Documento di ePolicy

GRIC828005

IC"LEOPOLDO II L." FOLLONICA 2

VIA BALDUCCI 2 - 58022 - FOLLONICA - GROSSETO (GR)

Paola Brunello

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 curricolo**
    1. Curricolo sulle competenze digitali per gli studenti
    2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
    3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
    4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
    1. Protezione dei dati personali
    2. Accesso ad Internet
    3. Strumenti di comunicazione online
    4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
    1. Sensibilizzazione e prevenzione
    2. Cyberbullismo: che cos'è e come prevenirlo
    3. Hate speech: che cos'è e come prevenirlo
    4. Dipendenza da Internet e gioco online
    5. Sexting
    6. Adescamento online
    7. Pedopornografia
5. **Segnalazione e gestione dei casi**
    1. Cosa segnalare
    2. Come segnalare: quali strumenti e a chi
    3. Gli attori sul territorio per intervenire
    4. Allegati con le procedure

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

L'Istituto Comprensivo "Leopoldo II di Lorena" di Follonica ha elaborato il presente documento dell'E Policy per promuovere e diffondere nell'intera comunità educante l'utilizzo positivo delle TIC nella didattica e negli ambienti scolastici e per definire le misure necessarie di prevenzione, di rilevazione e relativa gestione delle problematiche derivanti da un uso scorretto e inconsapevole 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 è responsabile della sicurezza dei dati offline e on line dell'intera comunità scolastica.

Promuove la cultura della sicurezza on line proponendo insieme all'animatore digitale e al referente sul bullismo e cyberbullismo corsi per l'utilizzo positivo delle TIC.

Garanìtisce l'applicazione del presente documento.

L'Animatore digitale supporta il personale scolastico in ambito tecnico-informatico e fornisce indicazioni utili sui rischi on line, sulla protezione e gestione dei dati personali. Monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola. Cura insieme al Referente bullismo e cyberbullismo la redazione e la revisione annuale del presente documento di e-Policy e ne favorisce la massima diffusione; promuove azioni di formazione interna alla scuola negli ambiti del PNSD.

Il Referente bullismo e cyberbullismo coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. Cura insieme all'animatore digitale la redazione e la revisione annuale del documento di e-Policy. Coordina gli interventi di gestione di eventuali azioni di cyberbullismo.

I Docenti diffondono tra i loro studenti e studentesse la cultura dell'uso responsabile delle TIC e della Rete. Inseriscono laddove sia possibile l'uso delle tecnologie digitali nella didattica. Segnalano qualsiasi abuso o violazione, anche sospetto, al D.S. per le

opportune indagini.

Il Personale Amministrativo, Tecnico e Ausiliario controlla che gli utenti autorizzati accedano alla Rete della scuola con apposita password esclusivamente per scopi istituzionali e consentiti, ovvero istruzione e formazione. Segnala al Dirigente scolastico, al referente del bullismo/cyberbullismo e ai docenti responsabili comportamenti non adeguati e/o episodi di bullismo e cyberbullismo. Collabora nel reperire, verificare e valutare informazioni inerenti possibili casi di bullismo e cyberbullismo.

I genitori partecipano alle iniziative organizzate dalla scuola sui temi della sicurezza on line; collaborano con i docenti comunicando con loro circa i problemi rilevati quando i/le propri/e figli/e non usano in modo responsabile le tecnologie digitali o internet. Si impegnano ad accettare quanto scritto nel documento E-Policy nel momento della sottoscrizione del patto di corresponsabilità.

Gli Alunni e le Alunne si impegnano ad utilizzare correttamente gli strumenti e le tecnologie digitali come previsto da questa e-policy. Con il supporto dei docenti devono imparare a tutelare se stessi e i propri/e compagni/e on line, comprendere le potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche la necessità di evitare il plagio e rispettare i diritti d'autore. Si fanno promotori di quanto appreso eventualmente attraverso percorsi di peer education.

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).

In caso di attività progettuale rivolta agli studenti tutti gli attori esterni sono tenuti a provvedere preventivamente alla raccolta delle debite autorizzazioni delle famiglie per proteggere i dati personali degli alunni e acconsentirne il trattamento.

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

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

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

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

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

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

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 nell'apposita sezione dedicata al Bullismo e cyberbullismo.

Inoltre nel sito istituzionale il documento E- Policy verrà pubblicato anche in versione child friendly; questa viene ulteriormente condivisa con gli alunni anche sulla Piattaforma in uso della scuola.

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.

In caso di infrazione all'E-policy saranno presi dei provvedimenti disciplinari da adottare da parte dei consigli di classe in proporzione sia all'età dello studente sia alla gravità dell'infrazione commessa. Essi possono essere: o richiamo verbale; o il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante) o sanzioni estemporanee commisurate alla gravità della violazione commessa (assegnazione di attività aggiuntive da svolgere a casa su temi di Cittadinanza e Costituzione); o nota informativa ai genitori o tutori mediante registro elettronico; o convocazione dei genitori o tutori per un colloquio con gli insegnanti; o convocazione dei genitori o tutori per un colloquio con il Dirigente scolastico, o sospensione dalle lezioni. Nel caso in cui l'infrazione si costituisca come reato, verrà effettuata segnalazione alle autorità competenti.

Nel capitolo 5 verranno analizzati nel dettaglio i comportamenti sanzionabili sia degli studenti sia dei docenti qualora utilizzino impropriamente device o la Rete o non intervengano nella segnalazione di condotte improprie dei/lle propri/e studenti/studentesse.

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.

La ePolicy è coerente con quanto stabilito dalla Legge (Statuto delle studentesse e degli studenti della scuola secondaria DPR 24 giugno 1998 n. 249 modificato dal DPR 21 novembre 2007 n. 235; Legge 29 maggio 2017 n. 71 "Disposizioni a tutela dei

minori per la prevenzione e il contrasto del fenomeno del cyberbullismo"; Legge 31 dicembre 1996 n. 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali") dai Regolamenti vigenti e dal Patto di Corresponsabilità.

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 della Policy avverrà contestualmente alla revisione del PTOF, a cura del Dirigente scolastico, dell'Animatore digitale, e dei collaboratori del Dirigente, a seguito di verifica atta a constatare l'insorgenza di nuove necessità e la revisione di tecnologie esistenti.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- 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

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

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

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

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

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

La scuola promuove una cultura multimediale, reticolare, attraverso una didattica stimolante e collaborativa: obiettivo primario è quello di sviluppare un sapere interdisciplinare attraverso la realizzazione di prodotti multimediali, l'uso delle Lavagne Interattive Multimediali e delle TIC più in generale, la didattica computazionale. Ciò consente di proporre una nuova dimensione del linguaggio scritto, un nuovo rapporto insegnamento/apprendimento e una diversa relazione docente/studente.

Il nostro Istituto si impegna all'elaborazione nell'ambito di un triennio di un curricolo digitale tenendo conto del Quadro comune di riferimento europeo per le competenze digitali (Digcomp del 2013, Digcomp 2.0 del 2016 e Digicomp 2.1del 2017 e il più recente aggiornamento Digicomp 2.2 pubblicato il 22/03/2022).

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'Istituto "Leopoldo II di Lorena" favorisce la partecipazione del personale docente ad inizative sull'uso delle TIC organizzate direttamente dalla scuola suggerite per esempio dall'animatore digitale, oppure proposte da altri enti, oppure liberamente scelte dai docenti . Si impegna inoltre ad organizzare momenti di formazione per migliorare le competenze didattiche digitali degli insegnanti.

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 invita a effettuare la formazione sul sito di Generazioni Connesse utilizzando le credenziali fornite tramite mail istituzionale.

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.

La scuola invita i genitori a effettuare il corso di educazione digitale per le famiglie e gli studenti Google be internet awsone, a visitare il portale di Generazioni Connesse e a consultare il materiale informativo presente nell'area dedicata al cyberbullismo del nostro Istituto.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore 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.

In fase di iscrizione degli alunni all'IC Leopoldo II di Lorena, i genitori sottoscrivono un'informativa sul trattamento dei dati personali in ottemperanza all'art. 13 D.Lgs 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).

All'inizio di ogni anno scolastico i genitori rilasciano il consenso all'utilizzo di materiale fotografico e audiovisivo riservato ed elaborati degli alunni per esporli anche in sedi diverse da quelle dell'Istituto quali pubblicazioni in formato digitale e siti web.

In caso di attività di ampliamento dell'offerta formativa, organizzate in collaborazione con Enti esterni, viene richiesto preventivamente ai genitori il consenso informato alle riprese audio/ video e al loro eventuale utilizzo per scopi didattici, informativi e divulgativi anche tramite pubblicazione su siti web.

L'accesso ai dati riportati nel registro elettronico (ritardi, assenze, note e valutazioni) è riservato ai genitori della Scuola Primaria e Secondaria di primo grado tramite l'invio di una password di accesso strettamente personale.

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'accesso alla rete Internet al Personale Docente viene consentito con la modalità di connessione "wireless" (mediante gli access point). Le alunne e gli alunni possono accedere alla rete Internet esclusivamente con dispositivi dell'istituzione scolastica, in occasione di attività didattiche e/o formative svolte nei laboratori sotto la responsabilità e la sorveglianza di un insegnante.

La rete Internet non può essere utilizzata per scopi vietati dalla legislazione vigente e gli utenti sono direttamente responsabili, civilmente e penalmente, a norma delle vigenti leggi, per ogni attività svolta.

È vietato scaricare e/o installare software sui PC e/o mobile device della scuola senza preventiva autorizzazione del referente per la Sicurezza Informatica.

Nella pratica didattica, il docente ha un ruolo fondamentale di responsabilità nel favorire l'uso corretto della rete, guidando gli studenti nelle attività online, stabilendo obiettivi chiari di ricerca, insegnando le strategie appropriate nella definizione e nella gestione delle risorse digitali su Web.

3.3 - Strumenti di comunicazione online

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

Il sito della nostra scuola è raggiungibile all'indirizzo http://www.iclorena.edu.it

Altri mezzi di comunicazione online, in dotazione alla scuola, sono: il registro elettronico *Scuole toscane* con tutte le sue funzionalità, la email, ulteriori applicativi e piattaforme di lavoro condiviso e collaborativo come Google Workspace for Education, app incluse. In seguito alla sospensione delle attività didattiche per l'emergenza coronavirus, si è reso necessario attivare modalità di didattica digitale integrata, al fine di garantire e tutelare il diritto all'istruzione, attraverso l'utilizzo della piattaforma sopraindicata.

3.4 - Strumentazione personale

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

La presente ***ePolicy*** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

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

L'utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica è possibile previa autorizzazione del docente. In questi casi lo studente ha il dovere: di assolvere assiduamente agli impegni di studio, di tenere comportamenti rispettosi e

corretti, di osservare le disposizioni organizzative dettate dai regolamenti di istituto secondo quanto descritto nel DM n. 30 del 15/03/2007 - "Linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, doveri di vigilanza e di corresponsabilità dei genitori e dei docenti".

La famiglia deve impegnarsi "a rispondere direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone o alle strutture scolastiche o, più in generale, violino i doveri sanciti dal regolamento di istituto e subiscano, di conseguenza, l'applicazione di una sanzione anche di carattere pecuniario". I docenti e il personale ATA hanno il dovere di vigilare sui comportamenti degli studenti e delle studentesse. Tale dovere sussiste in tutti gli spazi scolastici e comprende la responsabilità di segnalare eventuali infrazioni suscettibili di sanzioni disciplinari. In virtù della normativa vigente posta a tutela della privacy, è fatto divieto di utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire, divulgare e/o pubblicare immagini, filmati o registrazioni vocali senza il consenso esplicitamente espresso in forma scritta dagli interessati o i loro tutori (nel caso di minori). In altre parole, è punibile sia a livello civile che penale (oltre che le sanzioni previste dagli artt. 3 e 4, d.P.R. 24 giugno 1998, n. 249 - "Regolamento recante lo statuto delle studentesse e degli studenti della scuola secondaria"), chi abusa dei dati personali altrui raccolti (immagini, filmati, registrazioni vocali...), violandone la privacy.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

- Organizzare incontri per la consultazione degli studenti/studentesse suindicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamentisull'uso dei dispositivi digitali personali a scuola
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati 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 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 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)

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

Scegliere almeno 1 di queste azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte deglistudenti e delle studentesse
- Organizzare incontri per la consultazione degli studenti/studentesse suindicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamentisull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati 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 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 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.*

Sensibilizzazione: il nostro istituto si pone come obiettivo di attivare delle strategie a partire dalle classi quarte della scuola primaria e sino all'intero ciclo della secondaria di primo grado. Si organizzano attività, preventivamente programmate, in primo luogo per informare,in secondo luogo per educare alla consapevolezza e alla riflessione sui pericoli derivanti da un uso scorretto della rete e dalla dipendenza dallo smarthphone.

Prevenzione: si promuovuono negli studenti le competenze previste dal curriculo digitale. Inoltre per tutta la comunità scolastica sono previsti incontri con esperti esterni e promossa la conoscenza del presente e-policy e del progetto generazioni connesse.

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).

Il cyberbullismo può essere diretto quando il bullo utilizza strumenti di messaggistica istantanea che hanno effetto immediato sulla vittima oppure indiretto quando il bullo utilizza spazi pubblici della Rete (es. social network, blog, chat) per diffondere in maniera rapida, così da diventare virali, contenuti dannosi e diffamatori per la vittima.

Il cyberbullismo non riguarda unicamente la vittima e il cyberbullo, è un fenomeno sociale, infatti coinvolge un gruppo. Per questo motivo l'efficacia degli interventi di prevenzione e di contrasto è direttamente proporzionale al coinvolgimento di tutte le componenti della comunità scolastica (gruppo classe, personale scolastico, famiglie).

Ecco perchè tra le azioni già realizzate o pianificate per il futuro, dal nostro istituto per la prevenzione, il contrasto e la gestione dei casi di cyberbullismo, in linea con quello che prevede la normativa, ci sono:

- la nomina di un Referente per la prevenzione e il contrasto del cyberbullismo che ha acquisito le conoscenze utili a sviluppare le competenze richieste, a reperire strumenti e a produrre materiali da mettere a disposizione dell'intera comunità scolastica, grazie anche alla formazione completata sull'apposita piattaforma di Generazioni connesse per la stesura del presente documento programmatico ePolicy;
- l'attivazione di uno sportello di ascolto;
- la formazione del personale scolastico;
- la predisposizione di un Curricolo Digitale trasversale e verticale da integrare nella progettualità delle classi; l'ntegrazione dei curricoli disciplinari con attività legate al tema del bullismo e del cyberbullismo;
- la comunicazione tempestiva ai genitori degli alunni coinvolti in eventuali atti di cyberbullismo, fatta eccezione per gli episodi che costituiscono reato (Legge 71/2017, art.5); segnalazione agli organi competenti degli episodi imputabili come reati;
- 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.

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.

La nostra scuola prevede, durante le ore curricolari, la condivisione di riflessioni individuali al fine di sensibilizzare gli studenti alla capacità di discernimento e fornire loro dunque gli strumenti necessari per raggiungere gli obiettivi sopra elencati ovvero 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 e favorire una presa di parola consapevole e costruttiva.

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 prevede di fornire alla scuola, agli studenti e alle loro famiglie gli

strumenti necessari per riconoscere e prevenire il fenomeno di dipendedenza da internet o dal gioco on line, senza per questo demonizzare la tecnologia o il virtual game. In questo senso la scuola può insegnare molto da questo punto di vista integrando la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online.

La partecipazione al safer internet day è sicuramente un buono stimolo per attivare delle riflessioni sull'uso corretto della rete.

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.

Al fine di sensibilizzare i giovani e le loro famiglie sull'argomento, i docenti devono in primo luogo parlarne con alunne e alunni e rispettivi genitori, ricordando loro che l’invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Spesso i nativi digitali non sono pienamente consapevoli che una foto o un video diffusi in rete potrebbero non essere tolti mai più né si rendono conto di scambiare o diffondere materiale pedopornografico. È importante in questa azione di prevenzione la collaborazione della famiglia, informandola sull'opportunità di attivare forme di controllo della navigazione dei loro figli.

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.

Sensibilizzare attraverso dibattiti o attività specifiche , in collaborazione con la Polizia postale, i ragazzi dell'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione.

Sensibilizzare le famiglie sul problema invitandole a monitorare le attività dei propri figli in rete a partire dal momento in cui viene concessa loro la possibilità di navigare in modo solitario e di gestire autonomamente un proprio profilo sui social network o di utilizzare un proprio indirizzo di posta elettronica.

Qualora si venga a conoscenza di casi di adescamento on-line, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.

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.

La segnalazione facilita il processo di rimozione del materiale stesso dalla Rete e allo stesso tempo consente le opportune attività investigative finalizzate ad identificare chi possiede quel materiale, chi lo diffonde e chi lo produce, ma, soprattutto, ad identificare i minori abusati presenti nelle immagini e video, assicurando la fine di un abuso che potrebbe essere ancora in corso e il supporto necessario. Parallelamente, se si ravvisa un rischio per il benessere psicofisico delle persone minorenni coinvolte nella visione di questi contenuti, sarà opportuno rivolgersi ad un servizio deputato ad offrire un supporto psicologico anche passando per una consultazione presso il medico di base o pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza (Consultori Familiari, Servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, etc.). Nel caso in cui una persona minorenne sia direttamente coinvolta

nelle immagini, bisogna tenere in considerazione che l'attuale normativa (legge 172 del 2012, art. 351 c.p.p.) prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui la pedopornografia online, debba essere ascoltata dalle autorità competenti in sede di raccolta di sommarie informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

Scegliere almeno 1 di queste azioni:

☐ 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/lle studenti/studentesse

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

Scegliere almeno 1 di queste azioni:

☐ Organizzare uno o più incontri di 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/lle studenti/studentesse.

☐ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per

segnalare la presenza di materiale pedopornografico online.

Il personale scolastico dovrà segnalare tutte le situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o un piccolo gruppo) tramite un utilizzo irresponsabile di internet.

La scuola, quindi, avrà cura di porre attenzione alla rilevazione di rischi connessi alla navigazione sul web. In particolare si segnaleranno: - contenuti afferenti la violazione della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.); - contenuti relativi all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.); - contenuti attinenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudi o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc. Tutte le segnalazioni riportate dai docenti verranno registrate sull'apposita Scheda di Prima Segnalazione redatta dalla scuola.

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.

Nel CASO A, si dovrebbe coinvolgere innanzitutto il referente d'Istituto per il contrasto del bullismo e del cyberbullismo valutando insieme le possibili strategie d'intervento. Si potrebbe pensare anche alla possibilità di avvisare l'intero consiglio di classe e, se si ravvisa la necessità e l'urgenza, di coinvolgere il Dirigente Scolastico.

Nel frattempo, il docente (e i docenti informati) ascolta gli studenti e le studentesse, osservando e monitorando il clima di classe, ciò che accade, le dinamiche relazionali nel contesto classe, senza fare indagini dirette. Uno strumento utile per raccogliere informazioni può essere il diario di bordo (vrdi sllegato). Inoltre, il docente deve cercare di capire se gli episodi sono circoscritti al gruppo o se interessano l'intero Istituto. Operativamente è fondamentale coinvolgere tutti gli studenti e le studentesse, informandoli sui fenomeni e sulle caratteristiche degli stessi, suggerendo di chiedere aiuto se pensano di vivere situazioni, di subire atti identificabili come bullismo o cyberbullismo.

Sarebbe opportuno (sempre monitorando la situazione) prevedere momenti laboratoriali, utilizzando anche la piattaforma Generazioni Connesse nella parte dei contenuti e dei materiali; tali attività possono essere molto positive, stimolare il dialogo e la riflessione fra gli studenti e le studentesse. Infine, sottolineare che è il referente scolastico sulle tematiche che può prendere in carico la situazione, alla luce della normativa vigente e in particolare della Legge n.71 del 2017.

Se si ha un dubbio su come procedere o interpretare quello che sta accadendo a scuola, si può chiedere, in qualsiasi momento, una consulenza telefonica alla Helpline

del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Se gli agiti osservati si identificano come atti di bullismo o cyberbullismo, il docente e la scuola tutta devono intervenire seguendo il CASO B.

Nel CASO B, il docente deve condividere immediatamente quanto osservato con il referente per il bullismo e il cyberbullismo (e/o il referente indicato nell'ePolicy), valutando insieme le possibili strategie di intervento. Si avvisa anche il Dirigente Scolastico che convoca il consiglio di classe. Se non si ravvisano fattispecie di reato, si dovrebbe:

- informare i genitori (o chi esercita la responsabilità genitoriale) degli/delle studenti/studentesse direttamente coinvolti/e (qualsiasi ruolo abbiano avuto), se possibile con la presenza dello psicologo, su quanto accade e condividete informazioni e strategie;
- richiedere, in concomitanza, la consulenza dello psicologo scolastico a supporto della gestione della situazione, in base alla gravità dell'accaduto;
- informare i genitori degli/delle studenti/studentesse infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy);
- informare gli/le studenti/studentesse ultra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy);
- attivare il consiglio di classe;
- valutare come coinvolgere gli operatori scolastici su quello che sta accadendo.

A seconda della situazione e delle valutazioni effettuate con referente, dirigente e genitori, si potrebbe poi segnalare alla Polizia Postale: a) contenuto del materiale online offensivo; b) modalità di diffusione; c) fattispecie di reato eventuale.

Se è opportuno, richiedere un sostegno ai servizi e alle associazioni territoriali o ad altre autorità competenti (pensiamo al cyberbullismo, con il suo impatto sulla vita quotidiana della vittima, la quale sa che i contenuti lesivi sono online, diffusi fra molte persone conosciute e non, in un circuito temporale senza fine e senza barriere spaziali).

È bene sempre dialogare con la classe, attraverso interventi educativi specifici, cercando di sensibilizzare studenti e studentesse sulla necessità di non diffondere ulteriormente online i materiali dannosi, ma anzi di segnalarli e bloccarli. Ciò è utile anche per capire il livello di diffusione dell'episodio all'interno dell'Istituto.

In ogni plesso di scuola primaria e nella scuola secondaria si fa riferimento per eventuali segnalazioni ai relativi fiduciari.

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.

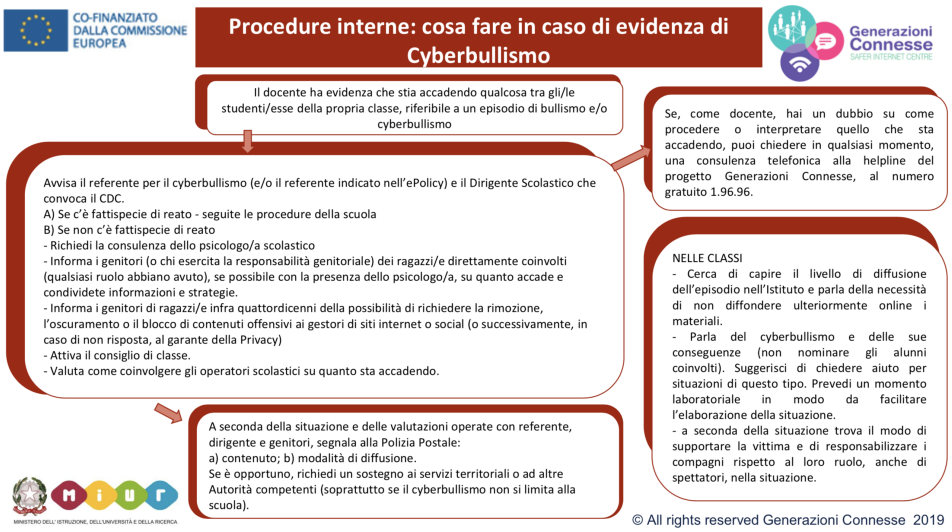
Questura Grosseto: tel 0564-433111/399111 mail: gab.quest.gr@pecps.poliziadistato.it

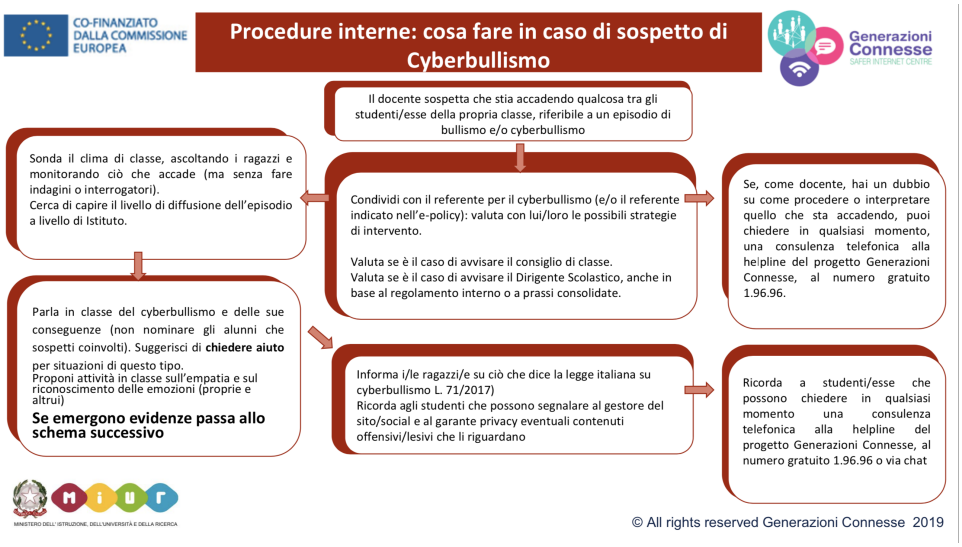
Consultorio Principale Follonica C/o Distretto socio-sanitario Viale Europa 1 Tel 0566/59521

Sito della **Polizia Postale**: http://www.commissariatodips.it/collabora.html
Sezione di **Grosseto** Viale Matteotti, 1 – tel. **0564/448609** – **0564/448443**

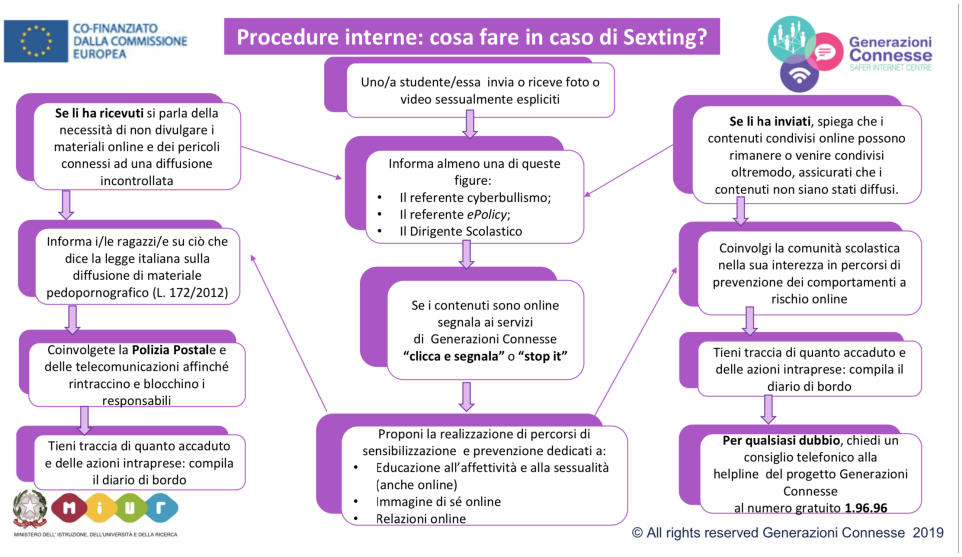
5.4. - Allegati con le procedure

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

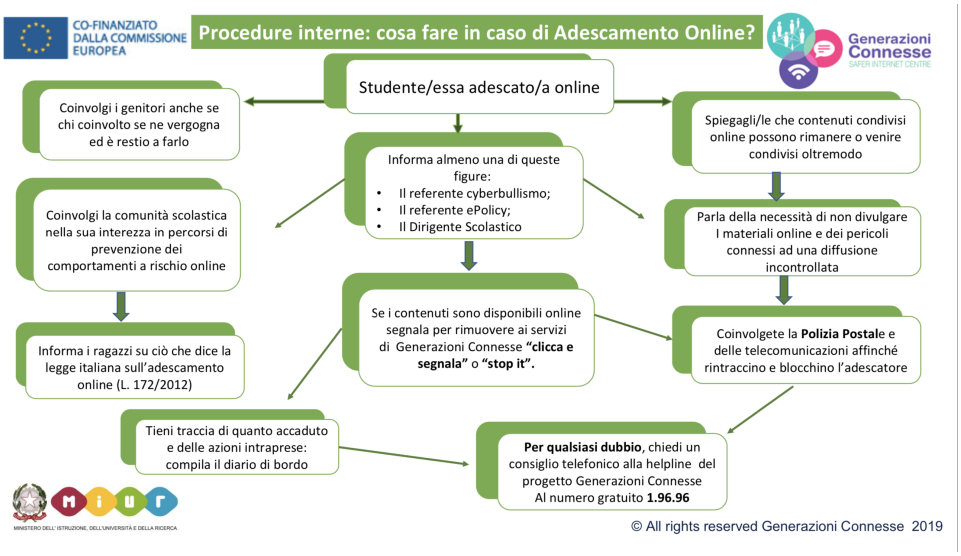




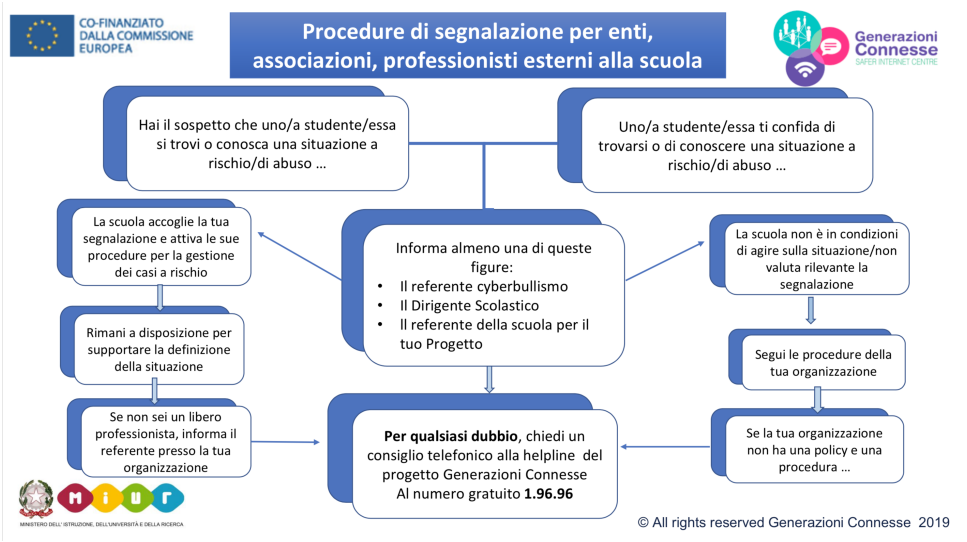
Procedure interne: cosa fare in caso di sexting?



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

Tutte le condotte riconducibili nelle definizioni giuridiche di bullismo e di cyberbullismo, sono sanzionate dalla Scuola, laddove poste in essere all'interno dell'istituto scolastico, con le seguenti modalità:

a. La scuola, nella persona della Dirigente Scolastica o di chi la rappresenta, informa tempestivamente i genitori (o chi esercita la responsabilità genitoriale), qualora venga a conoscenza di atti di bullismo o cyberbullismo che non si configurino come reato.

b. I comportamenti, accertati, che si configurano come forme di bullismo e cyberbullismo vengono considerati come infrazione grave e vengono sanzionati sulla base di quanto previsto nel regolamento disciplinare degli studenti . Lo studente che ha commesso atti di bullismo/cyberbullismo sarà soggetto a provvedimenti di natura disciplinare così come disciplinati dal D.P.R. 24 giugno 1998 n.249 (Statuto delle studentesse e degli studenti), modificato ed integrato dal D.P.R. 21 novembre 2007 n.235; sanzioni che vanno dalla sanzione scritta e/o sospensione in seguito alla verifica dell'intensità della condotta.

c. Gli episodi di bullismo e cyberbullismo saranno sanzionati, con sanzioni particolarmente incisive per i fatti di estrema gravità, attivando anche percorsi educativi di recupero, mediante lo svolgimento di attività di natura sociale, culturale e in generale a vantaggio della comunità scolastica; Vengono considerate deplorevoli le condotte dei compagni sostenitori del bullo perché, pur non partecipando direttamente alle prevaricazioni, con il loro assenso contribuiscono a rafforzare il comportamento del bullo.

d. Se si dovessero attivare percorsi di DDI, i docenti solleciteranno gli alunni ad impegnarsi a frequentare le lezioni sincrone in modo responsabile, evitando scambi di persona, supporti di altri soggetti, o comportamenti poco onesti. La partecipazione alle attività sincrone è soggetta alle stesse regole che determinano la buona convivenza in classe e soggiace alle medesime sanzioni previste dal vigente Regolamento d'Istituto, in particolare si richiede di: a. Rispettare gli orari indicati dal docente; b. Collegarsi da ambienti idonei (ad esempio in una stanza in casa in luogo tranquillo-isolato, mentre non si fanno altre cose; usare un linguaggio appropriato; tenere un abbigliamento corretto, ecc....); c. Nel caso siano impossibilitati a frequentare una o più lezioni sincrone (sia per motivi tecnici, tipo connessioni, che per altri motivi, tipo salute) gli studenti sono tenuti ad avvertire il docente di riferimento. d. È severamente vietato utilizzare chat private e registrare attività o riprendere le persone

attraverso video recording o strumenti catturaimmagini, ancorché disponibili tra le funzioni delle piattaforme digitali in uso. La diffusione di dati ed immagini personali, l'utilizzo improprio o addirittura offensivo dei canali di comunicazione connessi alla didattica a distanza è sanzionato in proporzione alla gravità dei comportamenti rilevati fino alla sospensione e alla non ammissione agli scrutini. L'alunno e la sua famiglia si assumono la piena responsabilità di tutti i dati da lui/lei inoltrati, creati e gestiti attraverso le piattaforme utilizzate o le diverse modalità di didattica attivate L'Istituto non sarà responsabile di quanto l'alunno/a potrà inserire sulle piattaforme o nelle chat che saranno attivate.