del suo funzionamento, della sua sicurezza e tutela da un uso improprio, e da attacchi esterni.

Prevede interventi di personale tecnico di assistenza per la soluzione di problematiche relative alla rete e all'uso del digitale segnalate dai docenti.

<u>Il personale amministrativo</u>

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

Il personale Tecnico e Ausiliario (ATA)
Promuove la politica di e-safety della scuola.

Segnala eventuali abusi nell'uso delle tecnologie digitali e di accesso a internet e di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

Gli studenti e le studentesse
Utilizzare responsabilmente le tecnologie digitali in coerenza con quanto richiesto dai docenti, nonché rispettando le norme codificate nei regolamenti di istituto.

Tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le, rispettando le buone pratiche di sicurezza in rete, con il supporto della scuola.

Saper distinguere, con l'aiuto dei docenti, le fonti di informazione attendibili in rete per utilizzarle in modo appropriato senza violazione dei diritti d'autore altrui.

Partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

Segnalare ai genitori e/o ai docenti situazioni di difficoltà o di bisogno di aiuto.

I genitori
Accettare e condividere quanto scritto nell'ePolicy dell'Istituto.

Partecipare attivamente nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali.

Relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet.

Gli Enti Educativi esterni e le Associazioni
Accettare e condividere quanto scritto nell'ePolicy dell'Istituto.

Conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC. Promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

1.3 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).

Premessa e obiettivi dell'informativa

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 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.

Destinatari

I destinatari di questo documento sono tutte le organizzazioni e i soggetti esterni che collaborano con l'Istituto.

Ambiti di applicazione e Ruoli

L'applicazione del presente documento si riferisce a tutti i progetti esterni messi in atto nell'Istituto. I docenti referenti del progetto sono le persone che si occupano di presentare il documento di ePolicy alle organizzazioni e ai soggetti esterni che collaborano con l'Istituto.

Eventuali infrazioni delle norme presenti nel documento di ePolicy dovranno essere comunicate ad almeno una delle seguenti figure: docente referente del progetto, referenti del plesso, Funzione strumentale, referente del bullismo e cyberbullismo, Animatore digitale, Dirigente Scolastico.

Regolamento/Codice di comportamento

L'accesso a internet è possibile e consentito esclusivamente per la didattica e per la comunicazione scolastica. Sarà schermato da filtri (firewall) che impediscono il collegamento a siti appartenenti a black list consentendo il collegamento solo a siti idonei alla didattica.

L’utilizzo delle attrezzature informatiche è consentito esclusivamente per scopi inerenti la didattica e la formazione. L'utilizzo da parte degli alunni deve avvenire sempre in presenza di un insegnante, il quale deve vigilare sulla correttezza delle operazioni svolte dei ragazzi.

Gli utenti si impegnano a non diffondere informazioni che appartengono a terzi senza l’autorizzazione degli stessi e nei singoli casi si impegnano a menzionare le fonti quando si servono di informazioni di terze persone. Sono proibite la duplicazione e la diffusione di programmi e documenti coperti dal diritto d'autore.

Gli utenti si impegnano a non consultare deliberatamente, conservare o diffondere documenti che possono ledere la dignità della persona, che hanno carattere pornografico, che incitano all'odio razziale o che costituiscono un'apologia del crimine o della violenza.

È vietato:

- l’uso di Internet per motivi personali;
- partecipare a forum o chat line se non per motivi attinenti alla propria attività istituzionale;
- navigare su siti internet potenzialmente pericolosi e/o illegali. (es: siti pornografici, di intrattenimento, ecc.);
- ascoltare la radio o guardare video o filmati utilizzando le risorse Internet per fini non didattici;
- inoltrare “catene” di posta elettronica (catene di S. Antonio e simili) anche se afferenti a presunti problemi di sicurezza;
- fornire password di accesso alla rete WI-FI dell’istituto agli alunni;
- aprire file con allegati in lingue straniere o provenienti da mittenti sconosciuti (potrebbero contenere virus o materiali non idonei).

Il divieto di utilizzare i telefoni cellulari, come per gli studenti, opera anche nei confronti del personale (docente e non docente). Questo può far uso di dispositivi mobili solo per fini connessi al proprio servizio o per fini personali in casi eccezionali opportunatamente giustificati.

Procedure di segnalazione
Le procedure di segnalazione per le situazioni di rischio sono riportate nel documento di ePolicy e allegate al presente documento.

Provvedimenti
Personale e studenti/studentesse saranno informati su infrazioni e eventuali sanzioni. A seconda dell'infrazione commessa in relazione all'ePolicy, i comportamenti da adottare saranno:

- richiamo verbale;
- informare i docenti coordinatori della classe, il referenti del plesso, la Funzione strumentale, il referente del bullismo e cyberbullismo, l’Animatore digitale e il DS;
- informare i genitori o i tutori;
- comminare sanzioni disciplinari, da valutare a seconda dei casi;
- procedere a comunicare l’accaduto, ove necessario, alle autorità competenti.

1.4 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 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'inizio dell'anno scolastico.

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di 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.

In particolare la condivisione di questo documento avverrà secondo le seguenti modalità.

Condivisione con gli alunni
Durante la prima settimana di scuola, verrà presentata la ePolicy agli alunni da parte dei docenti, insieme ai regolamenti correlati.

Durante il corso dell'anno i docenti svolgeranno alcune lezioni sulle buone pratiche per l' utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al cyberbullismo.

Condivisione con il personale
Le norme adottate dalla scuola in materia di sicurezza nell'utilizzo del digitale saranno discusse negli organi collegiali (collegio docenti, riunioni di dipartimento, consigli di classe) e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito web della scuola.

Il personale della scuola riceverà un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso materiali resi disponibili anche sul sito web della scuola.

Condivisione con i genitori
Le famiglie saranno informate attraverso la condivisione della ePolicy e di materiali informativi specifici sul sito web della scuola.

Nelle riunioni preliminari verrà presentata la ePolicy alle famiglie, insieme ai regolamenti correlati.

Saranno organizzate dalla scuola incontri informativi in collaborazione con gli enti del territorio, durante i quali si farà riferimento alla presente ePolicy, per sensibilizzare le famiglie sull'uso delle TIC.

1.5 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.

Personale e studenti/studentesse saranno informati su infrazioni e eventuali sanzioni. A seconda dell'infrazione commessa in relazione all'ePolicy, i comportamenti da adottare saranno:

- richiamo verbale;
- informare i docenti coordinatori della classe, il referenti del plesso, la Funzione strumentale, l'Animatore digitale e il Dirigente Scolastico;
- informare i genitori o i tutori;
- comminare sanzioni disciplinari, da valutare a seconda dei casi (ad esempio, segnazione di attività aggiuntivi da svolgere a casa su temi di Cittadinanza e Costituzione; divieto temporaneo di prendere parte alla ricreazione e simili);
- procedere a comunicare l'accaduto, ove necessario, alle autorità competenti.

1.6 Integrazione dell'ePolicy con Regolamenti esistenti

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

Il presente documento di ePolicy viene integrato nel PTOF, nel regolamento di Istituto e nel patto di Corresponsabilità.

1.7 Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'ePolicy 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 referente del bullismo e cyberbullismo e l'animatore digitale coordinano sotto la guida del DS l'aggiornamento del documento di ePolicy. Il documento sarà riesaminato annualmente, e se necessario verranno apportate modifiche.

Il nostro piano d'azioni

Azione 1 - Creazione del gruppo di lavoro ePolicy *(Azione sviluppabile nel breve periodo)*

Azione 2 - Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

Azione 3 - 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

Azione 4 - Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale

Azione 5 - Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse

Azione 6 - 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

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.

Fine scuola dell'Infanzia

Competenze specifiche
Utilizzare le nuove tecnologie per giocare, svolgere compiti, acquisire informazioni, con la supervisione dell'insegnante

Abilità
Cogliere le trasformazioni naturali

Scoprire le potenzialità espressive offerte dal computer

Osservare e descrivere le principali trasformazioni dell'ambiente naturale

Sperimentare alcune potenzialità espressive ed interattive offerte dal computer

Osservare, descrivere e rappresentare le trasformazioni dei fenomeni naturali e degli esseri viventi

Utilizzare le potenzialità offerte dal computer per esprimere la propria creatività

Conoscenze
Il computer e i suoi usi

Altri strumenti di comunicazione e i suoi usi (audiovisivi, telefoni fissi e mobili.)

Mouse

Tastiera

Icone principali di Windows, di Word, di Google Work-Space

Fine Scuola Primaria

Competenze specifiche
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

Abilità
Utilizzare semplici materiali digitali per l'apprendimento.

Utilizzare il PC, alcune periferiche e programmi applicativi.

Avviare alla conoscenza della Rete per scopi di informazione, comunicazione, ricerca e svago.

Individuare rischi fisici nell'utilizzo delle apparecchiature elettriche ed elettroniche e i possibili comportamenti preventivi

Individuare i rischi nell'utilizzo della rete Internet e individuare alcuni comportamenti preventivi e correttivi

Conoscenze
I principali dispositivi informatici di input e output

I principali software applicativi utili per lo studio, con particolare riferimento alla videoscrittura, alle presentazioni e ai giochi didattici.

Semplici procedure di utilizzo di Internet per ottenere dati, fare ricerche, comunicare
Rischi fisici nell'utilizzo di apparecchi elettrici ed elettronici

Rischi nell'utilizzo della rete con PC e telefonini

Fine Scuola Secondaria di I grado

Competenze specifiche
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

Abilità
Utilizzare la rete per scopi di informazione, comunicazione, ricerca e svago.

Riconoscere potenzialità e rischi connessi all'uso delle tecnologie più comuni, anche informatiche

Conoscenze

Procedure di utilizzo sicuro e legale di reti informatiche per ottenere dati e comunicare (motori di ricerca, sistemi di comunicazione mobile, email, chat, social network, protezione degli account, download, diritto d'autore, ecc.)

Fonti di pericolo e procedure di sicurezza

2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC 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.

I docenti potranno formarsi attraverso percorsi in itinere che prevedono:

- momenti di autoaggiornamento;
- momenti di formazione personale e/o collettiva organizzate dall'Animatore digitale, dal Team dell'innovazione digitale e dal Referente bullismo cyberbullismo;
- formazione dei docenti all'utilizzo del registro elettronico e dello scrutinio elettronico e dell'utilizzo di G-Suite;
- somministrazione di un questionario rivolto ai docenti per la rilevazione dei "bisogni formativi" e per la "rilevazione delle competenze";
- partecipazione alle iniziative promosse dall'Amministrazione centrale, dalle scuole in rete di distretto e di ambito, e da organizzazioni presenti sul territorio;
- corsi on-line promossi dal MIUR.

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.

Sarà predisposta una sezione online, sul sito d'Istituto: www.icceretolo.edu.it, per la messa a disposizione e la condivisione di materiali finalizzati all'aggiornamento sull'utilizzo consapevole e sicuro di internet. Qui sarà possibile trovare materiali informativi sulla sicurezza in internet per l'approfondimento personale, per le attività con gli studenti e gli incontri con i genitori, costituiti da guide in pdf, video, manuali a fumetti, e link messi a disposizione dal sito "Generazioni connesse" con il contributo della Polizia di Stato, dei Carabinieri, del Telefono Azzurro e di altri enti o associazioni competenti in materia.

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.

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. Nella sezione online sul sito d'Istituto www.icceretolo.edu.it, e sulla relativa sezione saranno messi in condivisione materiali dedicati ad alunni e alle famiglie come guide in formato .pdf e video che possono fornire spunti di approfondimento e confronto.

Il nostro Piano di Azioni

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.

- Effettuare un’analisi del fabbisogno formativo del corpo docente sull’utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

3. Gestione dell'infrastruttura e della strumentazione TIC 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 Dirigente e il personale scolastico da questi delegato sono responsabili del trattamento dei dati personali (degli alunni, dei genitori, ecc.) nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento delle proprie funzioni. Il personale incaricato deve applicare la procedura sul trattamento dei dati personali su supporto cartaceo e su supporto informatico per la protezione e la sicurezza degli stessi.

All'inizio dell'anno viene, inoltre, fornita ai genitori:

- informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori;
- richiesta di liberatoria per l'utilizzo delle immagini.

3.2 Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*

2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*

3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*

4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*

5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

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

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

Indicazioni generali

L'accesso a internet è possibile e consentito esclusivamente per la didattica, per l'utilizzo del Registro Elettronico e per la comunicazione scolastica. Sarà schermato da filtri (firewall) che impediscono il collegamento a siti appartenenti a black list consentendo il collegamento solo a siti idonei alla didattica.

L'utilizzo delle attrezzature informatiche è consentito esclusivamente per scopi inerenti la didattica e la formazione. L'utilizzo da parte degli alunni deve avvenire sempre in presenza di un insegnante, il quale deve vigilare sulla correttezza delle operazioni svolte dei ragazzi.

Norme di utilizzo della connessione internet di istituto
Gli utenti si impegnano a non diffondere informazioni che appartengono a terzi senza l'autorizzazione degli stessi e nei singoli casi si impegnano a menzionare le fonti quando si servono di informazioni di terze persone. Sono proibite la duplicazione e la diffusione di programmi e documenti coperti dal diritto d'autore.

Gli utenti si impegnano a non consultare deliberatamente, conservare o diffondere documenti che possono ledere la dignità della persona, che hanno carattere pornografico, che incitano all'odio razziale o che costituiscono un'apologia del crimine o della violenza. È vietato:

- l'uso di Internet per motivi personali;
- partecipare a forum o chat line se non per motivi attinenti alla propria attività istituzionale;
- navigare su siti internet potenzialmente pericolosi e/o illegali. (es: siti pornografici, di intrattenimento, ecc.);
- ascoltare la radio o guardare video o filmati utilizzando le risorse Internet per fini non didattici;
- inoltrare "catene" di posta elettronica (catene di S. Antonio e simili) anche se afferenti a presunti problemi di sicurezza;
- fornire password di accesso alla rete WI-FI dell'istituto agli alunni;
- aprire file con allegati in lingue straniere o provenienti da mittenti sconosciuti (potrebbero contenere virus o materiali non idonei).

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.

Google Workspace
A partire dall'anno scolastico 2019/20 l'Istituto Comprensivo Ceretolo di Casalecchio di Reno ha adottato la piattaforma G-Suite ora Google workspace, un insieme di applicativi messi a disposizione da Google per le scuole, al fine di facilitare, sostenere e motivare l'apprendimento attraverso le nuove tecnologie. L'account Google for Edu è attivo per tutti i docenti e tutti gli studenti della scuola primaria e secondaria di primo grado dell'Istituto. Gli studenti della nostra scuola riceveranno un account personale gratuito con nome utente e password per l'accesso alle applicazioni Google di cui potranno usufruire fino al termine del loro percorso scolastico nel nostro Istituto. Il nome utente sarà così formato: nome.cognome@icceretolo.istruzioneer.it.

E-Mail

L’account di posta elettronica che sarà utilizzato per comunicazioni sarà solo quello istituzionale, utilizzato ordinariamente dagli uffici amministrativi sia in entrata che in uscita. Inoltre, tutti i docenti e gli studenti avranno un indirizzo mail istituzionale compreso nel servizio Google WorkSpace. Esso sarà utilizzato unicamente per comunicazioni in entrata e in uscita, di carattere lavorativo e didattico. Gli utenti si impegnano a non diffondere informazioni che possono nuocere alla reputazione della scuola o essere contrarie alla morale o alle leggi in vigore. Prima di aprire una mail è necessario pensare a:

- Spam: email, messaggi istantanei e altre comunicazioni indesiderate;
- Pishing: frode online per sottrarre con l’inganno numeri di carte di credito, password, informazioni su account personale;
- Truffe: email spedite da criminali che tentano di rubare denaro.

Sito Web della scuola
Tutti i contenuti del sito dell’Istituto sono pubblicati dalla funzione strumentale Web, insieme al Dirigente scolastico, ne valuta la sicurezza e l’adeguatezza sotto i diversi profili dell’accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc. Il Dirigente scolastico, inoltre, si assume la responsabilità che il sito web dell’Istituto sia conforme alle linee guida di legge, in particolar modo si assicura che il lavoro pubblicato sia frutto delle attività svolte dalla scuola e qualora fossero pubblicati lavori di altri renderà note le fonti utilizzate impegnandosi a richiedere l’autorizzazione degli stessi e a proibire la diffusione e/o la duplicazione di programmi e documenti coperti dal diritto d’autore. La scuola offre all’interno del proprio sito una serie di servizi alle famiglie e agli utenti esterni: i docenti che desiderano pubblicare attività didattiche dovranno chiedere l’autorizzazione al Dirigente e/o alla funzione strumentale web.

Registro Elettronico
Questo strumento sarà utilizzato per la prenotazione di aule e laboratori.

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.

Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc.

Ai sensi del regolamento di istituto e in linea con i doveri sanciti dallo Statuto delle studentesse e degli studenti (D.P.R. n. 249/1998), è severamente proibito l'uso del telefono cellulare in orario scolastico, compresi gli intervalli ricreativi. La violazione di tale divieto configura un'infrazione disciplinare rispetto alla quale la scuola è tenuta ad applicare apposite sanzioni. L'uso del cellulare è consentito solo in caso di esplicita autorizzazione da parte dei docenti.

Il telefono cellulare deve essere tenuto spento. Eventuali esigenze di comunicazione tra gli alunni e le famiglie, in caso di urgenza, possono essere soddisfatte mediante gli apparecchi telefonici presenti a scuola

E' proibita, sia in orario scolastico che extrascolastico, la diffusione di immagini, video, comunicazioni via web, social network e/o chat lesivi della privacy e/o della dignità propria ed altrui. Le azioni che risultino improprie e/o dannose per l'immagine e il prestigio dell'Istituto, del personale scolastico e degli alunni, oltre che essere oggetto di provvedimenti disciplinari per violazione del Regolamento interno, possono costituire reato ed essere perseguibili per Legge.

Le responsabilità che dovessero derivare dal verificarsi di eventi riconducibili all'uso non corretto del telefono cellulare sono ascrivibili alle famiglie degli alunni eventualmente coinvolti. L'istituzione scolastica non si assume alcuna responsabilità né relativamente all'uso improprio che gli studenti dovessero fare del cellulare né relativamente a smarrimenti dei dispositivi personali degli alunni.

Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc.
Il divieto di utilizzare i telefoni cellulari opera anche nei confronti del personale (docente e non docente). Questo può far uso dispositivi mobili solo per fini connessi al proprio servizio o per fini personali in casi eccezionali opportunatamente giustificati.

Norme di utilizzo delle postazioni multimediali presenti nelle aule
Ogni docente è responsabile del PC di classe che avrà cura di:

- scaricare gli aggiornamenti di Windows e l'Antivirus;
- cancellare periodicamente tutti i documenti presenti sul desktop.

Ogni insegnante è tenuto a:

- accendere e spegnere la LIM sempre con il telecomando;
- spegnere l'hotspot sul PC, se attivato all'inizio della lezione;
- non collegare altri dispositivi elettronici alla multipresa;
- spegnere LIM e PC al termine delle lezioni;
- riporre il PC nel luogo indicato dai referenti; non spegnere mai il PC se sta eseguendo l'aggiornamento;
- controllare che durante la ricreazione LIM e PC di classe non vengano utilizzati dagli alunni;
- contattare il referente informatico di Plesso prima di installare nuovi Software;
- comunicare al referente informatico di Plesso eventuali problemi riscontrati su Hardware e Software;
- non spostare, copiare o cancellare file appartenenti al sistema operativo o ai programmi installati;
- non modificare la configurazione di sistema e in generale porre in essere ogni comportamento che possa danneggiare l'Hardware o il Software installato.

Norme di utilizzo delle postazioni multimediali presenti nei laboratori
Il personale docente deve:

- accedere con le classi al laboratorio secondo le modalità indicate dal responsabile di laboratorio (registro prenotazioni e registro presenze);
- installare Software solo dopo averlo comunicato al responsabile di laboratorio; comunicare al responsabile di laboratorio eventuali problemi di Hardware e Software; controllare che tutti i PC e le stampanti siano spenti al termine dell'attività didattica

Il nostro piano d'azioni

1. Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
2. Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
3. Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

4 Rischi on line: conoscere, prevenire e rilevare

4.1 Sensibilizzazione e Prevenzione

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

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

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

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

Nel caso della **sensibilizzazione** *si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.*

Nel caso della **prevenzione** *si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.*

Sensibilizzazione
La sensibilizzazione avverrà attraverso gli interventi dei docenti formati e di figure esterne, con le quali saranno attuate campagne di sensibilizzazione all'uso corretto della rete. Nella sezione sul sito di istituto saranno condivisi documenti utili e informativi relativi all'uso corretto della rete, tra i quali anche quelli messi a disposizione da "Generazioni Connesse" per alunni, docenti e genitori. Inoltre, il nostro istituto porta avanti ogni anno un concorso scolastico dal nome Digito Ergo Sum, con la finalità di promuovere un uso più sicuro e responsabile del web, delle nuove tecnologie e di contrastare comportamenti e fenomeni devianti legati all'utilizzo inconsapevole della rete.

Prevenzione
La prevenzione sarà attuata su tre livelli:

1. la prevenzione universale: parte dal presupposto che tutti gli studenti sono potenzialmente a rischio. Saranno interventi basati principalmente sulla sensibilizzazione.

2. La prevenzione selettiva: sarà dedicata a un gruppo di studenti in cui il rischio online è presente, individuato attraverso indagini specifiche, la conoscenza di presenza di fattori di rischio o da segnalazioni fatte dalla scuola.
3. La prevenzione indicata: sarà dedicata a casi specifici, con l'obiettivo di ridurre comportamenti problematici o dare supporto alle vittime.

4.2 Cyberbullismo: che cos'è e come prevenirlo

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

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

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

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015); promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education; previsione di misure di sostegno e rieducazione dei minori coinvolti;
- integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti.

Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.

Nomina del Referente per le iniziative di prevenzione e contrasto

Il Referente per le iniziative di prevenzione e contrasto ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.

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

Azioni
Saranno attuate campagne di sensibilizzazione e informazione, anche con l'ausilio di progetti e realtà esterne.

Verso gli studenti: si attiveranno progetti di sensibilizzazione, creando consapevolezza sulle varie problematiche, capire le sofferenze delle vittime, le responsabilità degli spettatori, e a chi chiedere aiuto e come reagire.

Verso i docenti: si potenzieranno le capacità di promuovere un clima positivo in classe, partecipando a corsi di formazione che abilitino gli insegnanti a prevenire o intervenire in situazioni problematiche.

Verso i genitori: si promuoveranno corsi di formazione volti a promuovere l'amicizia, l'empatia e la prosocialità, e a modificare le credenze che vedono normale accettazione dei comportamenti aggressivi nei figli.

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.

Azioni
Verso gli studenti: inserimento nel curriculo di temi legati all'interculturalità e al rispetto della diversità. Saranno favoriti lavori a partire dalla mini serie dei "Super-Errori" realizzata da Generazioni Connesse

Verso i genitori: informazione circa le possibilità di attivare forma di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli.

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.

Azioni
Verso gli studenti: informazioni sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali, e in alcuni casi rappresenta un vero e proprio illecito. Inserimento nel curriculo di temi legati alla salute, e saranno utilizzati questionari per riflettere su come ogni studente passa il tempo online.

Verso i genitori: informazione circa le possibilità di attivare forma di controllo parentale del tempo passato online, sui giochi e console e sensibilizzazione sulla necessità di monitorare l'esperienza di gioco dei propri figli.

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.

Azioni
Verso gli studenti: inserimento nel curriculo di temi legati all'affettività, alla sessualità e alle differenze di genere.

Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale nella navigazione.

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.

Azioni
Verso gli studenti: Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni virtuali, o reali, con minorenni per indurli alla prostituzione. Inserimento nel curriculo di temi legati all'affettività, alla sessualità e alle differenze di genere.

Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale nella navigazione, e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli.

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 Telefono Azzurro e "STOP-IT" di Save the Children.

Azioni
Verso gli studenti: inserimento nel curriculo di temi legati all'affidabilità delle fonti online, all'affettività, alla sessualità e alle differenze di genere.
Verso i genitori: informazione circa le possibilità di attivare forma di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli.

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

Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.

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.

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.

La scheda di segnalazione potrà essere compilata da qualsiasi persona che è venuta a conoscenza di un probabile caso violazione del documento di ePolicy.

La scheda di segnalazione sarà disponibile in formato cartaceo presso la portineria, e in formato digitale nella sezione dedicata sul sito di istituto.

Le schede di segnalazione cartacee una volta compilate potranno essere consegnate in portineria. Il collaboratore scolastico provvederà a inserire la segnalazione cartacea all'interno di un fasciolo. Le schede di dichiarazione compilate in formato digitale potranno essere spedite all'indirizzo mail del referente del bullismo e cyberbullismo.

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.

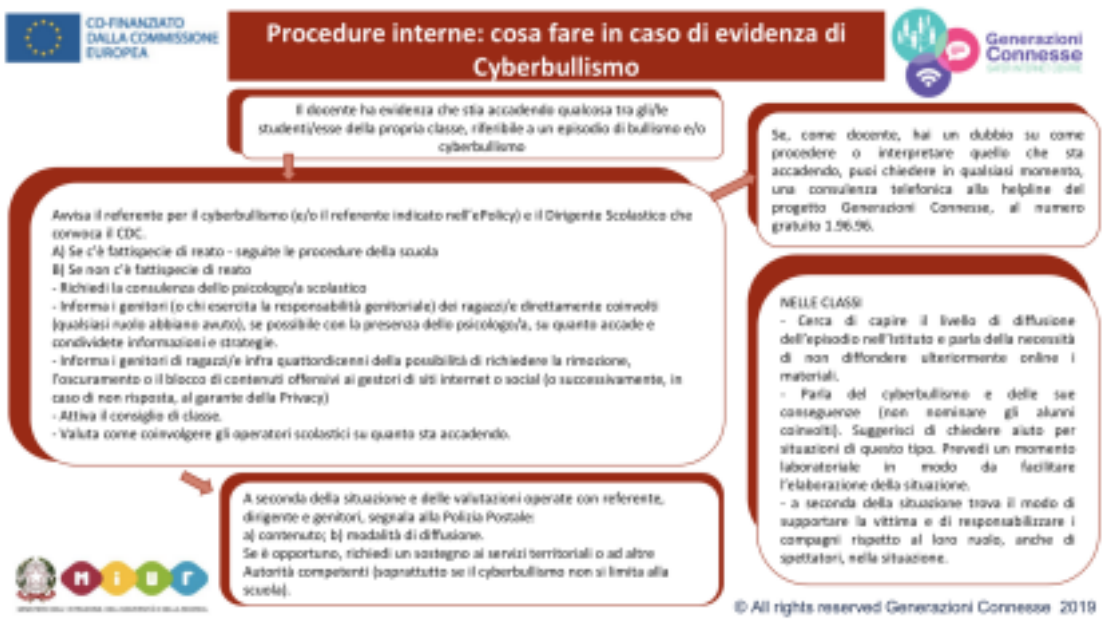
Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni 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.

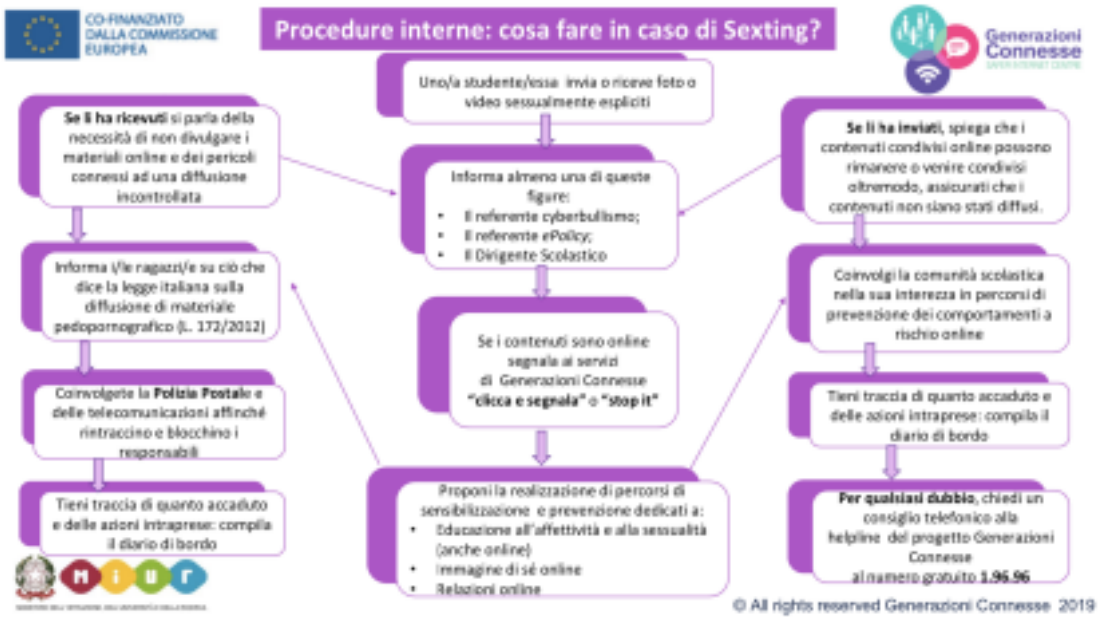
Inoltre, il nostro istituto si avvale della collaborazione di associazioni esterne e di educatori digitali.

5.4. Allegati con le procedure

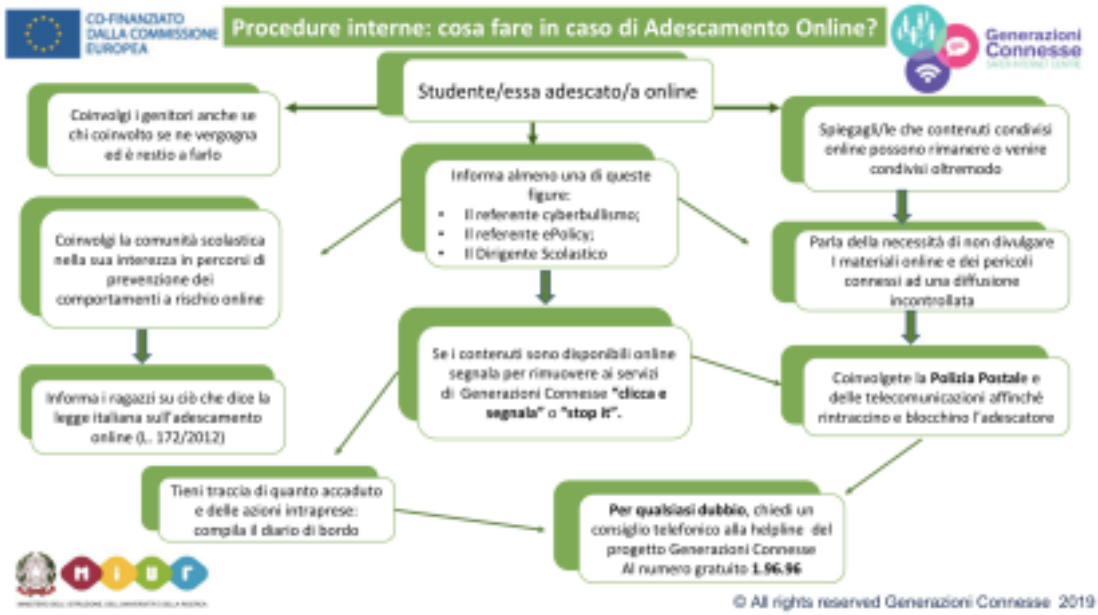
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



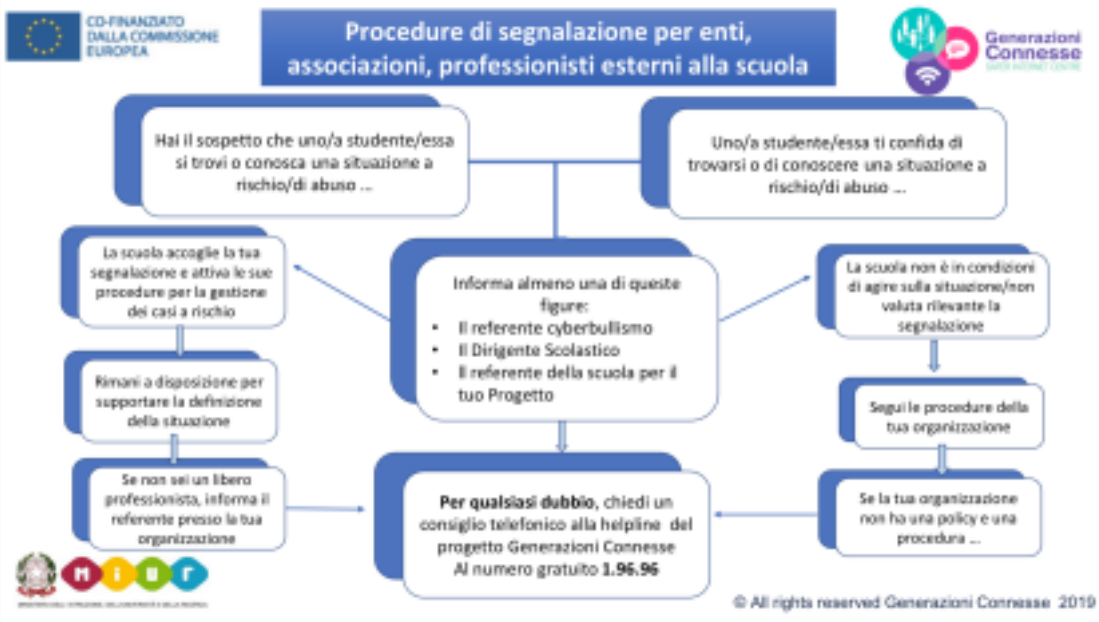
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

Scheda di segnalazione

Diario di bordo

iGloss@ 1.0 l'ABC dei comportamenti devianti online

Elenco reati procedibili d'ufficio

Il nostro piano d'azioni: azioni da sviluppare nell'arco dei tre anni scolastici successivi:

- creare una scheda di valutazione approfondita;

- creare un protocollo specifico di intervento di rete con il territorio;
- creare una scheda di monitoraggio;
- creare un team di gestione delle emergenze.