Documento di ePolicy

CEIC80800N

COLLECINI - GIOVANNI XXIII

VIA GIARDINI REALI - 81020 - CASERTA - CASERTA (CE)

Antonio Varriale

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.

Il presente documento nasce a seguito dell'adesione da parte del nostro Istituto al progetto promosso da Safer Internet Centre – Generazioni Connesse "a.s. 2019/20, diramato con nota MIUR

AOODRCA n. 0019710 dell'11/09/2019 ed avente ad oggetto: "Azioni di prevenzione dei fenomeni di bullismo e cyberbullismo e di azioni di educazione ad un uso corretto e consapevole della rete e delle nuove tecnologie".

Il documento è stato redatto dai membri del gruppo di lavoro delle epolicy, in conformità con quanto previsto dalle "LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo" (aprile 2015 e aggiornamento ottobre 2017) dalla Legge 107/2015 " Riforma del sistema nazionale di istruzione e formazione e delega per il riordino delle disposizioni legislative vigenti" e dalla legge 29 maggio 2017, n.71 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo.

Il progetto è coordinato dal MIUR con il partenariato di alcune delle principali realtà italiane che si occupano di sicurezza in Rete: Autorità Garante per l'Infanzia e l'Adolescenza, Polizia di Stato, il Ministero per i Beni e le Attività Culturali, gli Atenei di Firenze e 'La Sapienza' di Roma, Save the Children Italia, Telefono Azzurro, la cooperativa EDI onlus, , Skuola net e l'Agenzia di stampa DIRE e l'Ente Autonomo Giffoni Experience.

Il Safer Internet Centre (noto anche come SIC) nasce per fornire informazioni, consigli e supporto a bambini, ragazzi, genitori, docenti ed educatori che hanno esperienze, anche problematiche, legate a Internet e per agevolare la segnalazione di materiale illegale online. L'obiettivo generale è di sviluppare servizi dal contenuto innovativo e di più elevata qualità, al fine di garantire ai giovani utenti la sicurezza nell'ambiente on line/ ambiente fisico, considerando, al contempo, il connesso investimento come un'occasione 'virtuosa' per una crescita 'sociale' ed economica dell'intera collettività.

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 garante per la sicurezza, anche online, di tutti i membri della comunità scolastica;
- promuove ed attiva buone prassi mediante l'organizzazione di corsi di formazione specifici per tutte le figure scolastiche sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIUR;
- promuove, con la collaborazione del docente Referente d'Istituto per le tematiche del bullismo e del Cyberbullismo, corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC.
- ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

L'Animatore digitale

- Promuove percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica);
- coordina la diffusione dell'innovazione digitale nell'ambito delle azioni previste dal Piano nazionale Scuola Digitale;
- assicura che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

Il Referente bullismo e cyberbullismo

"Ogni Istituto scolastico, nell'ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo" (Art. 4 Legge n.71/2017, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo" (permalink – file 1 LEGGE 71_2017 in allegato).

- Promuove e coordina iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio.
- Coinvolge la comunità scolastica, (studenti, colleghi, genitori e altri attori del territorio) con progetti e percorsi formativi ad hoc;
- Collabora con tutte le agenzie educative e istituzionali presenti sul territorio per prevenire e gestire i casi di possibile cyberbullismo.

I Docenti

i Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete.

- Garantiscono l'integrazione di parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica;
- supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete;
- hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse, secondo le procedure indicate nel protocollo d'emergenza.

Il personale Amministrativo, Tecnico e Ausiliario (ATA)

- Svolge funzioni di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il dirigente scolastico e con il personale docente tutto;
- segnala comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure interne preposte.
- raccoglie, verifica e valuta le informazioni inerenti possibili casi di bullismo/cyberbullismo, insieme ad altre figure interne preposte.

Gli Studenti e le Studentesse

- Sono responsabili, in relazione al proprio grado di maturità e consapevolezza raggiunta, di utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti;
- sono tenuti/e, al rispetto delle norme che disciplinano l'utilizzo consapevole delle tecnologie con la finalità di salvaguardare la propria identità e quella degli altri;
- possono partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

I Genitori

- Partecipano attivamente, in continuità con l'Istituto scolastico, ad attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali;
- concordano con i docenti le linee educative che riguardano le TIC e la Rete
- Comunicano ai docenti i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Interne.;
- accettano e condividono quanto scritto nell'ePolicy dell'Istituto.

Gli Enti educativi esterni e le associazioni

- Osservano le politiche interne della scuola riguardo all'uso consapevole della Rete e delle TIC;
- adottano comportamenti sicuri per la protezione degli studenti e delle studentesse durante le attività in cui sono impegnati gli stessi.

Per quanto non espressamente indicato sui ruoli e sulle responsabilità delle figure presenti all'interno dell'Istituzione scolastica, si rimanda: alla Legge 59/97 Art. 21 CO° 8; alla Legge N.165/2001 Art. 25; al CCNL in vigore; al DPR n. 275/99; alla Legge n.107/2015; al Piano Nazionale Scuola Digitale.

Si rimanda, inoltre, alle norme in materia di corresponsabilità educativa e formativa che riguardano sia i genitori che la scuola nel percorso di crescita degli studenti e delle studentesse, in particolare:

al 2° comma dell'art. 2048 c.c.; al 1° comma dell'art. 30 della Costituzione; al 1° comma dell'art. 2048 c.c; all'art. 147 del c.c ed, infine, a quanto statuito in materia di culpa in vigilando, culpa in organizzando, culpa in educando.

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).

I soggetti esterni sono tenuti, inoltre, a conoscere le procedure di segnalazione da seguire e a rispettare il protocollo di emergenza qualora vengano a conoscenza di problematiche connesse ad un uso non consapevole delle tecnologie digitali,

Tutte le attività progettuali e di formazione devono essere preventivamente presentate ed esplicitate in modo dettagliato al Dirigente Scolastico, che dovrà autorizzarle con modalità e tempi concordati con il referente d'Istituto per il contrasto al bullismo e Cyberbullismo.

Le figure professionali e le organizzazioni coinvolte in progetti, laboratori e attività, dovranno prendere visione di tutti i documenti relativi alle norme succitate proposti dall'Istituto e sottoscriverli preliminarmente all'avvio dei programmi con gli studenti e le studentesse, in classe o fuori.

L'Istituto richiederà agli attori esterni i documenti richiesti per legge come fattore ulteriormente protettivo verso i minori, con l'obiettivo di verificare l'esistenza (o meno) di condanne per alcuni reati previsti dal Codice penale e nello specifico gli articoli 600-bis (prostituzione minorile), 600-ter (pornografia minorile), 600-quater (detenzione di materiale pornografico), 600-quinquies (iniziative

turistiche volte allo sfruttamento della prostituzione minorile), 609-undecies (adescamento di minorenni), o l'irrogazione di sanzioni interdittive all'esercizio di attività che comportino contatti diretti e regolari con i minori.

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.

Come suggeriscono le LINEE GUIDA PER L'USO POSITIVO DELLE TECNOLOGIE DIGITALI E LA PREVENZIONE DEI RISCHI NELLE SCUOLE, bisogna adottare una "strategia integrata e globale", che preveda il coinvolgimento di tutti gli attori della scuola ed una alleanza educativa tra scuola e famiglia, perché si consolidi l'idea di una "scuola comunità".

È questo il motivo per cui l'intero personale scolastico viene informato sul corretto uso dei dispositivi e della Rete in linea, anche facendo riferimento al Codice di Comportamento dei Pubblici Dipendenti. Tutto il personale scolastico è consapevole che una condotta non in linea con la normativa è sanzionabile.

Allo scopo di condividere regole comuni per l'utilizzo sicuro di Internet sia a casa che a scuola, si invitano i genitori a prestare la massima attenzione ai principi e alle regole contenute nel documento di e-Policy. Si richiede che ogni genitore o tutore si impegni nel farle rispettare ai propri figli anche in ambito domestico, innanzitutto assistendo i minori nel momento di utilizzo della rete vigilando sui contatti social e ponendo in atto tutti i sistemi di sicurezza del caso che aiutino a diminuire il rischio di imbattersi in materiale indesiderato.

Una strategia adottata dall'istituto è proprio quella di stilare una "netiquette" in versione child friendly, che consenta con un linguaggio semplice e diretto ai destinatari, ovvero agli studenti e alle studentesse di conoscere e comprendere poche semplici regole per l'accesso e in generale l'uso di Internet, tanto in ambito scolastico, quanto extrascolastico. A maggior ragione, la necessità di socializzare con tutti gli attori del mondo scuola un insieme di regole di buona educazione e buon comportamento in Rete è divenuto una emergenza contingente all'alba della Didattica a Distanza. A questo riguardo è stata emanata dal nostro Istituto una Circolare volta a regolamentare l'oggetto di cui sopra.

CIRCOLARE SUL CORRETTO UTILIZZO DELLE PIATTAFORME DIGITALI 16/04/2020

Al fine di garantire un uso corretto e responsabile degli strumenti digitali, nel rispetto della normativa vigente si precisa quanto segue. Gli strumenti di apprendimento digitale a distanza hanno scopi esclusivamente didattici e non possono essere utilizzate per altri scopi. Si tratta di ambienti "virtuali" che consentono a insegnanti e alunni di condividere materiali per lo studio individuale.

Tutte le attività sono condotte dai docenti nell'ambito dell'esercizio dell'attività di insegnamento ed esclusivamente per finalità didattiche.

Le interazioni tra minori e adulti consentite attraverso gli strumenti digitali sono riconducibili a quelle che si svolgono in classe nelle modalità di insegnamento ordinarie

L'accesso a questi strumenti può avvenire, disponendo di una connessione internet, sia da computer che da tablet o smartphone.

Lo studente è tenuto a utilizzare la piattaforma solo per fini didattici. Sarà cura dei singoli insegnanti attivare spazi disciplinari invitando gli studenti delle proprie classi o gruppi di lavoro.

NETIQUETTE PER L'AULA VIRTUALE

La netiquette è l'insieme delle regole che dettano i parametri di educazione e buon comportamento sulla Rete (dall'inglese net), è, cioè, sinonimo di buon comportamento quando si usa internet, e nel nostro caso quando si usano le classi virtuali.

Regole di comportamento

1. L'aula virtuale è un'aula a tutti gli effetti, poco importa se è nel tuo giardino, sul balcone o in cucina. Pertanto, considerala tale: quello che non è concesso in classe, non lo è nemmeno qui. Vestiti in modo consono, evita di dedicarti ad altre attività, silenzia il cellulare.

2. La puntualità è una delle regole più importanti da osservare. Se la video lezione inizia alle 9:00 fai in modo di esserci per quell'ora. Il tuo ingresso ad un orario successivo disturberà chi sta parlando e costringerà l'insegnante a ripetere quello che ti sei perso.

3. L'Host, cioè colui che ti invita nella classe, è il tuo docente che ti conosce attraverso il tuo nome e

cognome, quindi non puoi accedere con i nickname che utilizzi per i giochi on line o per altri social network.

4. NO AGLI INTRUSI L'aula virtuale è la tua classe, quindi, come in classe non possono entrare estranei, anche qui non è possibile; evita quindi di dare il link della video-lezione

ad altri.

5. Il microfono va attivato solo quando te lo chiede l'insegnante dandoti la parola; la classe virtuale è uno spazio più ristretto dell'aula fisica, e la connessione, per quanto veloce, spesso rende meno chiara la conversazione, la sovrapposizione di voci, pertanto, crea molta confusione.

6. La webcam invece va attivata, in classe non entri mascherato, e neanche nella classe virtuale devi farlo. Se il tuo docente è disponibile ad organizzare la video lezione è perché è importante che si mantenga il contatto "visivo" seppur a distanza; il docente ha necessità di guardarvi, solo così può capire se quello che sta dicendo è compreso da tutti o se si deve fermare e ripetere.

7. PRIVACY/RESPONSABILITÀ/PENALI Ricorda che le lezioni on line sono protette dalla

privacy che significa che anche eventuali registrazioni o foto (autorizzate o meno) della lezione stessa NON POSSONO e NON DEVONO essere diffuse in alcun modo. I trasgressori potranno essere sanzionati e nei casi più gravi ci si rivolgerà alle autorità competenti sulla base della normativa vigente sul rispetto della privacy e sui fenomeni di cyberbullismo.

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.

Le infrazioni alla policy possono essere rilevate da docenti, ATA nell'esercizio delle loro funzioni oppure possono essere segnalate da alunni e genitori, a docenti e ATA, referente cyberbullismo, collaboratore del Dirigente Scolastico, nonché al Dirigente stesso. Qualora le infrazioni configurino un vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico affinchè vengano adottate le misure del caso.

Al personale e agli alunni saranno date tutte le informazioni relative alle infrazioni in uso e le eventuali sanzioni contenute nel Regolamento di Istituto o nel presente documento. Nel caso in cui le infrazioni della Policy violino norme previste dal Regolamento di Istituto si procede secondo quanto previsto dal Regolamento stesso.

Il Dirigente Scolastico ha la facoltà di revocare l'accessibilità temporanea o permanente ai laboratori informatici e/o all'utilizzo di strumenti tecnologici (pc, tablet, notebook, ecc …) a chi non si attiene

alle regole stabilite.

Il Regolamento di Istituto vieta, in tutti gli ambienti scolastici, l'uso dei telefoni cellulari non necessari al lavoro scolastico. I telefoni cellulari devono essere tenuti spenti nello zaino per tutto l'orario di permanenza a scuola e durante lo svolgimento delle attività didattiche all'esterno della scuola. È vietato fotografare o riprendere immagini all'interno dell'edificio scolastico se non previa autorizzazione dei docenti.

Si rinvia alle sezioni del presente documento per le infrazioni e relative sanzioni specifiche.

Rispondendo alla necessità di atti di indirizzo nascente dall'avvio della Didattica a Distanza, nella CIRCOLARE SUL CORRETTO UTILIZZO DELLE PIATTAFORME DIGITALI 16/04/2020, l'Istituto ribadisce che non è consentito diffondere il materiale pubblicato al di fuori del gruppo di classe a meno che non si abbia l'autorizzazione a farlo. I genitori e gli studenti si impegnano a non consentirne l'uso a qualsiasi titolo ad altre persone per accedere alla piattaforma e ad utilizzare i servizi offerti, solo ed esclusivamente per le attività didattiche. È vietata a tale proposito la condivisione di immagini, dati o materiali offensivi, osceni o comunque non attinenti all'attività didattica. Gli studenti e le studentesse si impegnano inoltre a non utilizzare la piattaforma in modo da danneggiare, molestare, insultare altre persone o intervenire con commenti inappropriati sia verso gli insegnanti sia verso i compagni o comunque comunicare dati personali senza l'autorizzazione dell'interessato. L'infrazione alle regole nell'uso della piattaforma informatica potrebbe comportare sanzioni disciplinari come da Regolamento dell'Istituto e nei casi più gravi ci si rivolgerà alle autorità competenti sulla base della normativa vigente sul rispetto della privacy e sui fenomeni di cyberbullismo. Lo Studente e la sua famiglia si assumono la piena responsabilità di tutti i dati da lui inoltrati, creati e gestiti attraverso la piattaforma.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

Il documento di e-policy viene reso pubblico sul sito web della scuola, così come qualsiasi modifica o integrazione del documento stesso, in relazione alla normativa vigente.

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.

È importante che venga nominato un referente che si occupi della realizzazione di ciò che è indicato nella Policy, attraverso monitoraggio e miglioramento. Il regolamento del laboratorio, così come indicato nel regolamento di Istituto, detta le norme di comportamento sull' utilizzo di internet e viene condiviso dagli alunni che sono informati sul fatto che internet è monitorato dal personale scolastico.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- 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 uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per la stesura finale dell'ePolicy.
- 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.

Le competenze digitali verranno promosse in modo trasversale da tutti i docenti in relazione alle loro pratiche e modalità di insegnamento.

La progettazione del curricolo sulle competenze verrà realizzata partendo dai seguenti documenti di riferimento:

Piano Scuola Digitale (PNSD); Sillabo sull'Educazione Civica Digitale; DigComp 2.1.(ll quadro di riferimento per le competenze digitali dei cittadini); Raccomandazione del Consiglio europeo relativa alle competenze chiave per l'apprendimento permanente (C189/9, p. 9).

l'Istituto si impegna, pertanto, a sviluppare una serie di competenze e comportamenti adeguati alle età degli alunni, tra cui:

- Conoscere il potenziale delle TIC, sapendo ricercare e filtrare dati e informazioni;
- sviluppare una serie di strategie per valutare e gestire dati, informazioni e contenuti digitali;
- riconoscere e sapersi difendere da contenuti dannosi e pericolosi in rete;

- capire come interagire con gli altri attraverso le tecnologie digitali;
- capire come collaborare adeguatamente con gli altri attraverso le tecnologie digitali;
- conoscere le “Netiquette”, ovvero le norme di comportamento online;
- acquisire e/o affinare capacità di pensiero critico e divergente al fine di creare conoscenze e contenuti nuovi, originali e rilevanti;
- capire come utilizzare e condividere informazioni personali proteggendo se stessi e gli altri dai danni.
- conoscere le misure di sicurezza e protezione e tenere in debita considerazione l’affidabilità e la privacy;
- proteggere i dati personali e la privacy negli ambienti digitali.

Al termine del primo ciclo di istruzione, le competenze verranno certificate sulla base dei seguenti profili:

Primaria: Usare con responsabilità le tecnologie in contesti comunicativi concreti per ricercare informazioni e per interagire con altre persone, come supporto alla creatività e alla soluzione di problemi semplici.

Secondaria: Utilizzare con consapevolezza e responsabilità le tecnologie per ricercare, produrre ed elaborare dati ed informazioni, per interagire con altre persone, come supporto alla creatività e alla soluzione di problemi.

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.

La professione docente, oggi più che mai, anche alla luce della nuova esigenza di sapersi destreggiare con la Didattica a Distanza, è molto complessa e richiede competenze diverse ed integrate, fra queste anche quelle di tipo digitale. Le TIC, infatti, possono essere usate dagli insegnanti ad integrazione della didattica al fine di progettare, sviluppare, utilizzare, gestire e valutare i processi di insegnamento e apprendimento, in chiave inclusiva, di tutti gli studenti e le studentesse della classe, anche di quelli con disabilità.

Di conseguenza, il nostro Istituto si pone l’obiettivo di portare gli insegnanti ad avere un buon livello

di formazione in merito all'utilizzo e l'integrazione delle TIC nella didattica, affinché si sappiano destreggiare, partendo dai compiti più semplici, per arrivare ai compiti complessi che presentano molti fattori di interazione. Con l'introduzione delle tecnologie digitali nel contesto scolastico si vuole raggiungere un obiettivo finale di grande importanza: apportare una revisione delle metodologie didattiche, a cui sta lavorando anche il Gruppo di Ricerca e Sperimentazione, passando da un approccio di tipo tradizionale ad uno di tipo costruttivista, in cui, cioè, il sapere non è inteso come qualcosa di statico e precostituito, ma come qualcosa che si crea grazie all'interazione tra soggetti e gruppi. L'asse didattico della nostra scuola vuole, infatti, occuparsi di educare ai media promuovendo una riflessione critica, ad esempio lavorando sulla decodifica dei messaggi e sulla conoscenza dei linguaggi mediali. Nello specifico l'offerta si articola in più azioni:

1. Percorsi di formazione per un uso consapevole delle TIC, tra cui anche l'uso del registro elettronico e delle piattaforme digitali utilizzate nella Didattica a Distanza, rivolti agli insegnanti;
2. Il Progetto "Ogni parola può trasformarsi in un pugno o in una carezza. TU PUOI SCEGLIERE. Anche la nostra Scuola dice NO al bullismo", rivolto agli studenti della scuola secondaria di primo grado;
3. Percorsi di educazione affettiva, con un approccio curricolare al Bullismo, rivolti agli alunni della scuola primaria;
4. Aggiornamento periodico di software antivirus installati nei vari PC presenti nelle aule multimediali;

Sulla base di questi presupposti, il nostro Collegio dei Docenti, riconosce e favorisce la partecipazione del personale a varie iniziative, sia promosse direttamente dalla scuola, anche con l'aiuto dell'animatore digitale, del team digitale, che è già formato al III livello, e delle Funzioni Strumentali che si occupano dell'area della formazione, sia quelle liberamente scelte dai docenti, anche online, purché restino coerenti con il piano di formazione, come meglio indicato nel PTOF.

Risulta fondamentale, quindi, che i docenti tutti prendano consapevolezza dell'importanza dell'uso delle TIC nella didattica: un loro utilizzo strutturato e integrato non solo può rendere gli apprendimenti motivanti, coinvolgenti ed inclusivi, ma permette al docente di guidare studenti e studentesse rispetto alla fruizione dei contenuti online, ormai la modalità naturale di apprendimento al di fuori della scuola. Inoltre, permettono di sviluppare capacità che sono sempre più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza e il confronto fra pari in modalità asincrona.

La competenza digitale, oggi, è imprescindibile per i docenti così come per studenti e studentesse e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa e in grado di venire incontro ai nuovi stili di apprendimento. Il nostro Istituto, dunque, direttamente, anche attraverso le reti di scuole, o indirettamente, offre agli insegnanti la possibilità di una formazione permanente, garantendosi, così, un personale docente con una buona base di competenze, in alcuni casi anche di carattere specialistico, che gli conferisce la capacità di saper cogliere tale sfida, in modo da rispondere in maniera pertinente ai diversi bisogni formativi della classe, anche con la Didattica a Distanza, che nel nostro Istituto ha coinvolto la totalità delle classi: su un totale di 72 classi, hanno utilizzato la piattaforma WeSchool 20 classi della Scuola secondaria di primo grado e 20 classi della Scuola Primaria; le altre classi hanno usato l'applicazione di

messaggistica WatsApp e l'applicazione web based Padlet.

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.

Per il prossimo anno scolastico, il nostro Istituto si ripropone di:

1. Approfondire l'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica;
2. Analizzare le richieste che provengono dagli studenti e dalle studentesse in modo, poi, da riutilizzarle nel lavoro di educatori (attraverso le modalità che il docente indica e ritiene più confacenti alla classe) secondo quanto appreso durante la formazione ricevuta;
3. Promuovere la partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse";
4. Monitorare le azioni svolte per mezzo di specifici momenti di valutazione;
5. Organizzare incontri con professionisti della scuola o con esperti esterni, enti/associazioni, etc;
6. Predisporre un'area specifica sul sito dell'Istituto con materiali formativi per gli insegnanti, con link e materiali informativi del progetto "Generazioni connesse", a partire dall'inserimento del link del progetto: www.generazioniconnesse.it/ dove trovare ulteriori approfondimenti, spunti aggiornamenti e strumenti didattici utili da usare con gli studenti e le studentesse, per ciascun grado di scuola.

Nello specifico l'Istituto si ripropone di offrire a tutti i docenti un percorso formativo specifico ed adeguato che abbia ad oggetto non solo l'uso responsabile e sicuro della Rete ma anche i rischi legati a quest'ultime. Ciò nell'ottica di creare ulteriore sinergia fra scuola, studenti/studentesse e famiglie, di promuovere la condivisione di buone pratiche nell'utilizzo consapevole delle TIC e di prevenire e contrastare ogni forma di discriminazione, offesa, denigrazione e lesione della dignità dell'altro, nonché fenomeni di bullismo e cyberbullismo.

Anche alla luce della nuova Didattica a Distanza, bisogna formare i docenti sull'uso delle TIC nella

didattica in modo che ciascun insegnante si sappia sganciare dalla mera all'alfabetizzazione ai media per arrivare a considerare la sfera emotiva e affettiva degli studenti e delle studentesse che usano le nuove tecnologie. Essi/e, infatti, comunicano, esprimono se stessi e sviluppano l'identità personale e sociale, attraverso i dispositivi tecnologici che sempre di più consentono loro di poter entrare in contatto con il mondo che li circonda. Durante i mesi del Lockdown le nuove tecnologie sono state davvero l'unica forma di contatto con il mondo per i nostri bambini/e e ragazzi/e. I docenti, quindi, non possono non prestare attenzione a questi aspetti e devono saper padroneggiare tutti gli strumenti necessari per poter educare ragazzi e ragazze alle emozioni in contesto onlife, un neologismo a cui il mondo, compreso il mondo della scuola, ha dovuto abituarsi, soprattutto in questi ultimi mesi, contrazione di "online" e "offline", usato per descrivere l'esperienza che si vive in un mondo iper-connesso, dove non esiste più la distinzione tra essere online o essere offline.

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.

Gli studenti e le studentesse devono attenersi a quanto previsto dai Regolamenti Scolastici e dalle Circolari interne emanate dal Dirigente Scolastico, sulla base delle Note ministeriali, circa l'utilizzo consapevole delle tecnologie digitali all'interno del contesto scolastico.

I genitori, nell'azione di corresponsabilità didattico-educativa, rappresentano un punto di forza per l'implementazione dei rapporti "scuola-famiglia", quale garanzia e rispetto degli impegni sottoscritti e condivisi nello stesso Patto di Corresponsabilità, di natura anche pedagogica.

Il nostro piano d'azioni

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

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- 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.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.

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

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- 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.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'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'Istituto Comprensivo "F. Collecini Giovanni XXIII" di S. Leucio (CE) rispetta la privacy dei propri utenti e si impegna a proteggere i dati personali che gli stessi conferiscono all'I.C. stesso. Il Responsabile della protezione dei dati designato ai sensi dell'art. 37 del Regolamento UE 2016/679 ("GDPR") è il professionista indicato nell'apposita sezione del sito della scuola. Ai sensi dell'art. 38 comma 4 del GDPR, gli interessati (dipendenti, alunni, genitori, utenti del sito web, etc.) possono contattare senza formalità il Responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti. La raccolta ed il trattamento di dati personali avvengono, quando necessari, in relazione all'esecuzione di servizi richiesti dall'utente, o quando l'utente stesso decide di comunicare i propri dati personali; in tali circostanze, la presente politica della privacy illustra le modalità ed i caratteri di raccolta e trattamento dei dati personali dell'utente. L'Istituto tratta i dati personali forniti dagli utenti in conformità alla normativa vigente. In caso di raccolta di dati personali, l'I.C. "F. Collecini" informerà l'utente sulle finalità della raccolta al momento della stessa, ove necessario, richiederà il consenso dell'utente. L'Istituto non comunicherà i dati personali dell'utente a terzi senza il consenso dello stesso. Se l'utente decide di fornire alla scuola i propri dati personali, la scuola potrà comunicarli all'interno dell'Istituto od a terzi che prestano servizi alla scuola, solo rispetto a coloro che hanno bisogno di conoscerli in ragione delle proprie mansioni, e, ove necessario, con il permesso dell'utente. La scuola tratta i dati personali dell'utente per le seguenti finalità di carattere generale: per soddisfare le richieste a specifici prodotti o servizi, per personalizzare la visita dell'utente al sito, per aggiornare l'utente sulle ultime novità in relazione ai servizi offerti od altre informazioni che ritiene siano di interesse dell'utente che provengono direttamente dall'Istituto o dai suoi partners, e per comprendere meglio i bisogni dell'utente ed offrire allo stesso servizi migliori. Il trattamento di dati personali dell'utente da parte dell'Istituto per le finalità sopra specificate avviene in conformità alla normativa vigente a tutela dei dati personali. Si possono individuare al riguardo alcune linee guida di e-safety:

-Non violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione. Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su Internet, e sui social network in particolare. In caso di comunicazione sistematica o diffusione diventa infatti necessario, di regola, ottenere il consenso informato delle persone presenti nelle fotografie e nei video.

-Si deve quindi prestare particolare attenzione prima di caricare immagini e video su blog o social network, oppure di diffonderle attraverso sistemi di messaggistica istantanea. Succede spesso, tra l'altro, che una fotografia inviata a un amico o a un familiare venga poi inoltrata ad altri destinatari, generando involontariamente una comunicazione a catena dei dati personali raccolti. Tale pratica può dar luogo a gravi violazioni del diritto alla riservatezza delle persone riprese, e fare incorrere in sanzioni disciplinari, pecuniarie e in eventuali reati.

-L'utilizzo di telefoni cellulari, di apparecchi per la registrazione di suoni e immagini, quando autorizzato dai docenti, è consentito, ma esclusivamente per fini personali, e sempre nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte (siano essi studenti o professori) in particolare della loro immagine e dignità.

-Le istituzioni scolastiche hanno, comunque, la possibilità di regolare o di inibire l'utilizzo di registratori, smartphone, tablet e altri dispositivi elettronici all'interno delle aule o nelle scuole stesse. Gli studenti e gli altri membri della comunità scolastica, in ogni caso, non possono diffondere o comunicare sistematicamente i dati di altre persone (ad esempio pubblicandoli su Internet) senza averle prima informate adeguatamente e averne ottenuto l'esplicito consenso

-È consigliabile utilizzare canali istituzionali per comunicazioni a scopo didattico con le famiglie e gli studenti

-Come e-mail si utilizzerà quella istituzionale della scuola per averne tracciabilità della conversazione in un luogo protetto.

-Le fotografie o i video da pubblicare sul sito che includano allieve e allievi saranno selezionati con cura e non permetteranno a singoli di essere chiaramente identificati a meno che non si tratti di eventi particolari per cui le famiglie potranno concedere opportuna autorizzazione. La scuola cercherà di utilizzare fotografie o video di gruppo piuttosto che foto integrali di singoli.

-L'Istituto tratta i dati personali forniti dagli utenti in conformità alla normativa vigente. All'inizio del ciclo di istruzione 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. La modulistica per il consenso informato e tutte le circolari riguardanti il trattamento dei dati personali sono scaricabili sul sito web della scuola (http://www.collecini.edu.it) nella sezione Privacy.

-Ogni caso particolare sarà preso in considerazione per stabilire l'opportunità di pubblicare dati personali e sarà presentata apposita richiesta circostanziata che varrà solo per lo specifico evento.

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 ad internet è garantito in tutte le aule (rete Wi-Fi) e nel laboratorio di informatica (rete LAN), compatibilmente con l'infrastruttura presente sul territorio. L'utilizzo di internet nelle aule è regolamentato dai docenti che detengono, in via esclusiva, la password per l'accesso alla wi-fi. gli alunni possono collegarsi ad internet dai pc e notebook del laboratorio di informatica, la navigazione è guidata dai docenti. Si intende dotare la scuola di antivirus e di filtri di sicurezza per la navigazione di internet. La connessione alla rete wi-fi è riservata ai docenti per fini didattici ed è accessibile solo con l'inserimento di password. I computer del laboratorio di informatica hanno un nome utente identificativo. Solo le aule attrezzate con LIM sono dotate di pc portatili, accessibili da parte dei docenti, connessi alla rete wi-fi.

Accesso docenti

L'Istituto attualmente è dotato di una rete wireless destinata all' utilizzo didattico da parte del corpo docente. La password è unica a livello di Istituto/plesso. Ai docenti è consentito accedere ad Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto. Ciascun utente connesso alla rete dovrà rispettare la legislazione vigente, tutelare la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui ha accesso e rispettare la cosiddetta netiquette (insieme di regole, comunemente accettate e seguite da quanti utilizzano Internet e i servizi di rete, che disciplinano il comportamento di un utente nel rapportarsi agli altri utenti attraverso risorse come wiki, newsgroup, mailing list, forum, blog o e-mail).La componente studentesca dovrà impegnarsi a rispettare le norme di buon utilizzo che la scuola ha elencato nel presente documento. I computer portatile presenti nelle aule richiedono una password di accesso per l'accensione. Ogni docente è quindi tenuto ad un controllo della strumentazione in aula poiché l'uso del dispositivo è permesso agli alunni solo su autorizzazione dell'insegnante. Ogni docente accede al registro elettronico attraverso una password che non può essere comunicata a terzi, né agli alunni.

Accesso studenti

Il Regolamento di Istituto vieta l'uso del cellulare.

In particolare, agli studenti non è consentito accedere ad Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto. Durante l'orario scolastico agli alunni non è permesso l'utilizzo della telefonia mobile; è altresì vietato l'uso per scopo personale di tutti gli altri strumenti informatici di proprietà e non dello studente. L'eventuale utilizzo di strumenti informatici di proprietà dello studente durante l'attività didattica deve essere autorizzata dal docente. Relativamente agli alunni che accedono a Internet durante l'attività didattica sono consentiti la navigazione guidata da parte dell'insegnante e la stesura di documenti collaborativi purché sotto il controllo dell'insegnante e nel caso in cui tale attività faccia parte di un progetto di lavoro precedentemente autorizzato. È vietato l'accesso alle chat-room pubbliche o non moderate. La trasgressione a queste regole avranno sanzione decisa dal Dirigente e dal CdC secondo le presenti norme e in accordo al Regolamento di Istituto.

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 dell'Istituto Comprensivo è http://www.collecini.edu.it.Responsabile della gestione del sito è la funzione strumentale AREA 6 "Comunicazione web". L'Istituto ha creato una pagina Facebook con il proprio profilo. La gestione è affidata alla Funzione Strumentale AREA 6 " Comunicazione web".

Sito web della scuola

Il Dirigente Scolastico e il personale incaricato di gestire le pagine del sito della Scuola hanno la responsabilità di garantire che il contenuto pubblicato sia accurato e appropriato. La scuola offre all'interno del proprio sito una serie di servizi alle famiglie e ai fruitori esterni. Il personale che è in possesso delle credenziali per la gestione dei contenuti sul portale si assumerà la responsabilità editoriale di garantire che il contenuto inserito sia accurato e appropriato.

Social network per alunni, docenti e genitori.

Per la Legge l'utilizzo dei Social Network con la pubblicazione di nomi e giudizi sulle persone o sulle istituzioni e la diffusione di foto/filmati senza il consenso e, comunque, all'insaputa delle persone coinvolte può determinare ricadute di carattere anche penale, come ad esempio la diffamazione. Pertanto, tutti gli studenti sono tenuti a non prelevare o diffondere immagini, video o registrazioni – anche solo audio – non autorizzate e ad eliminare da internet eventuali riferimenti offensivi o

comunque illeciti (ed inopportuni) nei confronti dell'Istituto e dei suoi docenti e studenti. Allo stesso tempo, gli allievi e i genitori sono tenuti ad utilizzare in modo prudente i Social Network, in particolare Facebook e Whatsapp, limitandone l'uso alle sole comunicazioni funzionali, evitando ad ogni modo di esprimere giudizi sull'operato degli altri studenti o del personale della scuola, giudizi che una volta pubblicati comportano sempre una assunzione di responsabilità da parte di chi li ha scritti o anche semplicemente diffusi. Nella pratica didattica si cercherà di educare la componente studentesca al loro uso sicuro.

Registro elettronico

Ogni famiglia riceve le credenziali per l'accesso riservato al registro elettronico, in cui il corpo docente è tenuto a registrare assenze, valutazioni, note e osservazioni. La pubblicazione delle informazioni attraverso tale strumento assolve l'obbligo di comunicare prontamente ed efficacemente ogni evento riguardante l'alunno/a. Coloro che non possono accedere a Internet e di conseguenza non possono consultare il registro elettronico sono pregati di darne segnalazione al coordinatore del consiglio di classe, che verificherà la trascrizione delle comunicazioni sul diario e la firma dei genitori.

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.

(Durante l'orario scolastico, smartphone, tablet, pc portatili)

Per la componente studentesca

Gli studenti non possono utilizzare i propri dispositivi durante le attività didattiche come previsto dal regolamento di istituto, né possono accedere alla rete attraverso i dispositivi della scuola se non con autorizzazione dell'insegnante presente in aula e comunque per ricerche attinenti le attività

didattiche.

L'utilizzo in classe da parte degli studenti della scuola secondaria di dispositivi digitali personali (notebook portatili, tablet) in modalità BYOD (Bring Your Own Device) può essere consentito dal docente, durante lo svolgimento delle attività didattiche, dopo il rilascio di una autorizzazione in cui i genitori dichiarano di essere a conoscenza dell'utilizzo in classe dei dispositivi personali e si impegnano, con i docenti, nel responsabilizzare i propri figli/figlie sulle regole di utilizzo a cui attenersi.

Nella scuola primaria si chiede alle famiglie di non lasciare tali dispositivi ad alunne e alunni. Discenti con disturbi specifici di apprendimento o altre disabilità certificate, previa consultazione con il Consiglio di Classe, concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili e le modalità di custodia. Nel caso in cui debbano comunicare con la famiglia durante l'orario scolastico, alunne e alunni possono usare gratuitamente la linea fissa della scuola rivolgendosi a un operatore; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di parlare con i propri figli. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza. Salvo casi del tutto eccezionali, i telefoni cellulari non devono essere portati a scuola e non devono comunque essere utilizzati durante l'orario scolastico. Se – malgrado il divieto appena espresso – gli studenti verranno sorpresi ad usare il cellulare, verrà chiesto dal docente di porlo temporaneamente nel cassetto della cattedra, fino al termine delle lezioni dai docenti e poi restituito alla famiglia convocata o, in mancanza di questa, al ragazzo stesso. Verrà immediatamente comunicato l'accaduto al Dirigente e/o al suo primo collaboratore. Si convocheranno per vie brevi i genitori interessati ai quali verrà, possibilmente, riconsegnato il cellulare. Avuto inoltre riguardo per il fatto che gli smartphone possono essere utilizzati anche per scattare foto (o effettuare riprese filmate) e divulgarle, si informano i Sigg. genitori che eventi di questo tipo – se si concretizzano durante l'orario scolastico si possono configurare anche come reati per i quali non si esclude la segnalazione ai competenti organi di Pubblica Sicurezza. In particolare, a riguardo di un uso scorretto dello smartphone, si ricorda che:

a) La scuola non pone alcun ostacolo all'utilizzo di cd/dvd rom o di hard - disk portatili come strumenti di lavoro e di studio. Ciò che a riguardo compete alle famiglie è il controllo periodico del contenuto di questi strumenti per evitare che qualche studente divulghi a scuola immagini / testi filmati per così dire 'sconvenienti', avendoli scaricati (magari solo per curiosità).

b) Fermo restando il fatto che la scuola è un'istituzione educativa e che non è né prevista, né possibile, né tantomeno legittima la perquisizione quotidiana di tutti gli studenti all'inizio di ogni giorno di lezione, le responsabilità che dovessero derivare dal verificarsi di eventi riconducibili all'uso non corretto o non legittimo di uno qualsiasi degli oggetti di cui alla presente norma regolamentare sono tutte ascrivibili alle famiglie degli studenti eventualmente coinvolti.

c) Le responsabilità appena menzionate sono condivise dal personale scolastico solo quando e solo se ,avendo personalmente constatato o essendo venuto a conoscenza che qualche ragazzo/a fa uso di un device (smartphone o tablet) durante l'orario scolastico e lo utilizza in modo scorretto e contro il regolamento di istituto non dovesse immediatamente intervenire nelle forme già indicate e comunque in modo tale da prevenire o reprimere sul nascere situazioni incompatibili con le più elementari regole della civile convivenza.

Per la componente personale scolastico docenti/ata

I docenti possono utilizzare i dispositivi della scuola per realizzare tutte le attività connesse alla funzione docente. E' consentito per i docenti l'uso dei propri dispositivi in classe per quanto attiene l'attività didattica qualora siano necessari, ma non possono essere utilizzati durante le lezioni per questioni personali. Il personale preferirà, quando ciò è possibile, l'impiego della strumentazione fornita dalla scuola rispetto a quella personale (portatili, pc fissi, ...); le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali. Telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non all'interno di attività didattiche programmate. L'uso improprio della rete è contestato al titolare delle credenziali con cui è avvenuta la comunicazione. Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni. Durante l'attività didattica è opportuno che ogni insegnante: - dia chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti ecc.), condividendo con gli studenti la netiquette e indicandone le regole; - si assuma la responsabilità di segnalare prontamente eventuali malfunzionamenti o danneggiamenti al tecnico informatico; - non salvi sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili e proponga agli alunni attività di ricerca di informazioni in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento.

Il nostro piano d'azioni

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

- 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).

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

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.*

La sensibilizzazione può costituire il primo passo verso un cambiamento positivo, ma per far sì che l'intervento sia efficace, è importante che sia chiara l'azione verso cui i soggetti devono impegnarsi.

Due sono gli aspetti che bisogna tenere in considerazione:

- la consapevolezza dello status quo;
- la motivazione al cambiamento.

Per far sì che un intervento di sensibilizzazione sia efficace, è quindi importante fornire ai beneficiari informazioni chiare su quello che è lo stato attuale del tema che vogliamo trattare (ad es.

se si vuol trattare il tema del Cyberbullismo, sarà opportuno fornire informazioni su quali sono le caratteristiche del fenomeno e i dati rappresentativi).

Parlare di prevenzione in ambito digitale significa mettere in atto un insieme di attività, azioni ed interventi finalizzati a 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.

Si distinguono tre livelli di prevenzione:

- Prevenzione Universale. Un programma di questo tipo parte dal presupposto che tutti gli studenti siano potenzialmente a rischio. Si tratta quindi di interventi diretti al grande pubblico o a un intero gruppo di una popolazione che non è stato identificato sulla base del rischio individuale. Efficacia: trattandosi di programmi ad ampio raggio gli effetti di questi programmi possono essere modesti se confrontati con programmi che "trattano" un gruppo con un problema specifico. Tuttavia, questi interventi possono produrre cambiamenti in grandi popolazioni (ad es. si pensi ad un programma dedicato alle competenze emotive, oppure alla cittadinanza digitale).
- Prevenzione Selettiva. Un programma dedicato ad un gruppo di studenti in cui il rischio online è presente. In questo caso la presenza del rischio è stata individuata tramite precedenti indagini, segnalazioni fatte dalla scuola, oppure dalla conoscenza della presenza di fattori di rischio in quel determinato territorio. In questi casi gli interventi sono mirati e prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem solving. Può essere un valido programma se si osservano casi in cui la prevenzione universale non ha dato gli esiti previsti.
- Prevenzione Indicata. Un programma di intervento sul caso specifico, è quindi pensato e strutturato per adattarsi agli/lle studenti/studentesse con l'obiettivo di ridurre i comportamenti problematici, oppure dare supporto alle vittime. Per la sua natura questo tipo di intervento si avvale di professionalità diverse perché spesso affronta problemi legati alla salute mentale del minore per cui è opportuno coinvolgere anche la famiglia del/lla ragazzo/a.

Le dimensioni che il fenomeno coinvolge sono molteplici e non puramente tecniche e si rifanno alla capacità dei più giovani di gestire situazioni complesse che richiedono: la capacità di gestire la relazione con l'altro/a diverso/a da sé, le dimensioni dell'affettività e della sessualità, il riconoscimento di un limite, anche, ma non solo, legato ad una dimensione di legalità, l'utilizzo sicuro e consapevole delle tecnologie digitali.

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).

Rispetto al bullismo tradizionale, il ricorso ai mezzi tecnologici conferisce al cyberbullismo caratteristiche proprie:

- anonimato del bullo anche se si tratta di un anonimato illusorio perché ogni intervento su internet è tracciabile.
- indebolimento delle remore morali dovuto dalla convinzione di non essere visti
- assenza di limiti spazio-temporali perché gli episodi non sono circoscritti ad un ambiente particolare come la scuola, ma coinvolgono la vittima ogni volta che si collega ad internet
- impatto incontrollabile : i contenuti offensivi e denigratori restano on line e si diffondono senza limiti
- feedback non tangibile: il cyberbullo non assiste in diretta alle reazioni della vittima e ciò riduce fortemente l'empatia e il riconoscimento del danno provocato.

È possibile suddividere gli atti di cyberbullismo in due grandi gruppi:

- cyberbullismo diretto: il bullo utilizza strumenti di messaggistica istantanea (es. sms, mms) che hanno un effetto immediato sulla vittima, poiché diretti esclusivamente a lei.
- cyberbullismo indiretto: il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico.

È molto importante sottolineare come il cyberbullismo non sia una problematica che riguarda unicamente vittima e cyberbullo. È un fenomeno sociale e di gruppo. Infatti, centrale è il ruolo delle agenzie educative e di socializzazione (formali e informali) più importanti per gli adolescenti: la famiglia, la scuola, i media, le tecnologie digitali e il gruppo dei pari.

Di seguito, alcuni segnali generali che può manifestare la potenziale vittima di cyberbullismo:

- Appare nervosa quando riceve un messaggio o una notifica;
- Sembra a disagio nell'andare a scuola o finge di essere malata (ha spesso mal di stomaco o mal di testa);
- Cambia comportamento ed atteggiamento in modo repentino;
- Mostra ritrosia nel dare informazioni su ciò che fa online;
- Soprattutto dopo essere stata online, mostra rabbia o si sente depressa;
- Inizia ad utilizzare sempre meno Pc e telefono (arrivando ad evitarli);
- Perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;
- Il suo rendimento scolastico peggiora.

.

Chi compie atti di bullismo e cyberbullismo può anche essere responsabile di reati penali e danni civili.

I ragazzi e le ragazze che fanno azioni di bullismo possono commettere reati. Secondo il codice penale italiano i comportamenti penalmente rilevanti in questi casi sono:

- percosse (art. 581),
- lesione personale (art. 582),
- ingiuria (art. 594),
- diffamazione (art. 595),
- violenza privata (art. 610),
- minaccia (art. 612),
- danneggiamento (art. 635).

Per il nostro ordinamento l'imputabilità penale (ossia la responsabilità personale per i reati commessi) scatta al quattordicesimo anno.

Negli atti di Bullismo vanno distinte le diverse responsabilità ed a tal riguardo si identificano:

a. Culpa del bullo minore:

- che abbia almeno compiuto 14 anni;
- che, comunque, anche se maggiore di 14 anni, fosse cosciente e volente al momento del comportamento, cioè in grado di intendere e volere (tale non sarebbe, per esempio, un ragazzo con degli handicap psichici).

b. Culpa in vigilando dei genitori:

- i genitori, perché devono educare adeguatamente e vigilare, in maniera adeguata all'età del figlio, cercando di correggerne comportamenti devianti. Questa responsabilità generale persiste anche per gli atti compiuti nei tempi di affidamento alla scuola (culpa in educando).

c. Culpa in vigilando (ma anche in educando ed in organizzando della Scuola):

- gli insegnanti e la scuola: perché nei periodi in cui il minore viene affidato all'Istituzione scolastica il docente è responsabile della vigilanza sulle sue azioni e ha il dovere di impedire comportamenti dannosi verso gli altri/e ragazzi/e, insegnanti e personale scolastico o verso le strutture della scuola stessa. A pagare in primis sarà la scuola, che poi potrà rivalersi sul singolo insegnante. La responsabilità si estende anche a viaggi, gite scolastiche, manifestazioni sportive organizzate dalla scuola (culpa in vigilando). In questi casi interviene l'art. 2048 del Codice Civile (responsabilità dei precettori) e l'art. 61 della L. 312/1980 n. 312 (responsabilità patrimoniale del personale direttivo, docente educativo e non docente).
- esiste poi una culpa in organizzando, che si ha quando la scuola non mette in atto le azioni previste per la prevenzione del fenomeno o per affrontarlo al meglio (così come previsto anche dalla normativa vigente).

Nei casi più gravi, basta la denuncia ad un organo di polizia o all'autorità giudiziaria per attivare un procedimento penale (per es. lesioni gravi, minaccia grave, molestie); negli altri casi, la denuncia deve contenere la richiesta che si proceda penalmente contro l'autore di reato (querela).

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.

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?

La tecnologia ha modificato gli ambienti che viviamo e ha un impatto sulla qualità della vita. La scuola può insegnare molto da questo punto di vista se integra la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online poiché se si controlla la tecnologia se ne può usare il pieno potenziale e trarne vantaggi: strutturare regole condivise e stipulare con loro una sorta di "patto" d'aula proponendo delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d'aula (Es. adoperando la LIM o il dispositivo personale). È importante, quindi, non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli/lle studenti e delle studentesse, stabilendo chiare e semplici regole di utilizzo.

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.

I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di "revenge porn" letteralmente "vendetta porno" fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare

l'altra parte (la Legge 19 luglio 2019 n. 69, all'articolo 10 ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti.

Tra le caratteristiche del fenomeno vi sono principalmente:

- la fiducia tradita: chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale);
- la pervasività con cui si diffondono i contenuti: in pochi istanti e attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e infinito di persone e ad altrettante piattaforme differenti. Il contenuto, così, diventa facilmente modificabile, scaricabile e condivisibile e la sua trasmissione è incontrollabile;
- la persistenza del fenomeno: il materiale pubblicato online può permanervi per un tempo illimitato e potrebbe non essere mai definitivamente rimosso. Un contenuto ricevuto, infatti, può essere salvato, a sua volta re-inoltrato oppure condiviso su piattaforme diverse da quelle originarie e/o in epoche successive.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione.

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.

L'adescamento non avviene apparentemente con una dinamica violenta, ma il "prendersi cura" del minore rappresenta la conditio per carpirne la fiducia ed instaurare una relazione a sfondo erotico. In tal senso è utile conoscerne la fasi attraverso le quali si attua:

- Fase dell'amicizia iniziale: Questa è la fase in cui l'adescatore cerca i primi contatti con la vittima individuata, provando a socializzare con lei. Tenterà, quindi, di conoscerla meglio al fine di scoprirne bisogni, interessi e il contesto in cui vive. Condividendo argomenti di interesse del minore l'adescatore cercherà pian piano di conquistarsi la sua fiducia, ponendogli domande frequenti che attestano interesse e attenzione nei suoi confronti. Gradualmente affronterà con la vittima argomenti sempre più privati ed intimi.
- Fase di risk-assessment: in seguito ai primi contatti con il minore, l'adescatore cerca di comprendere il contesto in cui si svolge l'interazione (es. da dove si collega alla Rete? I genitori lo controllano quando chatta? Che rapporto ha con loro?). L'obiettivo dell'adescatore è quello di rendere sempre più privato ed "esclusivo" il rapporto, cercando di passare, ad esempio, da una chat pubblica ad una privata, da una chat alle conversazioni attraverso il telefono, per poterne così carpire il numero.
- Fase della costruzione del rapporto di fiducia: le confidenze e le tematiche affrontate divengono via via più private ed intime o comunque molto personali. In questa fase l'adescatore può iniziare a fare regali di vario tipo alla vittima e può anche avvenire lo scambio di foto, subito e non necessariamente a sfondo sessuale.
- Fase dell'esclusività: l'adescatore rende la relazione con il minore sempre più "segreta", isolandolo sempre più dalla famiglia e dagli amici. Chiederà alla vittima di non raccontare a nessuno ciò che sta vivendo. L'esperienza reciproca verrà presentata come un "geloso segreto" da custodire per non rovinare tutto. In questa fase l'adescatore potrà ricorrere a ricatti morali puntando sulla fiducia costruita, sulla paura o sul senso di colpa.
- Fase della relazione sessualizzata: in questa fase la richiesta di immagini o video sempre più privati e a sfondo erotico potrebbe essere più insistente, così come la proposta di incontri offline. Qualora il minore avesse già inviato immagini o video privati, potrebbe essere ricattato dall'adescatore: se non accettasse un eventuale incontro l'adescatore potrebbe diffondere quel materiale online. Questi, inoltre, tenderà a presentare sempre la situazione come "normale" al fine di vincere le eventuali resistenze del minore a coinvolgersi in tale rapporto.

Per riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli segnali che possono essere indicatori importanti, come ad esempio un cambiamento improvviso nel comportamento di un minore. A seguire, alcuni segnali e domande che potrebbero esserci di aiuto:

- Il minore ha conoscenze sessuali non adeguate alla sua età?
- Venite a conoscenza di un certo video o di una foto che circola online o che il minore ha ricevuto o filmato, ma c'è imbarazzo e preoccupazione nel raccontarvi di più…
- Il minore si isola totalmente e sembra preso solo da una relazione online?
- Ci sono prese in giro e allusioni sessuali verso un bambino/ragazzo in particolare?

Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad esempio, all'adescatore. È importante che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove.

Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video…).

L'adescamento, inoltre, può essere una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.

I minori vittime di adescamento riferiscono, generalmente, di sentirsi traditi, ma anche di provare un senso di colpa per essere caduti in trappola ed essersi fidati di uno sconosciuto.

Inutile sottolineare che nei casi più estremi in cui l'adescamento porta ad un incontro fisico e ad un abuso sessuale un sostegno psicologico esperto per il minore è da considerarsi prioritario e urgente.

Per consigli e per un supporto è possibile rivolgersi alla Helpline di Generazioni Connesse (19696): operatori esperti e preparati sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che dei bambini, degli adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti l'utilizzo dei nuovi media.

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.

L'abuso sessuale online rappresenta una particolare declinazione dell'abuso sessuale su bambini/e, ragazzi/e, la cui caratteristica fondante è il ruolo ricoperto dalle tecnologie digitali, le quali diventano il mezzo principale attraverso cui l'abuso viene perpetrato, documentato e diffuso in Rete con immagini e/o video. Le dinamiche attraverso cui l'abuso sessuale online si manifesta producono effetti sulle vittime che si aggiungono e moltiplicano a quelli associati all'abuso sessuale. Si pensi, a titolo di esempio, all'impatto che può avere la consapevolezza dell'esistenza (spesso anche in Rete) delle immagini e/o video dell'abuso sulla vittima, o a come gestire le stesse immagini e/o video durante la fase investigativa e giudiziaria. L'esposizione alle immagini dell'abuso, infatti, sia durante il processo giudiziario, sia durante il percorso di cura, deve essere attentamente valutata, poiché può comportare, per il/la minore coinvolto/a, un rischio di vittimizzazione secondaria.

Se si ravvisa un rischio per il benessere psicofisico dei/lle bambini/e, ragazzi/e coinvolte nella visione di questi contenuti sarà opportuno ricorrere, come previsto nel protocollo di emergenza, a 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.

Il nostro piano d'azioni

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

☐Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

☐ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.

☐ Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli 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

☐ Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

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

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

☐ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.

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.

Le procedure indicate in questa sezione si riferiscono, oltre a quelle sopra indicate, legate ad un utilizzo scorretto delle TIC (Tecnologie dell'Informazione e della Comunicazione), anche a tutte le azioni da mettere in pratica per la presa in carico e relativa gestione delle situazioni di bullismo.

IL TEAM DELL'EMERGENZA

Con apposito atto di nomina, il Dirigente Scolastico individua un gruppo o team specializzato con competenze, responsabilità, tempi e modalità d'azione specifiche, per la gestione dei casi.

Il team sarà coordinato dal referente per il contrasto del bullismo e del cyberbullismo.

Il team è composto da 3 o più persone, tra insegnanti con competenze trasversali e figure professionali diverse che lavorano nella scuola (psicologo o psicopedagogista), formate sul tema delle azioni indicate contro il bullismo/cyberbullismo.

Il Team per le emergenze, osservando quanto descritto nel Capitolo 1 del presente documento in quanto a ruoli e responsabilità, agisce in quanto a:

- responsabilità della presa in carico
- conduzione della valutazione
- responsabilità della decisione relativa alla tipologia di intervento
- implementare alcuni interventi
- monitoraggio del caso nel tempo
- responsabilità della decisione relativa all'andamento del caso nel tempo
- stretta connessione con i servizi del territorio

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.

PROTOCOLLO DI GESTIONE DELL'EMERGENZA

L'Istituto, oltre al dovere di sorveglianza degli insegnanti (culpa in vigilando) adotta il presente Protocollo di Gestione dell'emergenza che, accogliendo gli strumenti di segnalazione sopra indicati, definisce le procedure da seguire una volta che è avvenuto un presunto episodio di bullismo/cyberbullismo e vittimizzazione e prevede 4 passi fondamentali:

1. Prima segnalazione
2. Valutazione approfondita
3. Scelta dell'intervento e della gestione del caso
4. Monitoraggio

Lo schema allegato "Procedura per caso presunto bullismo e vittimizzazione a scuola" rappresenta graficamente il Protocollo di gestione dell'emergenza.

Il Protocollo di Gestione dell'emergenza comprende, in quanto azioni propedeutiche alla redazione della SCHEDA DI PRIMA SEGNALAZIONE, gli schemi allegati al presente capitolo e che rappresentano rispettivamente:

- Procedure interne in caso di Cyberbullismo
- Procedure interne in caso di Sexting
- Procedure interne in caso di adescamento on line
- Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola.

FASE 1 – ACCOGLIERE LA SEGNALAZIONE DI UN CASO PRESUNTO DI BULLISMO

Lo scopo di questa fase è quella di attivare un processo di attenzione e di successive valutazioni relative ad un presunto caso di bullismo/cyberbullismo.

La segnalazione può farla chiunque: vittima, genitori, testimoni, docenti, personale ATA. Accogliere la segnalazione non significa denunciare bensì prendere in carico una situazione che necessita di approfondimenti ed escludere che un caso di sofferenza non venga considerato perché sottovalutato o ritenuto di poca importanza.

Viene redatta utilizzando l'apposito modulo "SCHEDA DI PRIMA SEGNALAZIONE". La scheda, elaborata in modo semplice e funzionale alla raccolta di dati essenziali, sarà diffusa in modalità cartacea nei luoghi a cui hanno accesso tutti coloro che possano avere necessità di compilarla. Sarà altresì disponibile in modalità digitale nell'apposita sezione sul sito istituzionale dell'Istituto.

Uno o più componenti, appositamente designati, del team d'emergenza, raccolgono le schede di prima segnalazione per attivarne la relativa gestione e monitoraggio.

FASE 2 – VALUTAZIONE APPROFONDITA

Lo scopo di questa fase è valutare esattamente la tipologia e la gravità dei fatti per poter definire un intervento. Viene condotta dal team dell'emergenza insieme a chi ha fatto la prima segnalazione. E' importante che questa fase venga attivata entro almeno 2 giorni da quando è stata presentata la prima segnalazione affinché con l'acquisizione di ulteriori informazioni si possano prendere decisioni circa le modalità di gestione del caso. Il componente del team che prenderà in carico il caso, attraverso degli incontri e dei colloqui appositamente strutturati, redigerà lo screening utilizzando il modulo "VALUTAZIONE APPROFONDITA DEI CASI DI BULLISMO E VITTIMIZZAZIONE"

FASE 3 – GESTIONE DEL CASO

In base alle informazioni acquisite si delinea il LIVELLOD DI RISCHIO DI BULLISMO E VITTIMIZZAZIONE con conseguente grado di priorità dell'intervento:

- Livello CODICE VERDE = Situazione da monitorare con interventi preventivi nella classe
- Livello CODICE GIALLO = Interventi indicati e strutturati a scuola e in sequenza coinvolgimento della rete se non ci sono risultati
- LIVELLO CODICE ROSSO = Interventi di emergenza con supporto della rete

In base al livello verranno poi delineate le azioni da intraprendere e, il team dell'emergenza, ha il compito di coinvolgere le altre figure che supporteranno la realizzazione dell'intervento/degli interventi (es. i docenti della classe per l'intervento educativo con la classe).

Gli interventi sono di seguito classificati:

1. Approccio educativo con la classe, in cui vengono coinvolti gli insegnanti della classe per

affrontare direttamente l'accaduto e sensibilizzare rispetto al fenomeno generale
2. Intervento individuale, con il bullo e la vittima, in cui è richiesto il supporto di un docente con competenze trasversali e, ove possibile, del psicologo della scuola
3. Gestione della relazione, secondo l'approccio della Mediazione o dell'Interesse condiviso, a seconda del caso da trattare
4. Coinvolgimento della famiglia, che può essere realizzato anche in momenti diversi in funzione della specifica situazione, delle indicazioni del DS, dell'obiettivo del team, o del docente referente della scuola e delle capacità di quest'ultima di poter avviare una prima gestione del caso. Se i genitori sono coinvolti nella fase di valutazione iniziale o hanno segnalato loro stessi il problema, è importante impostare fin da subito una collaborazione attiva tra scuola e famiglia per la soluzione del caso.

L'art. 5 della L.71/2017 sancisce precise circostanze in presenza delle quali il DS provvede a informare la famiglia.

5. Supporto intensivo a lungo termine e di rete, da richiedere nel caso in cui

- gli atti di bullismo siano di una gravità elevata
- la sofferenza della vittima è molto elevata
- i comportamenti aggressivi e a rischio dei bulli sono considerevoli

Va evidenziato che gli insegnanti, in quanto incaricati di pubblico servizio, hanno obbligo di denuncia qualora vengano a conoscenza di reati perseguibili d'ufficio.

Nella scheda di approfondimento "I PRINCIPALI REATI PROCEDIBILI D'UFFICIO" ne sono indicati i principali. Non ci sono tuttavia reati specifici che descrivono comportamenti illeciti tenuti on-line e si deve quindi fare riferimento ai reati sopra elencati. Ad esempio i comportamenti come il Cyberbullismo e il Sexting vanno valutati caso per caso in quanto possono includere uno o più dei reati perseguibili d'ufficio elencati nella scheda di approfondimento.

Va altresì evidenziato che 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. Oltre al team dell'emergenza, sono disponibili 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.

FASE 4 – MONITORAGGIO

Il monitoraggio è una fase importante del processo che permette al team per la gestione delle

emergenze di verificare la presenza di cambiamenti a seguito dell'intervento/degli interventi messi in atto: lo strumento utile allo scopo è la "SCHEDA DI MONITORAGGIO"

A breve termine (entro una/due settimane) permette di capire se la situazione è migliorata o se sono necessarie azioni aggiuntive; a lungo termine (dopo circa 1 mese dalla redazione della Scheda di Monitoraggio) permette di verificare se il cambiamento ottenuto a seguito dell'intervento si mantiene nel tempo.

La fase di monitoraggio include anche la rilevazione di tutti gli episodi di bullismo/cyberbullismo gestiti in un apposito DIARIO DI BORDO, redatto dal referente d'istituto per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo.

5.3. - Gli attori sul territorio

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

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

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

- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da

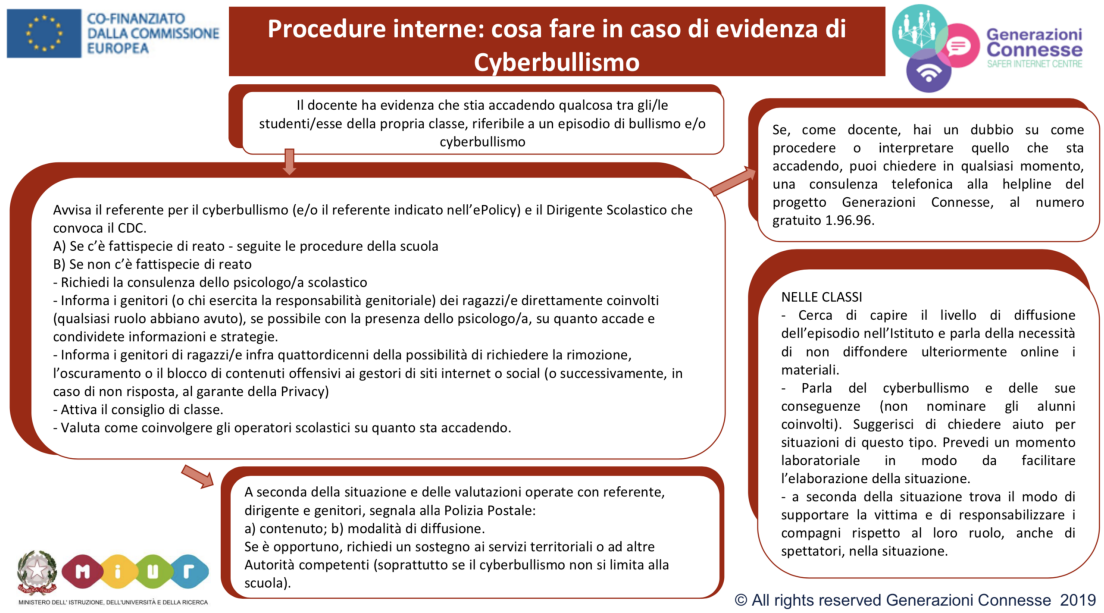
Internet e alle situazioni di rischio correlate.

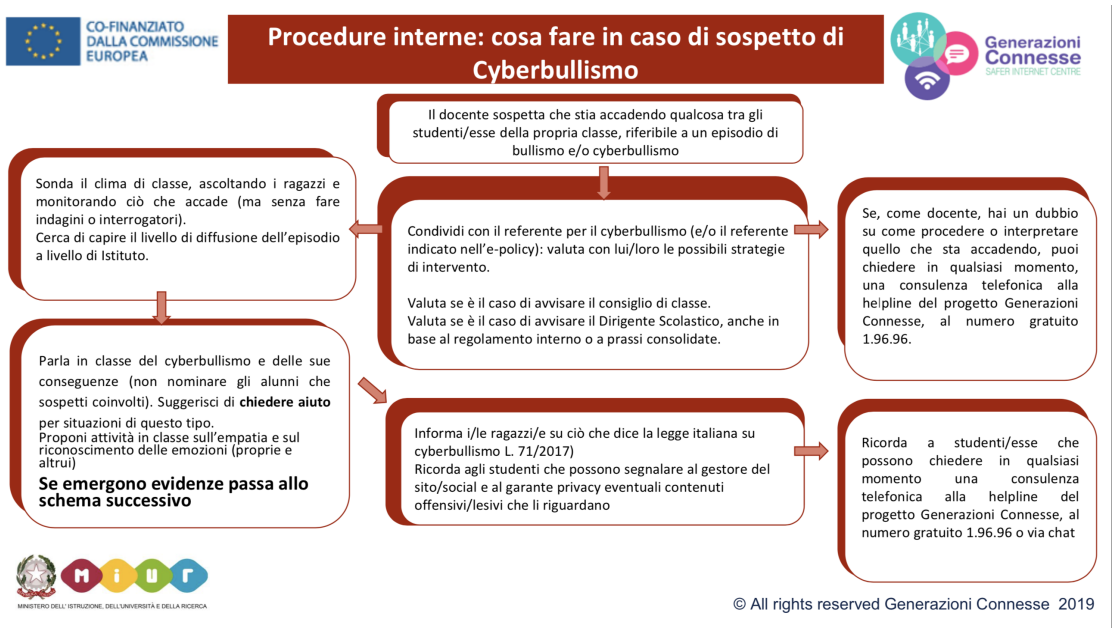
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico**: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

Nell'ambito della fase 3, ove si renda necessario il supporto intensivo di lungo termine e di rete, per individuare a chi rivolgersi e decidere quale agenzia contattare, il team dell'emergenza redige insieme al DS il modulo "INTERVENTO DI RETE CON IL TERRITORIO" utilizzando il Vademecum/guida operativa (allegato al presente documento) realizzato nell'ambito del progetto Generazioni Connesse SIC III – Safer Internet Centre Italia in cui è compresa la lista di servizi e istituzioni di cui sono forniti indirizzi e riferimenti telefonici, con una suddivisione regionale, per reperire risorse e supporto nei casi di bullismo e cyberbullismo.

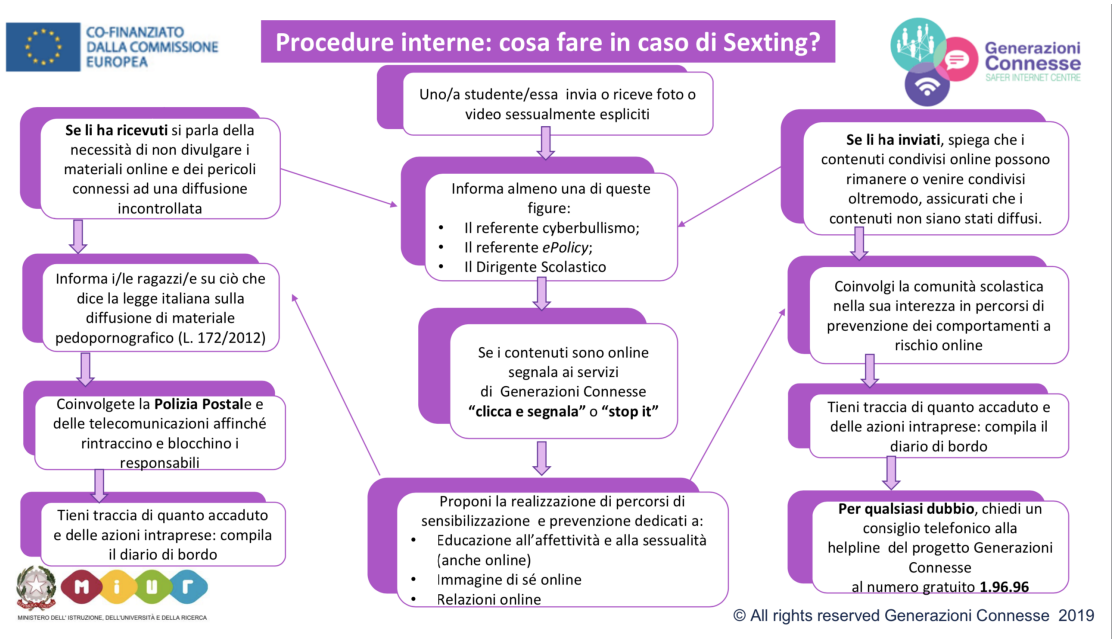
5.4. - Allegati con le procedure

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

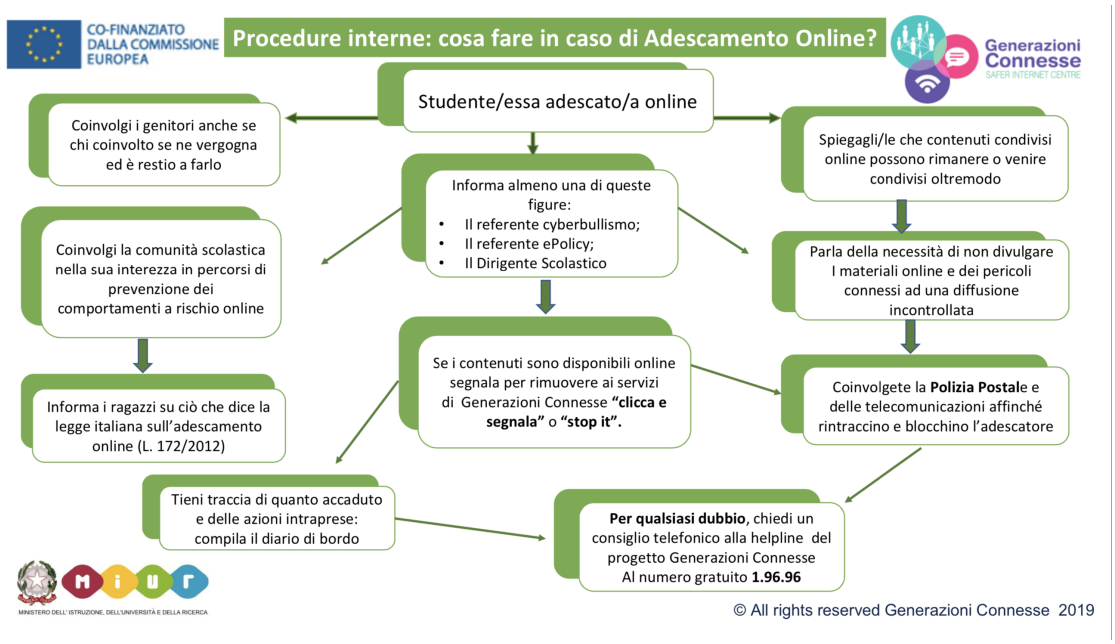




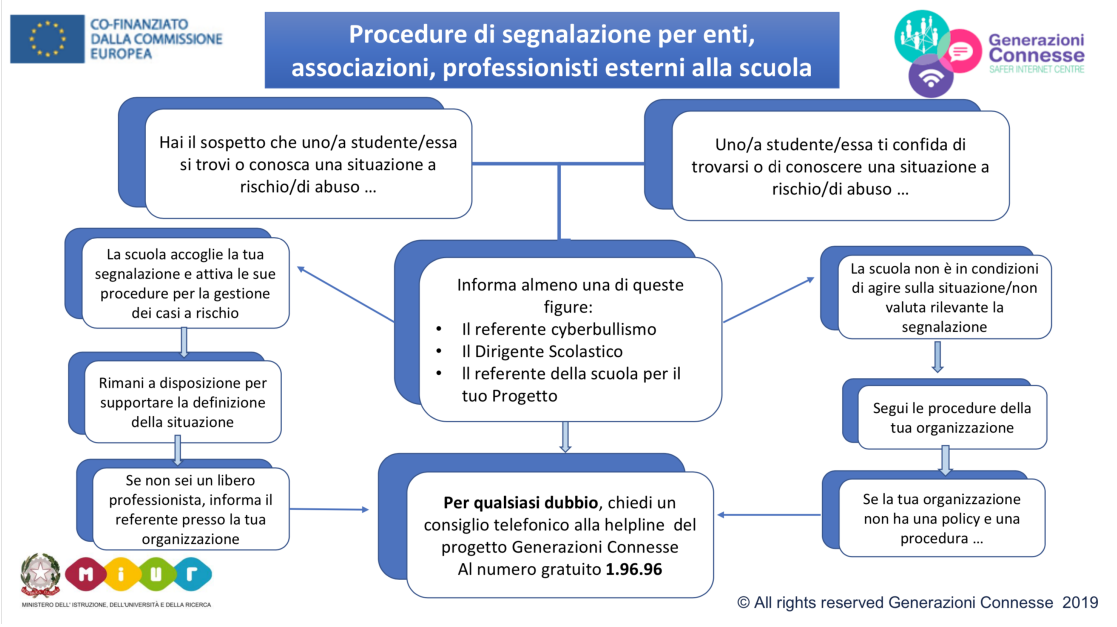
Procedure interne: cosa fare in caso di sexting?



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

Oltre agli schemi di procedura sopra indicati, che sono parte integrante del Protocollo di Gestione dell'Emergenza elaborato dall'Istituto, si allega tutta la modulistica e le schede di approfondimento trattate in questo capitolo:

- Schema "Procedura per caso presunto bullismo e vittimizzazione a scuola""
- Modulo "SCHEDA DI PRIMA SEGNALAZIONE"
- Modulo "VALUTAZIONE APPROFONDITA DEI CASI DI BULLISMO E VITTIMIZZAZIONE"
- Modulo "SCHEDA DI MONITORAGGIO"
- Modulo "INTERVENTO DI RETE CON IL TERRITORIO"
- "VADEMECUM – Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzi delle tecnologie digitali da parte dei più giovani" realizzato nell'ambito del progetto Generazioni Connesse SIC III – Safer Internet Centre Italia
- Diario di bordo
- Scheda di approfondimento " I PRINCIPALI REATI PROCEDIBILI D'UFFICIO"

Il nostro piano d'azioni

(2020/2021)

Organizzazione lancio del Protocollo di Emergenza rivolto a docenti, studenti/esse, famiglie.

(TRIENNIO)

Riformulazione del documento di E-policy per l'implementazione delle problematiche relative al bullismo basato sul pregiudizio (etnico, omofobico, verso la disabilità)

Organizzazione incontri di formazione rivolto ai docenti sulle tecniche di gestione della relazione, ascolto attivo, comunicazione non verbale.