



Documento di ePolicy

RMIS121002

GIORGI - WOOLF

VIALE P. TOGLIATTI 1161 - 00155 - ROMA - ROMA (RM)

ELENA TROPEA

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.

Oggi i ragazzi sono esposti a diversi stimoli provenienti dalla rete, sempre più coinvolti in un mondo virtuale nella doppia veste di creatori e fruitori di servizi web. Pur essendo nativi digitali necessitano di una guida per fruire in modo consapevole alle diverse risorse della rete in modo da sviluppare un approccio responsabile e un atteggiamento vigile sui diversi rischi della rete. Tutta la comunità scolastica si relaziona quotidianamente con le TIC (Tecnologie dell'informazione e della comunicazione) creando diversi sistemi comunicativi che offrono nuove opportunità ma anche nuovi pericoli e rischi. La cittadinanza digitale ci impone di aver ben chiare sia le opportunità che la rete offre sia i rischi che si incontrano in rete. Per tale motivo il nostro Istituto ha deciso di elaborare e dotarsi di un efficace strumento operativo come l'e-policy per regolamentare l'utilizzo delle TIC così da garantire un approccio positivo, critico e consapevole da parte degli studenti e studentesse, e a cui tutta la comunità può fare riferimento per poter acquisire quelle conoscenze e competenze necessarie per sviluppare, accrescere e consolidare una piena cittadinanza digitale oltre ad un uso sicuro e creativo della rete e delle risorse che mette a disposizione. In tale documento si pone attenzione soprattutto a delineare tutte quelle politiche preventive e di sensibilizzazione per contrastare comportamenti a rischio in rete.

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 ha la responsabilità di garantire la sicurezza di tutta la comunità scolastica, e quindi anche di quella in rete. Coadiuvato dal DPO (Data Protection Officer) sull'uso delle TIC:

- promuove e garantisce percorsi formativi rivolti a tutta la comunità scolastica su un uso consapevole delle Tic, e in collaborazione con il referente del Bullismo e Cyberbullismo e l'Animatore Digitale sulla sicurezza e sulle problematiche legate ai rischi in rete ;

- regolare il comportamento degli studenti e studentesse e imporre sanzioni disciplinari in caso di comportamenti inadeguati e uso improprio delle TIC;
- nel caso in cui venga a conoscenza di casi di comportamenti a rischio in rete o di episodi di bullismo o cyberbullismo, che non si configurino come reato, informa tempestivamente i genitori dei ragazzi coinvolti. Favorisce interventi mirati per classi e Consigli di classe.

Il DPO

Il DPO (Data Protection Officer) si occupa della gestione e del trattamento dei dati personali ed è responsabile di tutte le problematiche inerenti alla privacy.

L'Animatore Digitale

L'animatore digitale si occupa di:

- supportare tutto il personale scolastico nell'uso delle Tic;
- garantire la sicurezza interna della rete dell'Istituto;
- monitorare e rilevare problematiche emergenti rispetto all'utilizzo sicuro delle TIC e di Internet a scuola;
- individuare soluzioni innovative da diffondere all'interno della comunità scolastica;
- garantire l'aggiornamento delle componenti hardware e software della scuola.

La funzione strumentale per l'innovazione digitale

Si occupa di:

- Promuovere e formare i docenti sull'uso della piattaforma Office365 adottata dall'istituto;
- Redige il regolamento per la DDI;
- Predisporre le regole e i comportamenti per la privacy e la sicurezza nella piattaforma Office365;
- Elabora il documento sulla netiquette interna.

Referente del Bullismo e Cyberbullismo

- Coordina e promuove iniziative volte al contrasto del bullismo e cyberbullismo;
- Coordina e dirige percorsi formativi sul contrasto al bullismo e cyberbullismo volti al personale scolastico;
- Segnala con tempestività al Dirigente scolastico situazioni a rischio online o casi di bullismo e cyberbullismo.
- Coordina iniziative di prevenzione e contrasto del bullismo e cyberbullismo messe in atto dalla scuola, anche avvalendosi della collaborazione delle Forze di Polizia o di associazioni e centri di aggregazione giovanile presenti sul territorio;
- Si occupa di indirizzare studenti e studentesse e genitori, laddove rileva criticità, presso lo sportello di ascolto messo a disposizione dell'Istituto

Docenti

I Docenti si impegnano a:

- seguire percorsi formativi anche messi a disposizione dell'Istituto, sull'uso consapevole delle TIC, sull'uso della piattaforma Office365 adottata dalla scuola, sulla sicurezza in rete, sull'uso del digitale con particolare riferimento alla dimensione etica (tutela della privacy, diritto d'autore ecc..)
- supportare gli alunni sull'uso consapevole della rete e delle TIC utilizzati per scopi didattici;
- rispettare l'obbligo di riservatezza dei dati personali e non, in conformità alla normativa vigente (L. 675/1996);
- segnalare al Dirigente scolastico o ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola;
- segnalare al coordinatore di classe e al referente del bullismo eventuali episodi di bullismo o cyberbullismo rilevate all'interno della classe.

Il DSGA

Il direttore dei servizi generali e amministrativi e si preoccupa di:

- assicurare, nel limite delle risorse finanziarie, la manutenzione delle strutture informatiche al fine del suo funzionamento, della sicurezza e tutela da un uso improprio;
- assicurare, nel limite delle risorse finanziarie, la presenza di personale di supporto ai laboratori didattici.

Il Personale Amministrativo, Tecnico e Ausiliario (ATA)

Il Personale ATA è tenuto ad assicurarsi di:

- aver consapevolezza riguardo alle questioni di sicurezza informatica, alla politica adottata dall'Istituto e alle relative buone pratiche;
- segnalare qualsiasi abuso al Dirigente scolastico.

Gli studenti

Gli studenti e le studentesse hanno il compito di:

- leggere il Regolamento d'Istituto di cui la scuola si è dotato;
- utilizzare con responsabilità le TIC uniformandosi alle indicazioni dei docenti;
- saper distinguere, anche con l'aiuto dei docenti, le fonti di informazioni attendibili in rete;
- avere consapevolezza dei rischi in rete, dell'uso consapevole del cellulare, delle fotocamere e dei rischi che si incorrono nel diffondere notizie false o immagini senza il consenso delle persone coinvolte.
- Essere consapevoli della gravità di atti di bullismo e cyberbullismo a tutela della propria e altrui incolumità, al fine di evitare violazioni del Regolamento

d'Istituto e del Patto di Corresponsabilità o, nei casi più gravi reati puniti dalla Magistratura.

I Genitori

I Genitori svolgono un ruolo fondamentale nel garantire che gli studenti e le studentesse comprendano la necessità di un utilizzo sicuro, consapevole ed appropriato di tutti i dispositivi digitali e della rete. È fondamentale che essi prendano visione dell'e-policy e di:

- Sostenere e collaborare con i docenti nell'azione educativa sull'uso consapevole delle TIC;
- Contribuire alla sensibilizzazione dei propri figli sulla sicurezza e i rischi della rete;
- Collaborano con i docenti per scoraggiare e contrastare l'uso non responsabile, scorretto o pericoloso delle tecnologie digitali;
- Incoraggino l'uso delle Tic per i compiti a casa vigilando sui propri figli sull'uso in totale sicurezza e consapevolezza delle tecnologie in ambiente domestico.

Gli Enti educativi esterni e le associazioni

Gli enti educativi e le associazioni che entrano in contatto con l'Istituto hanno il compito di:

- Rispettare le politiche interne dell'Istituto sull'uso consapevole delle TIC e della rete;
- Garantire comportamenti sicuri per la protezione degli studenti e delle studentesse durante le attività che vengono svolte e che coinvolgono gli stessi.

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).

Lo scopo principale dell'Epolicy è quello di individuare regole e comportamenti da condividere con soggetti esterni, i quali avranno cura di prenderne visione. Per ogni progetto esterno viene individuato un docente referente che si fa garante del corretto svolgimento del progetto e segnala eventuali criticità alla Dirigenza. Inoltre l'Istituto è dotato di un regolamento che tutela la privacy dei ragazzi nei vari progetti in cui sono coinvolti, avvisando le famiglie e chiedendo il consenso su attività che coinvolgono i loro figli.

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.

L'e-policy, come tutti i regolamenti del nostro Istituto, verrà comunicato con circolare a tutta la comunità scolastica oltre ad essere pubblicato sul sito della scuola, nel giornalino scolastico e sulla piattaforma ufficiale (Teams).

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.

È molto importante intervenire, laddove si manifestassero dei comportamenti non idonei, su tutto il gruppo classe con attività specifiche volte alla sensibilizzazione e con lo scopo di promuovere una maggiore consapevolezza sui rischi di un uso inappropriato delle TIC e di Internet e sul senso civico.

In base alla gravità e alla natura dell'infrazione la scuola, dopo aver informato la famiglia e attivato interventi rieducativi, valuterà la necessità di denunciare l'episodio agli organi competenti e di garantire un immediato supporto psicologico attraverso lo sportello di ascolto presente nella nostra scuola.

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.

L'ePolicy sarà integrato con il Regolamento d'Istituto, Il Regolamento- netiquette adottato per la piattaforma Office365 che la scuola utilizza per comunicazioni in rete tra docenti e docenti, docenti e studenti, docenti e famiglie e Enti esterni; con Il Piano Triennale dell'Offerta formativa, con il curriculum d'Istituto di Educazione Civica.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il monitoraggio e l'aggiornamento del documento di E-Policy sarà affidato al referente del Bullismo e Cyberbullismo e ai docenti che hanno partecipato alla stesura dello stesso. Il documento verrà aggiornato in corrispondenza di cambiamenti significativi a livello normativo sull'uso delle TIC e sarà monitorato valutando l'efficacia dello stesso in riferimento al raggiungimento degli obiettivi specifici raggiunti dallo stesso.

Il nostro piano d'azioni

Azioni da svolgere nell'anno scolastico 2022/2023:

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

Azioni da svolgere nei prossimi 3 anni:

- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy 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.

I Docenti del nostro Istituto hanno sviluppato a partire dall’anno scolastico 2020/2021 un curriculum verticale di Educazione civica, in linea con la legge 92 del 20 agosto 2019 e con le Linee guida pubblicate con il D.M. n. 35 del 22.06.2020. I presenti documenti hanno introdotto l’insegnamento trasversale dell’educazione civica che il nostro istituto ha accolto redigendo un curriculum delle competenze per singola annualità. Infatti al termine di ciascun anno e in riferimento al curriculum di Educazione Civica d’Istituto che integra i nuclei fondanti (Costituzione, Ambiente, Digitale) gli studenti e le studentesse realizzano un prodotto che rende evidenti le competenze acquisite e previste in uscita come richiesto dal quadro normativo Europeo.

Nell’ambito delle Tic la competenza digitale presuppone l’utilizzo delle nuove tecnologie con dimestichezza, spirito critico, responsabilità per apprendere, lavorare, comunicare, collaborare e partecipare attivamente alla vita sociale. Essa presuppone l’alfabetizzazione informatica e digitale, l’alfabetizzazione mediatica, la creazione di

contenuti digitali, la netiquette da seguire in rete e negli ambienti digitali, la sicurezza dei dati che circolano in rete e alle violazioni della privacy, le questioni legate al copyright e alle proprietà intellettuali. Per questo il nostro Istituto si impegna a portare avanti percorsi volti a promuovere l'acquisizione di tali competenze, al fine di educare tutta la comunità scolastica, e in particolare gli studenti e le studentesse verso un uso sempre più consapevole e responsabile delle Tic.

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.

Ogni docente deve conoscere e saper usare le Tic (Tecnologie dell'Informazione e della comunicazione) sia per un uso consapevole ma soprattutto come parte integrante della didattica al fine di sviluppare, progettare, utilizzare, gestire e valutare i processi di insegnamento e apprendimento di tutti gli studenti e le studentesse della classe, con particolare attenzione anche alle persone con disabilità per le quali le nuove tecnologie possono rappresentare una parte integrante dell'apprendimento. Per questo motivo l'Istituto Superiore Giorgi- Woolf incoraggia l'uso delle TIC nella didattica come parte integrante di essa e ha dotato la scuola di Digital-Board per permettere al maggior numero di insegnanti un accesso a contenuti digitali. Inoltre la scuola fornisce la possibilità ai docenti di partecipare a corsi di formazione interna ed esterna, aggiornamento, supporto e assistenza per l'uso di tutte le tecnologie di cui la scuola è dotata.

2.3 - Formazione dei docenti sull'utilizzo consapevole e sicuro di

Internet e delle tecnologie digitali

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

La scuola attiva ogni anno un corso sul bullismo e cyberbullismo per formare i nuovi docenti dell'istituto sul tema e sulle politiche adottate dalla scuola. Inoltre sulla base della rilevazione dei bisogni formativi dei docenti promuoverà e organizzerà di volta in volta interventi formativi mirati. Inoltre l'Animatore Digitale e la Figura Strumentale per l'innovazione digitale sono quotidianamente impegnate a supporto dei docenti. In particolare l'Animatore Digitale si occupa di controllare ed implementare le infrastrutture digitali (hardware e software) utilizzate presso l'Istituto. Mentre la Figura Strumentale per l'innovazione digitale cura il corretto funzionamento della piattaforma Teams e verifica che docenti e alunni ne facciano un uso appropriato.

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.

Il nostro istituto si fa promotore e collaboratore di diverse iniziative del nostro

territorio che vengono presentate sul sito della scuola. Le famiglie sono invitate a partecipare liberamente o su indicazioni del consiglio di classe in base alla necessità dei singoli alunni. Le diverse iniziative, insieme al Patto di corresponsabilità firmato dalle famiglie, garantiscono la collaborazione tra tutti gli attori educanti.

Il nostro piano d'azioni

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

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare un evento di presentazione e conoscenza dell'Epolicy rivolto ai docenti.

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

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggior interesse nell'ambito dell'educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

L'istituzione scolastica può trattare i dati personali necessari al perseguimento di specifiche finalità istituzionali oppure quelli espressamente previsti dalla normativa vigente di settore tutelandone la segretezza come previsto dalla legge (L. 675/1996).

In ogni caso viene fornito all'interessato (studente, genitore, docente, personale ATA) un'adeguata informativa sulle caratteristiche e modalità dell'utilizzo dei loro dati, indicandone i responsabili di trattamento. Laddove previsto l'informativa comprende uno specifico e libero consenso, mediante apposita modulistica, nella quale viene indicato chiaramente quali saranno le finalità da perseguire, senza che vengano richiesti ulteriori dati ma quanto strettamente necessario.

Lo studente e la famiglia hanno diritto di conoscere quali informazioni che li riguardano sono conservate presso il nostro Istituto, di rettificare o aggiornarne il contenuto.

La scuola è dotata di un regolamento di Istituto che disciplina l'accesso ai vari laboratori, agli spazi alternativi per l'apprendimento e alla rete LAN.

Il personale docente, non docente e gli studenti del nostro Istituto sono dotati di un account sulla piattaforma Office365 e di un email istituzionale con dominio giorgiwoolf.it.

3.2 - Accesso ad Internet

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

disabilità.

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

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

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

L'istituto, in tutte le sue sedi, gode di una strumentazione tecnologica diffusa in tutti gli spazi, grazie ai finanziamenti europei statali PON e ai progetti del Piano Nazionale Scuola Digitale.

La connettività è garantita sia in modalità via cavo sia Wi-Fi ed offre la connessione ad internet per le attività sia didattiche sia amministrative.

La rete didattica fornisce in sicurezza la connessione a tutte le classi provviste di strumentazione tecnologica, ai laboratori scientifici, multimediali, alla biblioteca e alle aule multifunzionali destinate al lavoro dei docenti. In tutti questi spazi l'utilizzo quotidiano del registro elettronico è gestito da Spaggiari-ClassiveViva che ne garantisce la protezione dei dati, così come la normativa richiede. 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 nei laboratori.

Gli assistenti tecnici informatici e l'animatore Digitale 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.

In accordo alle politiche di gestione della privacy e della sicurezza nativamente

implementate dalla piattaforma Office365, l'accesso alla medesima da parte di alunni e docenti è regolato dalle più ristrette norme inerenti la materia. La scuola ha inoltre adottato i seguenti criteri generali di security: gestione delle utenze, gestione degli accessi (password, backup, ecc.), e-mail, archiviazione documenti.

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.

Relativamente agli ambienti di apprendimento il nostro istituto per la sede Giorgi si avvale di:

- 5 laboratori di informatica
- 4 laboratori di mecatronica
- 3 laboratori elettronica
- 2 laboratori di elettrotecnica
- 1 laboratorio di fisica
- 1 laboratorio di chimica
- 3 laboratori di automazione
- 1 biblioteca
- 40 Aule dotate di digital board
- 7 Digital board disponibili sui piani
- 1 Cabinet con n 40 tablet
- 20 Portatili

Tutti i laboratori sono dotati di Digital Board o LIM.

Relativamente agli ambienti di apprendimento il nostro istituto per la sede Woolf si avvale di:

- 2 laboratori di informatica
- 1 laboratorio di fisica
- 1 laboratorio di grafica
- 2 laboratori di moda
- 1 laboratorio di fotografia

- 4 Aule dotate di Digital Board

Per quanto riguarda gli strumenti di comunicazione esterna il nostro istituto utilizza il sito web (www.giorgiwoolf.edu.it) costantemente aggiornato.

Per quanto riguarda la comunicazione interna viene utilizzato

- Il registro elettronico (portale SpaggiariClasseViva) che consente di gestire in modo ottimale le comunicazioni scuola-famiglia.
- L'email istituzionale giorgiwoolf.it e la piattaforma Office365

Applicazioni e piattaforme che hanno favorito un lavoro collaborativo e condiviso (Teams, Form, Pacchetto Office Online)

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.

Per gli studenti

Durante le attività didattiche gli studenti sono autorizzati ad utilizzare la strumentazione personale quali cellulari, tablet, PC 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, salvo diversa indicazione da parte del docente. 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.

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.

Il nostro piano d'azioni

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

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Organizzare uno o più eventi o attività volti a formare il personale scolastico dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali, con la partecipazione del DPO
- Organizzare uno o più eventi o attività volti a formare il personale scolastico dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

- Organizzare uno o più eventi o attività volti a formare i genitori 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 scolastico dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali, con la partecipazione del DPO
- 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.

Il curriculum di Educazione Civica sviluppato dal nostro istituto prevede, per ogni annualità, consente la riflessione sui nuclei fondanti l'Educazione Civica fornendo strumenti di analisi e lettura consapevole delle opportunità e dei rischi del digitale, non dando mai per scontato che "i nativi digitali, non abbiano bisogni formativi specifici"

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).

La nostra scuola è dotata di un Referente Bullismo-Cyberbullismo d'istituto che si occupa di sensibilizzazione e prevenzione al bullismo e cyber bullismo sia i docenti che gli alunni.

In ogni classe viene nominato annualmente un referente del bullismo per ogni componente (docente, alunni, genitore) che lavora in sinergia con il Referente Bullismo-Cyberbullismo ove necessario.

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.

Le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica nell'arco dei tre anni di valenza del PTOF:

- Partecipazione ad eventi e incontri con le Forze dell'Ordine per la prevenzione del bullismo e del cyberbullismo e per la prevenzione e la sensibilizzazione sui reati legati all'utilizzo di internet e delle piattaforme online,
- Elezione annuale del referente bullismo e cyberbullismo,
- Attivazione di iniziative, di progetti e di PCTO 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
- Attivazione di percorsi di Materia Alternativa, dall'a.s. 2021/2022 la disciplina tratta l'Educazione all'empatia

- Uso integrato delle TIC nella didattica, nel rispetto della libertà di insegnamento dei singoli docenti
-

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?

Il nostro istituto partecipa da anni al progetto Game Over in collaborazione con la Caritas di Roma. Il progetto è rivolto alle classi seconde dell'istituto, per sensibilizzare e contrastare la ludopatia tra la popolazione giovane che come conseguenza porta all'isolamento sociale e a problematiche interrelazionali e interpersonali.

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 medialmente 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.

Le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica nell'arco dei tre anni di valenza del PTOF:

- Partecipazione ad eventi e incontri con le Forze dell'Ordine per la prevenzione del bullismo e del cyberbullismo e per la prevenzione e la sensibilizzazione sui reati legati all'utilizzo di internet e delle piattaforme online,
- Partecipazione al progetto Scuole Sicure in collaborazione con la Polizia di Stato rivolto alle classi prime,
- Elezione annuale del referente bullismo e cyberbullismo,

- Attivazione di iniziative, di progetti e di PCTO 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
 - Attivazione di percorsi di Materia Alternativa, dall'a.s. 2021/2022 la disciplina tratta l'Educazione all'empatia
 - Uso integrato delle TIC nella didattica, nel rispetto della libertà di insegnamento dei singoli docenti
-

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.

Le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica nell'arco dei tre anni di valenza del PTOF:

- Partecipazione ad eventi e incontri con le Forze dell'Ordine per la prevenzione del bullismo e del cyberbullismo e per la prevenzione e la sensibilizzazione sui reati legati all'utilizzo di internet e delle piattaforme online,
- Partecipazione al progetto Scuole Sicure in collaborazione con la Polizia di Stato rivolto alle classi prime,
- Elezione annuale del referente bullismo e cyberbullismo,
- Attivazione di iniziative, di progetti e di PCTO 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

- Attivazione di percorsi di Materia Alternativa, dall'a.s. 2021/2022 la disciplina tratta l'Educazione all'empatia
 - Uso integrato delle TIC nella didattica, nel rispetto della libertà di insegnamento dei singoli docenti
 - Progetto sull'Educazione alla Salute in collaborazione con ANLAIDS.
-

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](#).

Le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica nell'arco dei tre anni di valenza del PTOF:

- Partecipazione ad eventi e incontri con le Forze dell'Ordine per la prevenzione del bullismo e del cyberbullismo e per la prevenzione e la sensibilizzazione sui reati legati all'utilizzo di internet e delle piattaforme online,
- Partecipazione al progetto Scuole Sicure in collaborazione con la Polizia di Stato rivolto alle classi prime,
- Elezione annuale del referente bullismo e cyberbullismo,
- Attivazione di iniziative, di progetti e di PCTO 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
- Attivazione di percorsi di Materia Alternativa, dall'a.s. 2021/2022 la disciplina tratta l'Educazione all'empatia
- Uso integrato delle TIC nella didattica, nel rispetto della libertà di insegnamento dei singoli docenti

Il nostro piano d'azioni

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

- 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 laboratori di educazione alla sessualità e all'affettività,

rivolti agli/le studenti/studentesse.

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

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

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/le 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.

Tutti gli attori della scuola, ognuno con le proprie competenze, sono tenuti ad impegnarsi per prevenire, riconoscere, segnalare ed affrontare episodi di bullismo e cyberbullismo ed a operare affinché la scuola sia un ambiente sereno ed armonioso.

In ogni classe viene nominato annualmente un referente del bullismo per ogni componente (docente, alunni, genitore) che lavora in sinergia con il Referente Bullismo-Cyberbullismo d'Istituto ove necessario.

5.2. - Come segnalare: quali strumenti e a chi

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

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

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

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

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

Strumenti a disposizione di studenti/esse

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

- un indirizzo e-mail specifico per le segnalazioni;

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

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito [1.96.96](tel:19696).

Caso A: sospetto

Il docente ha il sospetto che stia avvenendo qualcosa tra gli studenti della sua classe, riferibile ad un episodio di bullismo e cyberbullismo, sexting o adescamento online. Le due opzioni di segnalazioni sono le seguenti:

1. Confronto verbale tra il docente di classe e il docente referente del bullismo della classe e successivamente con il docente referente per le iniziative di prevenzione e contrasto del cyberbullismo;
2. Comunicazione formale dei fatti al docente referente facendo uso dell'indirizzo mail istituzionale dedicato

CASO B: EVIDENZA

Il docente ha evidenza certa che stia accadendo qualcosa tra gli studenti della propria classe, riferibile ad un episodio di bullismo e cyberbullismo, sexting o adescamento online. La procedura di segnalazione è la seguente:

Informa immediatamente del fatto sia coordinatore di classe che il docente referente per le iniziative di prevenzione e contrasto del cyberbullismo che prende in carico la pratica. Il docente referente ne dà immediata notizia al Dirigente Scolastico (o al primo collaboratore e/o al secondo collaboratore).

Il Dirigente Scolastico, con il coordinatore di classe e il referente del bullismo scolastico incontrano la famiglia e l'alunno e, ove necessario, informa le forze dell'ordine.

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.

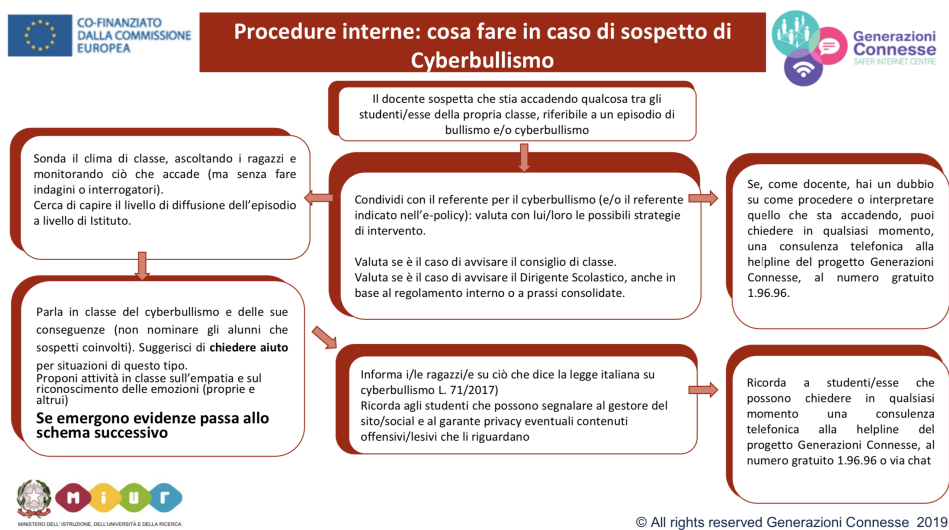
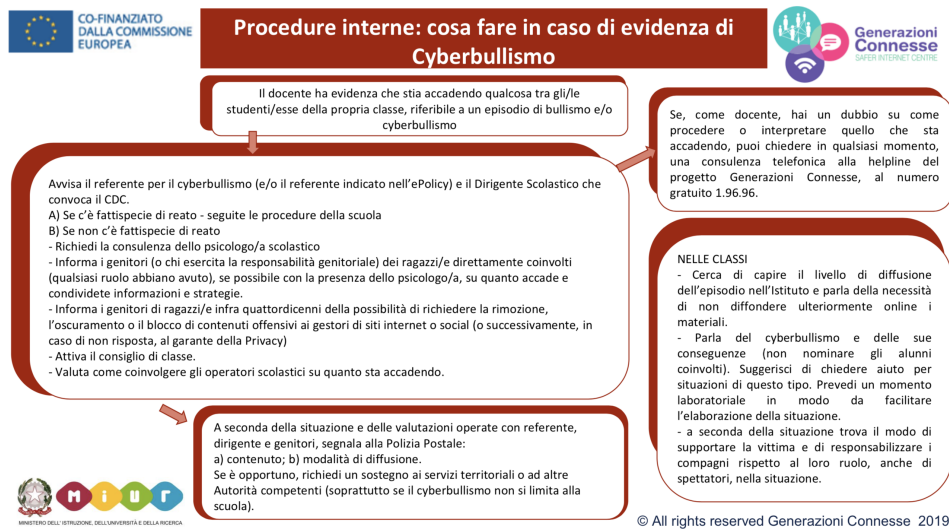
Per una mappatura degli indirizzi di tali strutture è possibile consultare il [Vademecum](#) di Generazioni Connesse “Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all’utilizzo delle tecnologie digitali da parte dei più giovani” (seconda parte, pag. 31), senza 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.

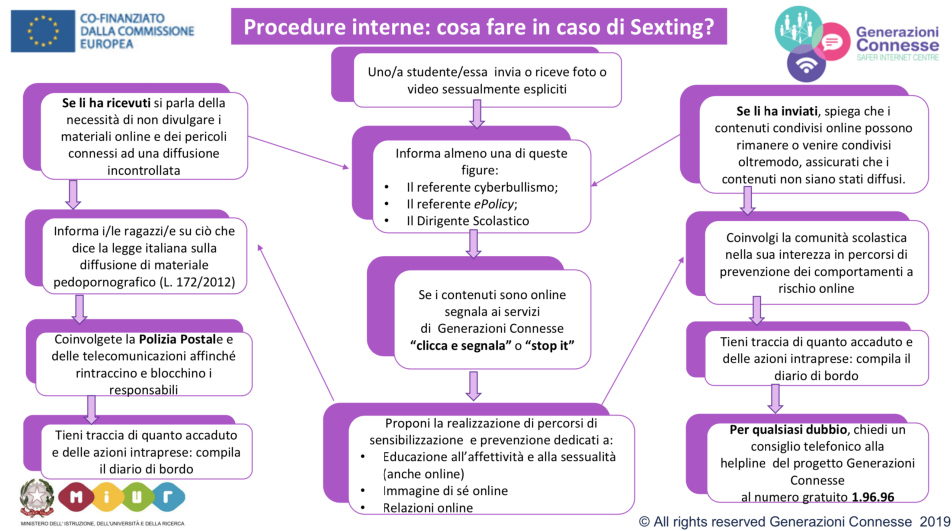
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell’infanzia.
 - **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare 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.
-
- CARITAS LAZIO, progetto Game Over
 - ALS ROMA 2
 - ASL ROMA 1
 - ANLAIDS Onlus, progetto prevenzione alla salute

5.4. - Allegati con le procedure

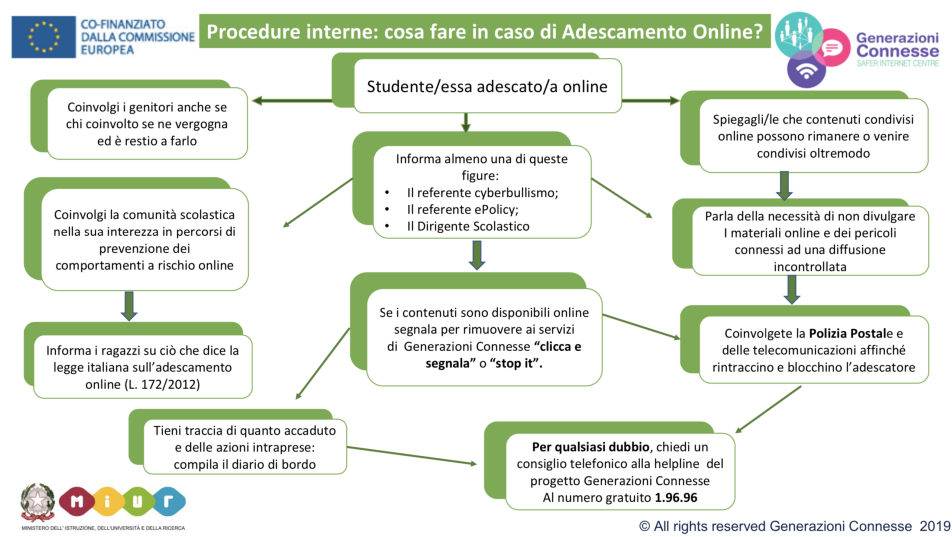
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



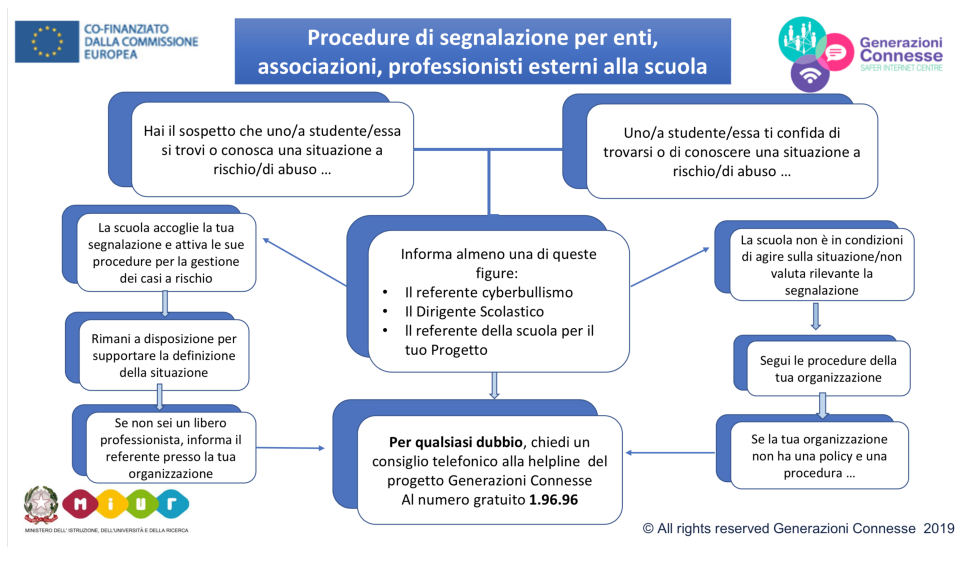
Procedure interne: cosa fare in caso di sexting?



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

- Integrazione del regolamento di Istituto nell'ottica dell'Epolicy
- Pubblicazione sul sito scolastico www.giorgiwoolf.edu.it del documento di Epolicy
- Creazione e pubblicazione sul sito della modulistica specifica per la segnalazione di episodi di Bullismo e Cyberbullismo.
- Pubblicazione sul sito scolastico dell'email del referente contro il bullismo e del cyberbullismo

