



Documento di ePolicy

POIS00200L

A. GRAMSCI - J. M. KEYNES

VIA DI REGGIANA 106 - 59100 - PRATO - PRATO (PO)

Stefano Pollini

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

1. **Presentazione dell'ePolicy**

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

2. **Formazione e curriculum**

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

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

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

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

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

5. **Segnalazione e gestione dei casi**

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

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

La nostra Scuola ha incrementato l'uso delle tecnologie informatiche nella didattica e nell'organizzazione generale della scuola, le TIC sono utilizzate sia come strumento per svolgere esperienze formative, sia per condurre in modo più efficiente le funzioni amministrative.

Abbiamo considerato che gli studenti sono indubbiamente la generazione più immersa nelle tecnologie digitali e che non possono essere lasciati soli nella gestione dei profondi cambiamenti offerti dalle TIC.

Dunque, la policy di e-safety nasce dalla rilevazione di questo bisogno ed è volto a definire:

- norme comportamentali e procedure per l'utilizzo delle tecnologie nell'ambito dell'Istituto;
- misure per la prevenzione e per la rilevazione e la gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

1.2 - Ruoli e responsabilità

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

Il Dirigente Scolastico

il Dirigente Scolastico garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica. E' formato sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIUR. Promuove la cultura della sicurezza online e, ove possibile, dà il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, con corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC. Il Dirigente Scolastico ha la responsabilità di gestire ed intervenire nei

casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

L'animatore Digitale

L'Animatore digitale supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica).

Referente informatico della Rete

Monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e ha il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

Referente Bullismo e Cyberbullismo

"Ogni Istituto scolastico, nell'ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo" (Art. 4 Legge n.71/2017, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo" (permalink - file 1 LEGGE 71_2017 in allegato). Tale figura ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può **avvalersi della collaborazione delle Forze di polizia**, delle associazioni e dei centri di aggregazione giovanile del territorio. Fondamentale, dunque, il suo ruolo non solo in ambito scolastico ma anche in quello extrascolastico, in quanto (ove possibile) potrebbe coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

I Docenti

i Docenti hanno un ruolo centrale nel **diffondere la cultura dell'uso responsabile delle TIC e della Rete**. Integrano le parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica. I docenti dovrebbero accompagnare e supportare 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

Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il dirigente scolastico e con il personale docente tutto.

Le studentesse e gli studenti

gli Studenti e le Studentesse devono, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola **imparano a tutelarsi online**, tutelare i/le propri/e compagni/e e rispettarli/le; partecipano 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.

I Genitori

I Genitori, in continuità con l'Istituto scolastico, si rendono partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali; si relazionano 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. **È estremamente importante che accettino e condividano quanto scritto nell'ePolicy dell'Istituto.**

1.3 - Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

Le organizzazioni, le associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve o/e lungo periodo, dovranno prendere atto di quanto stilato nell'e-policy dell'Istituto e/o eventualmente sottoscrivere un'informativa sintetica del documento in questione, presente nel contratto.

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

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

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

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

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

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

Il presente documento di e-Policy viene condiviso con tutta la comunità educante, al fine di promuovere competenze digitali diffuse e, nel contempo, ciascun attore scolastico, diventi a suo volta promotore del documento stesso. A tal fine si prevede:

1. Condivisione e comunicazione della Policy agli alunni:

- all'inizio dell'anno scolastico, i docenti, in occasione dell'illustrazione del regolamento d'istituto alle studentesse e agli studenti, presenteranno il documento di e-policy della scuola;
- nel corso dell'anno ciascun docente darà spazio alla diffusione delle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e al contrasto ai fenomeni di bullismo e di cyberbullismo.

2. Condivisione e comunicazione della Policy al personale:

- Le norme adottate dalla scuola in materia di sicurezza nell'utilizzo del digitale saranno discusse negli organi collegiali (collegio docenti, riunioni di dipartimento) 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.

3. Condivisione e comunicazione della Policy ai genitori:

- le famiglie saranno informate in merito alla linea di condotta adottata dalla scuola per un uso sicuro e responsabile delle tecnologie digitali e di internet attraverso la condivisione del presente documento e di materiali informativi specifici sul sito web della scuola;
- al fine di sensibilizzare le famiglie sui temi dell'uso delle TIC saranno organizzati dalla scuola incontri informativi, durante i quali si farà riferimento alla presente policy.

1.5 - Gestione delle infrazioni alla

ePolicy

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

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

1. Infrazioni degli alunni.

È bene che i docenti introducano attività laboratoriali volti a sviluppare negli studenti e nelle studentesse una sempre maggiore consapevolezza dei rischi legati a un uso imprudente e improprio delle TIC e della Rete e che forniscano loro, ogni qualvolta avvenga un'infrazione alle regole stabilite, gli strumenti per affrontare le conseguenze dei loro errori.

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

- a. colloquio con lo/a studente/essa coinvolto/a;
- b. eventuale confronto con i genitori;
- c. ripristino delle regole di convivenza all'interno della classe;
- d. interventi di educazione tra pari (peer education);
- e. incontri con esperti esterni e con il CIC della scuola;
- f. provvedimenti disciplinari educativi (eventuale sospensione con obbligo di frequenza presso strutture convenzionate dove svolgere mansioni di pubblica utilità sociale);
- g. eventuale segnalazione alle autorità (polizia postale, Garante per la protezione dei dati personali, Garante dell'Infanzia e dell'Adolescenza, servizi minorili dell'amministrazione della Giustizia, richiesta di ammonimento da parte del Questore).

2. Infrazioni del personale scolastico

Le infrazioni alla e-policy da parte del personale scolastico possono riferirsi sia alla mancata osservanza delle regole indicate nella Policy, sia alla mancata sorveglianza e pronto intervento nel caso di infrazione da parte degli alunni.

3. Infrazioni dei genitori

Compito dei genitori è supportare gli insegnanti e il personale scolastico nel riconoscimento e nella costruzione di azioni di contrasto efficaci ai principali rischi rappresentati dalla uso della Rete e delle TIC, di utenti molto giovani e spesso poco avveduti. Nel caso di infrazione si prevedono interventi, rapportati alla sua gravità, che vanno dalla semplice comunicazione del problema, alla convocazione da parte del coordinatore di classe o del Dirigente Scolastico.

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 Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto. La policy richiede l'integrazione con l'inserimento delle seguenti norme:

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

Disposizioni sull'uso dei software:

1. I software installati sono ad esclusivo uso didattico.
2. E' fatto divieto di usare software non conforme alle leggi sul copyright.

Accesso a internet:

1. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante.
2. Internet non può essere usato per scopi vietati dalla legislazione vigente.
3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle

vigenti leggi, per l'uso fatto del servizio Internet.

4. E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza. 5. Il tecnico responsabile che verifichi un uso del pc della scuola contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

Utilizzo dello smartphone e dei vari dispositivi tecnologici:

1. è vietato l'uso dello smartphone e dei dispositivi tecnologici da parte degli studenti e delle studentesse, durante lo svolgimento delle attività didattiche, salvo preventivo accordo con il docente per lo svolgimento di attività didattiche. Il divieto deriva dai doveri sanciti dallo Statuto degli studenti e delle studentesse (D.P.R. n. 249/1988). La violazione di tale divieto configura una infrazione disciplinare rispetto ai quali la scuola è tenuta ad applicare apposite sanzioni. I suddetti dispositivi devono essere tenuti spenti e opportunamente custoditi e depositati nei borsoni, zaini, giacconi, giammai sul banco né tra le mani. In caso di accordi con i docenti e per lo svolgimento di compiti e/o verifiche gli smartphone e altri dispositivi tecnologici possono essere depositati presso la cattedra.

2. Considerato che gli smartphone e altri dispositivi tecnologici possono essere utilizzati anche per scattare foto, effettuare riprese filmate, condividere contenuti con i social media, la scuola informa che, il verificarsi di tali eventi in orario scolastico, qualora configuri un'ipotesi di reato, verrà segnalato agli organi competenti.

3. In ogni caso, i genitori tengano conto che le comunicazioni urgenti ed improcrastinabili possono essere trasmesse ai loro figli durante l'orario scolastico rivolgendosi telefonicamente alle singole sedi scolastiche ovvero all'URP.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il monitoraggio dell'implementazione de documento di e-Policy e del suo eventuale aggiornamento sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore digitale, del Referente del bullismo e del cyberbullismo e del Gruppo di lavoro della policy.

Sarà finalizzato a rilevare la situazione iniziale delle classi e gi esiti a fine anno, in relazione all'uso sicuro e responsabile delle TIC e della Rete. Il monitoraggio sarà rivolto anche ai docenti, al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

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

Azioni da svolgere nei prossimi 3 anni:

- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori

Capitolo 2 - Formazione e curriculum

2.1. Curriculum sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più “intuitivo” ed “agile” rispetto agli adulti, ma non per questo sono dotati di maggiori “competenze digitali”.

Infatti, “la competenza digitale presuppone l’interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l’alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l’alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l’essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico” ([“Raccomandazione del Consiglio europeo relativa alla competenze chiave per l’apprendimento permanente”](#), C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curriculum digitale.

Per farlo, innanzitutto, dobbiamo avere ben chiaro cosa s’intende per “competenze digitali. Le competenze digitali richiamano diverse dimensioni sulle quali sarà possibile lavorare in classe, in un’ottica che integra la dimensione tecnologica con quella cognitiva ed etica (Calvani, Fini e Ranieri 2009):

- **dimensione tecnologica:** è importante far riflettere i più giovani sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana, onde evitare automatismi che abbiano conseguenze incerte, attraverso un’adeguata comprensione della “grammatica” dello strumento.
- **dimensione cognitiva:** fa riferimento alla capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete,

valutandone credibilità e affidabilità.

- **dimensione etica e sociale:** la prima fa riferimento alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui, e di usare le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri. La seconda, invece, pone un po' più l'accento sulle pratiche sociali e quindi sullo sviluppo di particolari abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online.

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

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

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

L'uso delle TIC nella didattica può rendere gli apprendimenti più motivanti, coinvolgenti ed inclusivi, inoltre permette al docente di guidare studenti e studentesse rispetto alla fruizione dei contenuti online, ormai la modalità naturale di apprendimento al di fuori della scuola, sviluppando anche capacità che sono sempre più importanti in ambito lavorativo, come il lavoro di gruppo anche a distanza e il confronto fra pari in modalità asincrona. Utile a tale proposito il canale YouTube [App Per Prof](#) .

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.

L'Istituto potrà programmare azioni come:

- **Analisi del fabbisogno formativo degli insegnanti sull'uso sicuro della Rete;**
- **Promozione della partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse".**
- **Organizzazione di incontri con professionisti della scuola o con esperti esterni, enti/associazioni, etc.**

Verrà predisposta inoltre un'area specifica sul sito dell'Istituto con materiali formativi per gli insegnanti, nella quale verranno messi a disposizione anche materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di Internet, incluso il link e i materiali informativi del progetto "**Generazioni connesse**".

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.

Sul sito scolastico verranno offerti consigli ai genitori su come gestire la relazione dei propri figli con le tecnologie digitali, in particolare verranno **forniti consigli sull'uso delle tecnologie digitali nella comunicazione** con i figli e in generale in famiglia, facendo riferimento anche alla sezione dedicata ai genitori del sito www.generazioniconnesse.it;

potranno essere organizzati inoltre percorsi di sensibilizzazione e formazione dei genitori su un uso responsabile e costruttivo della Rete in famiglia e a scuola.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022)

- 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.

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

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente

incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

Il nostro istituto si è prontamente adeguato alla suindicata normativa adempiendo a quanto in essa prescritto. E' stata attivata una specifica sezione Privacy sul sito web dell'istituto: https://www.istitutogkprato.edu.it/wp-content/uploads/2020/03/informativa_didattica_a_distanza_is_gramsci_prato-1.pdf.

Inoltre è stata predisposta una pagina sul sito dell'istituto dedicata alle problematiche connesse al bullismo e cyberbullismo: <https://www.istitutogkprato.edu.it/bullismo-cyberbullismo/>

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.

Da implementare con le indicazioni contenute nella lezione.

L'istituto gode di una strumentazione tecnologica diffusa capillarmente in tutti gli spazi, grazie ai finanziamenti europei statali PON, a quelli della Regione Toscana, ai progetti del Piano Nazionale Scuola Digitale. La connettività è garantita dalla fibra ottica in modalità via cavo e Wi-Fi ed offre la connessione ad internet per le attività sia didattiche sia amministrative. Il Dirigente Scolastico, il Direttore dei Servizi Generali e Amministrativi ed il personale degli uffici della segreteria sono profilati con account personalizzati e accedono ai servizi tramite procedura di autenticazione personale che prevede l'utilizzo di password aventi caratteristiche adeguate. L'assistenza tecnica del server e delle apparecchiature informatiche è affidata a d amministratore di rete esterno, soggetto specializzato nel settore, che provvede al controllo sul backup dei dati, all'aggiornamento dei sistemi operativi e degli antivirus installati sulle macchine e al controllo del funzionamento del firewall. La rete didattica, dotata di firewall dedicato, fornisce in sicurezza la connessione alle 70 classi provviste di strumentazione tecnologica, ai laboratori scientifici, e a quelli dedicati all'educazione motoria, alla biblioteca e alle aule multifunzionali destinate al lavoro dei docenti, all'auditorium per un totale di **250 PC** in rete. Il firewall non permette l'accesso ai siti non attendibili e ai social. L'accesso alla strumentazione e alla connessione è consentito ai docenti solo ai fini didattici ed è normato da password gestite dal responsabile della rete Lan-Wlan dell'Istituto e dagli assistenti tecnici informatici. Gli studenti accedono alla rete sotto il controllo dei docenti e degli assistenti durante le attività didattiche. La sensibilizzazione rispetto all'uso delle password viene fatta attraverso la diffusione di circolari circa l'utilizzo della strumentazione tecnologica da parte dei docenti. In particolare gli assistenti tecnici informatici hanno cura di aggiornare periodicamente il software e il sistema operativo a garanzia della protezione da aggressioni esterne e dalle vulnerabilità che emergono nel tempo. L'uso della tecnologia a scuola riguarda principalmente le attività laboratoriali per cui sia i docenti sia gli studenti adottano le indicazioni previste dai regolamenti approvati dal Consiglio di Istituto circa l'accesso alla Rete e ai dispositivi tecnologici. I regolamenti sono pubblicati sul sito web della scuola.

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.

Per la comunicazione interna viene utilizzato

-il registro elettronico che consente di gestire in modo ottimale la comunicazione con le famiglie che

hanno la possibilità di essere costantemente informate interagendo direttamente con la scuola

-mail scolastica

-applicativi e piattaforme che hanno favorito un lavoro collaborativo e condiviso rendendo possibile

un agevole passaggio alla didattica a distanza nel periodo di lockdown.

- ricorso qualora se ne presenti l'esigenza e a discrezione delle singole classi e/o C.D.C di gruppi whatsApp

3.4 - Strumentazione personale

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

La presente **ePolicy** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei

dispositivi mobili a scuola (BYOD, "Bring your own device").

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

Da implementare con le indicazioni contenute nella lezione.

Strumentazione personale

Per gli studenti

Durante le attività didattiche gli studenti sono autorizzati ad utilizzare la strumentazione personale quali cellulari, tablet ecc. solo ed esclusivamente per uso didattico e sotto il controllo del docente; altresì agli allievi non è permesso utilizzare i telefoni cellulari per telefonare, scattare foto, registrare filmati durante le lezioni o durante l'orario scolastico.

È vietato inviare messaggi illeciti o inappropriati, nonché fotografie o filmati.

La connessione ai servizi di internet per la propria **strumentazione viene fatta su rete personale. Eccezione sono gli alunni con BES o DSA, per i quali la scuola garantisce il supporto tecnologico idoneo, ma su richiesta dell'interessato: a loro è consentito l'uso della strumentazione personale con l'accesso alla rete wifi dell'istituto.**

Per i docenti

Durante le ore delle lezioni non è consentito l'utilizzo del cellulare se non per finalità strettamente didattica. È consentito l'uso di altri dispositivi elettronici personali sempre solo a scopo didattico ed integrativo di quelli scolastici disponibili. Durante il restante orario di servizio è permesso l'uso di portatili, tablet, per attività funzionali all'insegnamento in entrambe le situazioni ed è garantito l'accesso alla rete wifi negli spazi comuni previsti dalla logistica della rete stessa.

Per il personale della scuola Durante l'orario di servizio al personale scolastico è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022).

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle

studentesse

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA

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

- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- 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
- 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)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

Capitolo 4 - Rischi on line: conoscere, prevenire e rilevare

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

- Nel caso della **sensibilizzazione** si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.
- Nel caso della **prevenzione** si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.

Gli insegnanti, per la natura stessa del loro lavoro, devono in molti casi fungere da "torre di

avvistamento", avamposto privilegiato delle problematiche e dei rischi che gli adolescenti possono trovarsi ad affrontare ogni giorno.

Responsabilità degli insegnanti è, dunque, imparare a riconoscere i rischi più comuni

che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente.

Azioni

Scuola e famiglia possono essere determinanti nella diffusione di un atteggiamento mentale e

culturale che consideri la diversità come una ricchezza e che educi all'accettazione, alla

consapevolezza dell'altro, al senso della comunità e della responsabilità collettiva.

Occorre pertanto

rafforzare e valorizzare il Patto di Corresponsabilità educativa previsto dallo Statuto delle studentesse e degli studenti della scuola secondaria. La scuola è chiamata ad adottare misure atte a prevenire e contrastare ogni forma di violenza e di prevaricazione; la famiglia è chiamata a collaborare, non solo educando i propri figli, ma anche vigilando sui loro comportamenti.

Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte

degli studenti vi sono le seguenti:

- diffusione di un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web;
- organizzazione di incontri con testimoni (vittime e familiari) ed esperti (psicologo, Polizia Postale, Arma dei Carabinieri, associazioni ed enti attivi sul territorio ecc.) nelle singole classi e aventi per oggetto le tematiche del cyberbullismo, del sexting e dell'adescamento;
- partecipazione a eventi e spettacoli dedicati al tema del cyberbullismo;
- promozione di azioni formative rivolte al personale docente e alle famiglie e mirate alla rilevazione dell'insorgere di problematiche legate all'uso improprio del web;
- attività dello Sportello d'ascolto in presenza e servizio di consulenza on-line.
- attivazione di iniziative e di progetti mirati all'inclusione, all'accettazione e alla valorizzazione della diversità, al dialogo interreligioso e interculturale, alla destrutturazione degli stereotipi, alla prevenzione della violenza di genere.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione,

trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo”.

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

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di [cyberbullismo](#) e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
 - Ha il compito di coordinare le iniziative di prevenzione e contrasto del [cyberbullismo](#). A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
 - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d’istituto), atti e documenti (PTOF, PdM, Rav).

Saranno promosse azioni di sensibilizzazione e prevenzione (come dettagliate al punto 4.1) relative al fenomeno del cyberbullismo in tutte le sue manifestazioni.

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.

Saranno promosse azioni di sensibilizzazione e prevenzione (come dettagliate al punto 4.1) relative al fenomeno dell'hate speech.

4.4 - Dipendenza da Internet e gioco online

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

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

L’istituto promuoverà azioni di prevenzione attraverso percorsi sul benessere digitale.

Saranno inoltre promosse azioni di sensibilizzazione e prevenzione (come dettagliate al punto 4.1) relative al fenomeno della dipendenza da internet e gioco online.

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.

Saranno promosse azioni di sensibilizzazione e prevenzione (come dettagliate al punto 4.1) relative al fenomeno del sexting.

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.

Saranno promosse azioni di sensibilizzazione e prevenzione (come dettagliate al punto 4.1) relative al fenomeno dell’adescamento online.

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](#).

Saranno promosse azioni di sensibilizzazione e prevenzione (come dettagliate al punto 4.1) relative al tema della pedopornografia.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022).

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/le studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.
- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

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

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

prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.

- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.
- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

segnalare la presenza di materiale pedopornografico online.

5.2. - Come segnalare: quali strumenti e a chi

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

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

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

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

Per tutti i dettagli fate riferimento agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto

Generazioni Connesse, al numero gratuito [1.96.96](tel:1.96.96).

5.3. - Gli attori sul territorio

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

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

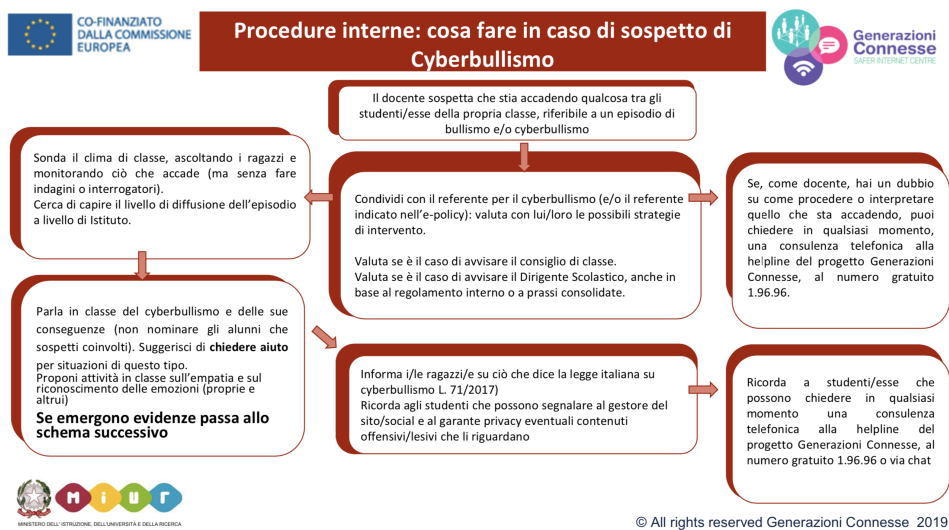
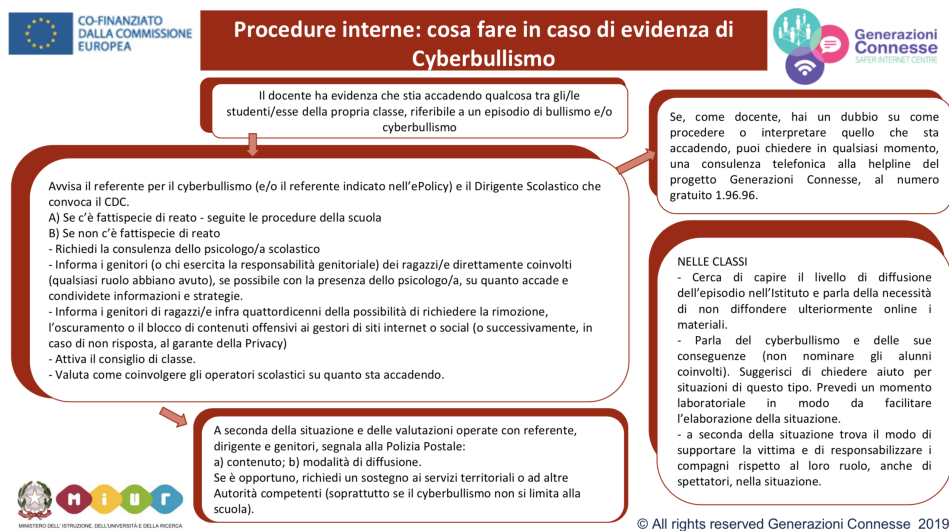
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all’utilizzo di Internet può presentare.

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

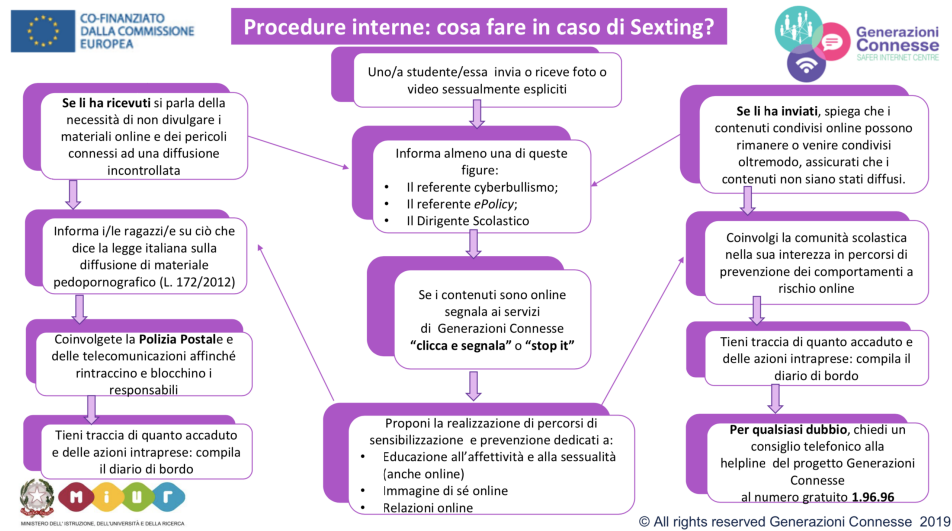
- **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

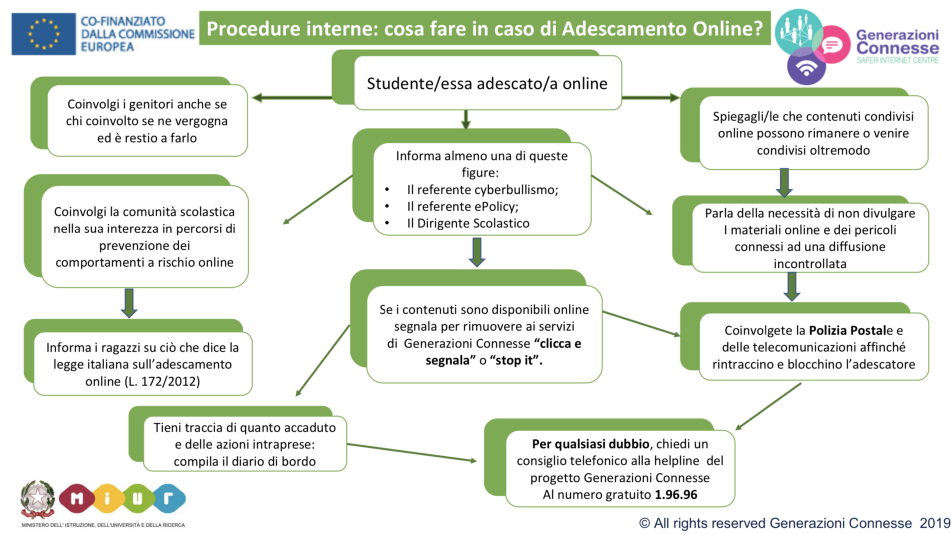
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



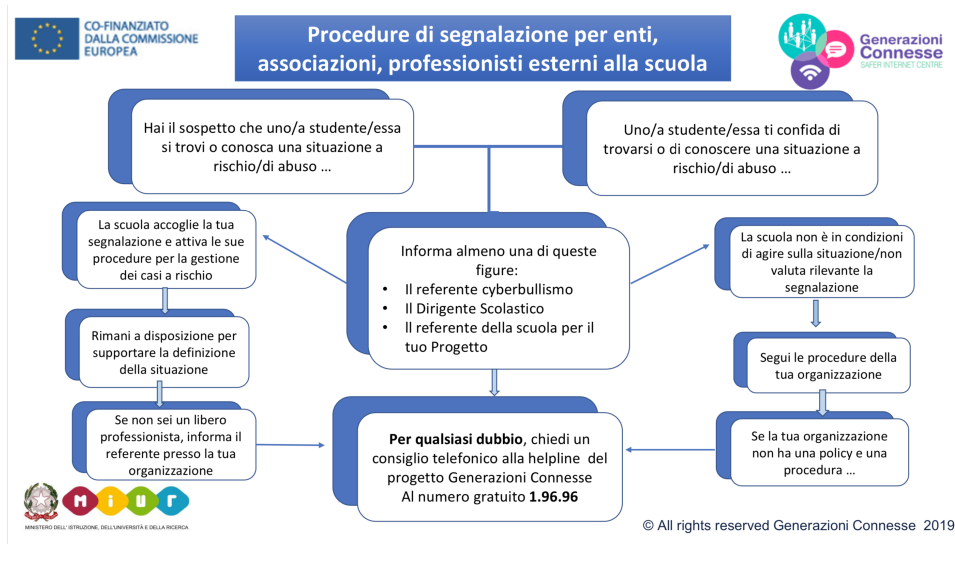
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il nostro piano d'azioni

L'Istituto si impegna durante l'anno scolastico 2021/2022 a stampare e rendere visibili, tramite affissione nei luoghi di maggiore frequentazione da parte di tutta la comunità scolastica, i manifesti e gli espositori riepilogativi che danno indicazioni sulle procedure di segnalazione nei casi fin qui citati. Inoltre verrà pubblicato sul sito della scuola, nella pagina dedicata al bullismo e cyberbullismo e ai rischi della Rete, il documento [iGloss@ 1.0 l'ABC dei comportamenti devianti online](#).

