Ministero dell'istruzione, dell'università e della ricerca
Istituto Comprensivo "S. Andrea"
Via Locatelli 41 – 20853 Biassono (MB) Tel. 039 490661
e-mail: mbic82600c@istruzione.it mbic82600c@pec.istruzione.it

E POLICY – a.s. 2020/21

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:

- Presentazione dell'ePolicy
- Scopo dell'ePolicy
- Ruoli e responsabilità
- Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
- Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
- Gestione delle infrazioni alla ePolicy

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

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.

È fondamentale ricordare le figure professionali che a vario titolo si occupano all'interno dell'Istituto della gestione e della programmazione delle attività formative, didattiche ed educative, come bisogna considerare le figure che appartengono alla comunità educante.

- Il **Dirigente Scolastico** Mariagnese Trabattoni garantisce la sicurezza anche online dei membri della comunità scolastica e per questo è formato adeguatamente sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del M.I. – Oltre a promuovere la cultura della sicurezza online, dà il proprio contributo all'organizzazione insieme all'Animatore digitale e al docente referente sulle tematiche del bullismo/cyberbullismo al fine di promuovere corsi di formazione specifici per le figure scolastiche sull'utilizzo positivo e responsabile delle TIC. Il Dirigente Scolastico ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

- L'**Animatore digitale** supporta il personale scolastico da un punto di vista sia tecnico-informatico che in riferimento ai rischi online, alla protezione e gestione dei dati personali. E' pure uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (per es: si occupa dello sviluppo delle competenze digitali previste nell'ambito dell'educazione civica) e ha il compito di monitorare, rilevare episodi o problematiche connesse all'uso delle TIC a scuola. Controlla che gli utenti autorizzati accedano correttamente alla Rete della scuola con apposita password, per scopi istituzionali e consentiti di istruzione e per la formazione. Nel nostro Istituto ricopre questa funzione la docente Monica Fusco.

- il **Referente bullismo e cyberbullismo** coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo avvalendosi, a stretto contatto con il Dirigente Scolastico, della collaborazione delle Forze di Polizia e delle associazioni presenti sul territorio che svolgono azione di prevenzione e controllo. Tale referente opera sia in ambito scolastico che extrascolastico, in quanto predispone progetti e percorsi formativi rivolti agli studenti della Primaria e della Secondaria di I grado nel corso di specifiche attività interdisciplinari organizzate in classe anche in occasione della giornata del Save Internet Day. Il Referente del bullismo e cyberbullismo predispone la formazione per i colleghi durante specifici incontri alternando gli interventi tra le riflessioni sul versante psicologico del fenomeno e le valutazioni rivolte alla normativa e alla conseguente modalità di intervento. Organizza incontri coi genitori con "*serate a tema*" invitando a partecipare psicologi e pedagogisti attivi sul campo del cyber bullismo nonché responsabili delle forze dell'ordine. In particolare le figure presenti nel nostro istituto sono le seguenti:
  - Referente bullismo/cyberbullismo: Antonella Casiraghi
  - Collaboratori del referente bullismo/cyberbullismo: Barbara Porro (scuola secondaria di primo grado) e Clara Montecchio Mariacristina Massari (scuola primaria)
  - Referente Ludopatia: Giulia Colzani
  - Funzione strumentale per le Nuove Tecnologie: Tiziano Cesana

- I **Docenti** diffondono la cultura dell'uso responsabile delle TIC e della Rete integrando il curricolo delle proprie discipline con approfondimenti che promuovono, laddove possibile, l'uso delle tecnologie digitali nella didattica. Gli insegnanti, per altro, accompagnano e supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'utilizzo della LIM o degli 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.

- Gli **Studenti e le Studentesse**, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzano al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti. Con il supporto della scuola imparano a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le; partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e si fanno promotori di quanto appreso attraverso possibili percorsi di peer education.

- I **Genitori**, in continuità con l'Istituto scolastico, sono coinvolti dalla Scuola ad essere partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali. Si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicano con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet. Sono coinvolti nel condividere quanto scritto nell'ePolicy dell'Istituto. E' bene ricordare che esiste una corresponsabilità educativa e formativa che riguarda sia i genitori che la scuola nel percorso di crescita degli studenti e delle studentesse. A tal proposito le fonti normative sono le seguenti:
  - per i docenti → 2° comma dell'art. 2048 c.c.: *"I precettori e coloro che insegnano un mestiere o un'arte sono responsabili del danno cagionato dal fatto illecito dei loro allievi e apprendisti nel tempo in cui sono sotto la loro vigilanza"*.
  - per i genitori
    → 1° comma dell'art. 30 della Costituzione: *"è dovere e diritto dei genitori mantenere, istruire ed educare i figli, anche se nati fuori del matrimonio"*;
    → 1° comma dell'art. 2048 c.c. :*" il padre e la madre o il tutore sono responsabili del danno cagionato dal fatto illecito dei figli minori non emancipati o delle persone soggette alla tutela, che abitano con essi (...)"*;
    → l'art. 147 del c.c.: *"l'obbligo di mantenere, istruire, educare e assistere moralmente i figli, nel rispetto delle loro capacità, inclinazioni naturali e aspirazioni (...)".*

Dato questo quadro normativo, rispetto ad un profilo processuale anche in materia di bullismo e cyberbullismo (dunque non in via esclusiva), si parla di tre tipologie di "culpa":
- **culpa in vigilando:** concerne la mancata sorveglianza attiva da parte del docente responsabile verso il minore (cosi come da art. 2048 del c.c.). Tale condizione è superabile se ci si avvale di una prova liberatoria di non aver potuto impedire il fatto (recita il terzo comma dell'art. 2048 c.c.: "*le persone indicate nei commi precedenti sono liberate dalla responsabilità soltanto se provano di non aver potuto impedire il fatto*");
- **culpa in organizzando:** si riferisce ai provvedimenti previsti e presi dal Dirigente Scolastico ritenuti come non soddisfacenti e quindi elemento favorevole al verificarsi dell'eventuale incidente;
- **culpa in educando:** a capo ai genitori i quali hanno instaurato una relazione educativa con il/la figlio/a, ritenuta come non adeguata, insufficiente o comunque carente tale da metterlo/a nella situazione di poter recare danno a terzi.

- Gli **Enti educativi esterni e le associazioni** che entrano in relazione con la scuola per l'attivazione del POF, si conformano alla politica della Scuola riguardo all'uso consapevole della Rete e delle TIC. Promuovono comportamenti sicuri, la sicurezza online e assicurano la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

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).

Saranno individuate un insieme di regole o norme di comportamento da condividere per tutelare questi ultimi e la scuola stessa, ma anche porre in essere nuove modalità per rilevare, limitare e contrastare

possibili pericoli legati a condotte educative non professionali al fine di rendere l'ePolicy uno strumento efficace per la tutela degli studenti e delle studentesse, intesa in senso ampio, con le organizzazioni/associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve e/o lungo periodo. Tale documento potrà chiarire il sistema di azioni e le procedure di segnalazione da seguire valide anche per i professionisti e le organizzazioni esterne, finalizzate a rilevare e gestire le problematiche connesse ad un uso non consapevole delle tecnologie digitali. L'ePolicy, inoltre, tutela i ragazzi e le ragazze da comportamenti potenzialmente rischiosi messi in atto da soggetti esterni alla scuola e che si trovano ad operare all'interno dell'Istituto. È importante garantire che i soggetti esterni, eroganti attività in ambito scolastico, siano sensibilizzati e resi consapevoli sia dei rischi online che possono correre gli studenti e le studentesse che dei comportamenti corretti che devono adottare a scuola. Come fattore ulteriormente protettivo verso i minori l'istituto richiede il casellario giudiziale agli attori esterni per 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. È un fattore preferenziale la presenza di un codice di condotta adottato dalla propria organizzazione o associazione (cooperativa, ente di formazione, servizio, etc.). Nell'ePolicy sono esplicitate nel regolamento le modalità di utilizzo di dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola in modo da evitare un uso improprio o deontologicamente scorretto. 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).

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

Il documento di E-policy è 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 è 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 ed è 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 sono 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.

E' indispensabile che il documento di ePolicy debba essere condiviso e comunicato all'interno comunità educante, ponendo al centro gli studenti e le studentesse nonché sottolineando i compiti, le funzioni e le attività reciproche.
Nello specifico è importante condividere e comunicare il documento di ePolicy:

- per dare agli studenti e alle studentesse una base di partenza per un uso consapevole e maturo dei dispositivi e della tecnologia informatica. E' rilevante dare loro le regole condivise di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici e fornire elementi per riconoscere e quindi prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e;
- al personale scolastico affinché siano orientati sui temi in oggetto, a partire da un uso corretto dei dispostivi e della Rete in linea anche con il codice di comportamento dei pubblici dipendenti;
- ai genitori sul sito istituzionale della scuola, nonché tramite momenti di formazione specifici e durante gli incontri scuola-famiglia.
- ogni attore scolastico, dai docenti agli/lle studenti/esse, si deve fare promotore del documento di ePolicy.

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.

La scuola individua con chiarezza le modalità di gestione di eventuali infrazioni all'ePolicy privilegiando le azioni educative e valuta i diversi gradi di gravità di eventuali violazioni. Per redigere l'ePolicy nel modulo 5 sono analizzati alcuni dei principali rischi connessi ad un uso poco consapevole delle tecnologie digitali e sono esposte le relative procedure di segnalazione e gestione delle infrazioni anche in riferimento agli specifici regolamenti in materia. La Scuola rifletterà sulle possibili condotte sanzionabili in relazione all'uso improprio delle TIC e della Rete a scuola da parte degli studenti e delle studentesse, come ad esempio:

- la condivisione online di immagini o video di compagni/e senza il loro consenso o che li ritraggono in pose offensive e denigratorie;
- la condivisione di scatti intimi e a sfondo sessuale; la condivisione di dati personali; l'invio di immagini o video volti all'esclusione di compagni/e.

A seconda dell'età dello studente o della studentessa, la Scuola deve intervenire sul contesto classe con attività specifiche educative e di sensibilizzazione per promuovere una maggior consapevolezza circa l'utilizzo delle TIC e di Internet. È opportuno, qualora fosse necessario, che la Scuola valuti la natura e la gravità di quanto possa essere accaduto, al fine di considerare la necessità di denunciare l'episodio (con il coinvolgimento ad es. della Polizia Postale) o di garantire l'immediato supporto psicologico allo/la studente/ssa attraverso i servizi predisposti.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

Si allegano all'ePolicy i Regolamenti Scolastici aggiornati per favorirne un'adeguata integrazione.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'E-policy è aggiornata periodicamente e/o quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone. Il monitoraggio del documento di ePolicy prevede una valutazione della sua efficacia a partire dagli obiettivi specifici che lo stesso si pone come la promozione delle competenze digitali e dell'uso delle TIC nei percorsi educativi e didattici, la prevenzione e la gestione dei rischi online etc...
Il Dirigente Scolastico nomina un referente che si debba occupare della revisione e/o dell'aggiornamento dell'ePolicy.

Azioni - 1 anno

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

Azioni - 3 anni

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

- Num. Docenti 94
- Num. Studenti secondaria 291 primaria 4 e 5 (83 + 96)
- Numero Genitori 940

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.

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.

Gli insegnanti usano le TIC ad integrazione della didattica al fine di progettare, sviluppare, utilizzare, gestire e valutare i processi di insegnamento e apprendimento di tutti gli studenti della classe, anche delle persone con disabilità (in chiave inclusiva). Di conseguenza, gli insegnanti devono raggiungere un buon livello di formazione in merito all'utilizzo e l'integrazione delle TIC nella didattica. Il nostro Istituto, attraverso il Collegio dei Docenti, riconosce e favorisce la partecipazione del personale ad iniziative promosse dalla scuola, dalle reti di scuole e quelle liberamente scelte dai docenti (anche online), coerenti con il piano di formazione. In seguito al questionario conoscitivo delle competenze informatiche dei docenti, il team digitale predispone una formazione in piccoli gruppi con il coinvolgimento di docenti esperti nei programmi di videoscrittura, presentazioni, di calcolo, app online e altri programmi specifici delle diverse discipline. 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.

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, saranno 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.

Il nostro Istituto organizza corsi di formazione per docenti e genitori sulle opportunità e i rischi offerti dalla rete, in collaborazione con gli esperti dell'azienda Cisco; sulle tematiche del cyberbullismo**,** disinformazione e fakenews con psicologi e figure dell'ambito giuridico-normativo. Il sito istituzionale è aggiornato con iniziative e materiali volti ad informare la comunità educante sugli aspetti legati

all'uso consapevole e corretto delle TIC, al fine di prevenire eventuali comportamenti a rischio. Sempre sul sito istituzionale della scuola, sono inclusi link e materiali informativi del progetto "Generazioni connesse".

2.4 Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

Ogni anno scolastico l'Istituto:

- aggiorna o integra con specifici riferimenti alle tecnologie digitali e all'ePolicy sia il regolamento d'Istituto che il "Patto di corresponsabilità";
- fornisce ai genitori consigli sull'uso delle tecnologie digitali nella comunicazione con i figli e in generale in famiglia, indicando sul sito istituzionale il riferimento alla sezione dedicata ai genitori del sito www.generazioniconnesse.it;
- organizza percorsi di sensibilizzazione e formazione dei genitori su un uso responsabile e costruttivo della Rete in famiglia e a scuola in collaborazione con gli esperti del settore, con i Servizi Sociali del Comune e il personale docente specificatamente formato.

Durante i consigli di classe sia della Primaria che della Secondaria di I grado, si condividono le regole sull'uso delle tecnologie digitali da parte dei genitori nelle comunicazioni con la scuola e con i docenti (es. mail, gruppo whatsapp, sito della scuola, registro elettronico).

Azioni 2 – 1 anno

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

Azioni 3 anni

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle 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 sono 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.

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).
È importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali che si trovano a trattare, in particolare quando sono coinvolti soggetti minorenni adeguandosi al GDPR (General Data Protection Regulation) 2016/679. In particolare la scuola ha sia il compito di tutelare la privacy degli/lle studenti/esse e delle loro famiglie, che l'incarico di informare e soprattutto rendere consapevoli gli/le studenti/esse di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri.
E' opportuno ricordare che il nostro Istituto tratta solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali, oppure quelli espressamente previsti dalla normativa di settore. Per tali trattamenti non si è tenuti a chiedere il consenso degli studenti. Alcune categorie di dati personali degli studenti/esse e delle famiglie, come quelli sensibili e giudiziari, devono essere trattati con estrema cautela, nel rispetto di specifiche norme di legge.
Tramite apposita informativa la scuola informa gli interessati delle caratteristiche e modalità del trattamento dei loro dati, indicando i responsabili del trattamento. Gli interessati sono sia gli/le studenti/esse che le famiglie e gli stessi professori. La rete wifi dell'intero Istituto è dotata di un proxy e di un firewall hardware per la messa in sicurezza della rete intranet scolastica. Per l'utilizzo della piattaforma didattica Gsuite si invia alle famiglie l'apposita modulistica per informare e richiedere il consenso all'utilizzo. Sono istituiti corsi di formazione destinati ai responsabili e agli incaricati del trattamento.

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.

Il curricolo scolastico prevede che gli/le studenti/esse imparino a trovare materiale, recuperare documenti e scambiare informazioni utilizzando le TIC. E' anche fondamentale dotare gli studenti delle competenze necessarie ad affrontare la complessità del mondo dell'informazione, per metterli in grado di destreggiarsi tra notizie e fake news, discussioni online e discorsi d'odio (*hate speec*).
L'Istituto è dotato di Regolamento sull'utilizzo delle TIC.
→ Gli studenti si impegnano a:
- utilizzare la rete nel modo corretto
- rispettare le consegne dei docenti
- non scaricare materiali e software senza autorizzazione
- non utilizzare unità removibili personali senza autorizzazione
- tenere spento lo smartphone
- segnalare immediatamente materiali inadeguati ai propri insegnanti.

→ I docenti si impegnano a:
- utilizzare la rete nel modo corretto
- non utilizzare device personali se non per uso didattico
- formare gli studenti all'uso della rete
- dare consegne chiare e definire gli obiettivi delle attività
- monitorare l'uso che gli studenti fanno delle tecnologie a scuola.

Inoltre l'Istituto al fine di salvaguardare la sicurezza in rete, prevede di:
- Mantenere separate le reti didattica e segreteria: importante per garantire maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le due reti grazie al firewall.
- Aggiornare periodicamente software e Sistema operativo: garantire che il sistema sia aggiornato lo protegge dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo.
- Definire la programmazione di backup periodici: cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi (possibilmente anche una copia offline).
- Garantire formazione adeguata allo staff, incluso il corpo docenti: la formazione deve riguardare la gestione dei dispositivi, la conoscenza delle regole basilari sulla sicurezza.
- Predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo: se non è previsto uno stand-by, il dispositivo resta accessibile nel caso in cui qualcuno dimentichi di spegnerlo, con il rischio potenziale di accesso da parte di persone non autorizzate.

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.

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.

Azioni – 1 anno
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.

Azioni – 3 anni
- 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.*

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

Interventi di sensibilizzazione

Per l'Istituto è una priorità la tutela della sicurezza degli studenti e delle studentesse che si connettono al web. Per questo motivo si organizzano differenti azioni di sensibilizzazione rivolte a:

- insegnanti mediante specifici incontri di formazione in Collegio Docenti nel corso dei quali si sottolineano gli aspetti normativi e le responsabilità specifiche del docente;
- genitori con riunioni mirate a conoscere la problematica sia sul versante sociale che psicologico affiancando approfondimenti tecnici che portino a conoscenza degli aspetti più innovativi della tecnologia anche a disposizione dei più giovani;
- studenti e studentesse sia della Primaria che della Secondaria di I grado con incontri di formazione nel corso dei quali, avvalendosi anche di esperti esterni del settore e nel campo psicologico e pedagogico, si danno giusti consigli discutendo su quali conseguenze possa avere il comportamento di una persona in rete specificando con opportune esemplificazioni il significato di *cybermobbing* per le vittime. Si evidenzia come ci si possa proteggere gli studenti mantenendo un comportamento rispettoso (*netiquette*), evitando di postare dati e informazioni sensibili sul proprio profilo (per es. foto imbarazzanti o troppo discinte), curando solo amicizie personali e proteggendo la sfera privata mediante criteri d'impostazione sicuri.

Interventi di prevenzione

Al fine di individuare strategie di prevenzione e di contrasto al cyberbullismo e favorire opportune azioni educative e pedagogiche, l'Istituto promuove:

- l'acquisizione delle competenze digitali per 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 conoscenza e la diffusione delle regole basilari della comunicazione e del comportamento sul web, come:

- la *netiquette*, un termine che unisce il vocabolo inglese *network* (rete) e quello francese *étiquette* (buona educazione): un insieme di regole informali che disciplinano il buon comportamento di un utente sul web di Internet, specie nel rapportarsi agli altri utenti attraverso risorse come newsgroup, mailing list, forum, blog, reti sociali o e-mail;
- le norme di uso corretto dei servizi in rete (ad es. navigare evitando siti web rischiosi/deep web; non compromettere il funzionamento della rete e degli apparecchi che la costituiscono con programmi come virus, malware, costruiti appositamente);
- la sensibilizzazione alla lettura attenta delle privacy policy, il documento cioè che descrive nella maniera più dettagliata e chiara possibile le modalità di gestione e il trattamento dei dati personali degli utenti e dei visitatori dei siti internet e dei social networks da parte delle aziende stesse;
- la costruzione di una propria web-reputation positiva;
- la sensibilizzazione sugli effetti psico-fisici del fenomeno dilagante del "*vamping*" (il restare svegli la notte navigando in rete);
- la regolamentazione dell'utilizzo dei telefoni cellulari e di altri dispositivi elettronici a scuola mediante specifici regolamenti deliberati sia in Collegio dei Docenti che in Consiglio di Istituto. Regolamenti che sono illustrati anche ai genitori nel corso delle assemblee e nei consigli di classe.

Le dimensioni che il fenomeno del cyberbullismo 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. Per questo motivo l'Istituto rafforza la sua capacità di rispondere a questi bisogni attraverso strumenti e misure specifiche. Allo stesso modo quando un evento problematico connesso ai rischi online coinvolge il contesto scolastico, l'Istituto si attiva per poter dare una risposta il più possibile integrata, mediante procedure chiare definite nei Regolamenti che prevedono la collaborazione con la rete dei servizi locali come i Servizi Sociali del Comune, l'Ats Brianza e la Polizia Postale**.**

E' importante sottolineare che la responsabilità dell'azione preventiva ed educativa mette in campo oltre alla Scuola anche altre agenzie educative, come la famiglia e le associazioni presenti sul territorio, ciascuna con un proprio compito nei confronti di bambini e bambine e degli adolescenti. Tali agenzie devono collaborare con la scuola ad un progetto comune, nell'ambito di funzioni educative condivise. La necessità di questa collaborazione deve nascere in modo consapevole il riconoscimento sia da parte dei genitori che da parte degli insegnanti della rispettiva difficoltà a svolgere da soli la

propria funzione formativa ed educativa anche a causa della sproporzione tra le competenze sempre crescenti che le tecnologie digitali richiedono loro e quelle che si avvertono di possedere. La necessità di supportare un uso positivo e consapevole delle TIC da parte dei più giovani, sia in un'ottica di tutela dai rischi potenziali che nella valorizzazione delle opportunità esistenti, pone la scuola e i genitori di fronte alla sfida di riconsiderare la propria identità, il proprio ruolo educativo e le proprie risorse, oltre allo stato dei rapporti reciproci per un patto educativo da rinnovare costantemente.

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).

L'Istituto sta da anni sviluppando forme di prevenzione che conducono gli alunni a riflettere che il cyberbullismo è una forma di prepotenza virtuale messa in atto attraverso l'uso di Internet e delle tecnologie digitali. Spesso i termini "*bullismo e cyberbullismo*" sono usati impropriamente e si riconducono ad essi i più svariati episodi di violenza o offese fra ragazzi/e. Bullismo e cyberbullismo hanno, però, connotati ben precisi e non vanno confusi con altre problematiche del mondo giovanile. In particolare si sottolinea come i tratti specifici del *bullismo online* sono correlati all'impatto che le tecnologie digitali hanno sia nella vita dei ragazzi che negli nella vita degli adulti in riferimento alle caratteristiche stesse della Rete.

Tratti specifici su cui riflettere perché il fenomeno è talvolta sottovalutato anche dal mondo adulto, familiare e scolastico, sono:

- l'impatto nel senso che la diffusione di materiale tramite Internet è incontrollabile perché, nell'essere virale, può giungere a distruggere in alcuni casi la reputazione della vittima;
- la convinzione dell'anonimato che è un "*falso mito della Rete*" porta l'Istituto a mantenere massima allerta sapendo che ci sono strumenti opportuni come richiedere l'intervento della Polizia Postale;
- l'assenza di confini spaziali in quanto il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio. La vittima può essere raggiungibile a casa e vive nella costante percezione di non avere vie di fuga;
- l'assenza di limiti temporali può avvenire a ogni ora del giorno e della notte;
- la riduzione dell'empatia nei cyberbulli;

- il feedback non tangibile cioè il cyberbullo non vede in modo diretto le reazioni della vittima riducendo l'empatia e il riconoscimento del danno provocato.

La mediazione tecnologica, infatti, porta ad un certo distanziamento fra aggressore e vittima, causando quello che Bandura ha definito come il "*disimpegno morale*" che è l'indebolimento del controllo morale interno dell'individuo, con la conseguente minimizzazione delle responsabilità individuali. Per contrastare il fenomeno del "*disimpegno morale*" l'Istituto è attento a definire i Regolamenti in cui sono definite le norme di comportamento con conseguenti sanzioni nel caso di violazione da parte degli alunni. Negli incontri con gli Esperti esterni, che sono invitati annualmente nelle classi soprattutto nella Secondaria di I grado, si trasmette il messaggio dalla diffusione del senso di responsabilità. Mettere un "like" su un social network, commentare o condividere una foto o un video che prende di mira qualcuno o soltanto tacere pur sapendo, mette ragazzi e ragazze nella condizione di avere una responsabilità. La responsabilità è condivisa. Il cyberbullismo è un fenomeno sociale e di gruppo. È centrale, infatti, il ruolo delle agenzie educative e di socializzazione più importanti per gli adolescenti: la famiglia, la scuola, i media, le tecnologie digitali e il gruppo dei pari. A tal proposito si programmano incontri di formazione con i genitori con cadenza quadrimestrale definendo momenti di riflessione e di confronto sul vissuto dei propri figli. In questi incontri si ribadisce che la responsabilità è dei genitori che devono educare adeguatamente e vigilare, in maniera adeguata all'età del figlio, cercando di correggerne comportamenti devianti. I genitori devono essere consapevoli che la loro responsabilità è generale e persiste per gli atti compiuti nei tempi di affidamento alla scuola. Gli insegnanti dell'Istituto vigilano perché sono responsabili e hanno il dovere di impedire i comportamenti dannosi degli alunni. La scuola mette in atto le azioni previste per la prevenzione del fenomeno o per affrontarlo al meglio organizzando sistematicamente corsi di formazione per il Collegio dei Docenti con il supporto dell'insegnante referente del contrasto al cyberbullismo all'interno dell'Istituto. Il referente ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo svolgendo un importante compito di supporto al Dirigente Scolastico per la revisione/stesura di Regolamenti come il Regolamento d'istituto, atti, documenti come il PTOF (Piano triennale dell'Offerta Formativa), il PdM (Piano di Miglioramento), il Rav (Rapporto di Autovalutazione) e il Patto di Corresponsabilità. In particolare i docenti sono stati aggiornati sulla conoscenza approfondita della Legge 71/2017 "*Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyber bullismo*" che prevede misure prevalentemente a carattere educativo/rieducativo. Sono programmati corsi di formazione per i consigli di classe per aiutare i docenti a individuare, oltre ai casi di cyberbullismo, i segnali generali che può manifestare l'alunno come potenziale vittima di cyberbullismo difendendo così gli studenti più fragili e vulnerabili. Con il supporto dei servizi socio-sanitari, che offrono pure supporti psicologici e/o di mediazione, si effettuano valutazioni circa l'eventuale stato di disagio vissuto dal minorenne vittima di cyberbullismo.

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 sono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

All'interno della conoscenza del fenomeno dell'*hate speech* si vuole portare gli alunni a riflettere che:

- il discorso d'odio on line procura sofferenza attraverso il veicolare delle parole che possono ferire violando i diritti umani. Il discorso d'odio online è grave tanto quanto le espressioni offline, ma è più difficile da individuare e da combattere;
- gli atteggiamenti alimentano gli atti. Il discorso dell'odio è pericoloso anche perché può contribuire a inasprire le tensioni razziali e altre forme di discriminazione e di violenza;
- l'odio online è espresso con le parole, ma anche sotto forma di video, foto e di contenuto testuale. Le forme visive o multimediali hanno purtroppo un impatto più forte sugli atteggiamenti consci e inconsci;
- l'odio on line prende di mira i gruppi come le persone con disabilità, ma anche i singoli individui sono sempre maggiormente oggetto di attacchi con conseguenze talvolta fatali per alcuni giovani vittime di cyberbullismo che sono stati spinti al suicidio;
- internet è difficilmente controllabile. È più facile e comporta meno rischi insultare o molestare online, perché le persone spesso si esprimono sotto la copertura dell'anonimato;
- l'odio on line ha radici profonde. Gli atteggiamenti e le tensioni sociali che suscitano sentimenti di odio online affondano le loro radici nella società;
- impunità e anonimato sono le presunte caratteristiche delle interazioni sociali in rete. Queste abbassano le remore etiche. In realtà, però, qualsiasi azione compiuta sul web consente di rintracciare il suo autore.

L'Istituto organizza un percorso di Educazione Civica che intende prevenire l'*hate speech* attraverso la "*responsabilizzazione dell'uso delle parole*" imparando a riconoscere contenuti offensivi ed evitando di utilizzare toni di voce accesi che possano insultare.
Lo sviluppo sia delle competenze digitali che l'educazione ad un uso etico e consapevole delle tecnologie assumono quindi un ruolo centrale per la promozione della consapevolezza di queste dinamiche in rete. Occorre fornire ai giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di *hate speech* e promuovere la partecipazione civica e l'impegno anche attraverso i media digitali e i social network nonché favorire una presa di parola consapevole e costruttiva da parte dei giovani. Si potrebbe dare vita il 13 novembre di ogni anno scolastico alla "*Giornata mondiale della gentilezza"*. Sarebbe un'occasione per sollecitare le parole e i gesti di cura e di attenzione verso gli altri.

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.

La dipendenza da Internet intesa come progressivo e totale assorbimento del soggetto alla Rete, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica che deve attenzionare il fenomeno e fornire gli strumenti agli studenti e alle studentesse affinché questi siano consapevoli dei rischi che comporta l'iperconnessione.
Rischi che si manifestano proprio come una vera e propria dipendenza e abuso da Internet che rivelano le seguenti caratteristiche specifiche:

- dominanza: l'attività controlla i pensieri ed il comportamento del soggetto, assumendo un valore primario tra tutti gli interessi;
- alterazioni del tono dell'umore: il soggetto prova un aumento d'eccitazione o maggiore rilassatezza come conseguenza dell'incontro con l'oggetto della dipendenza;
- conflitti inter-personali tra il soggetto e coloro che gli sono vicini;
- conflitti intra-personali interni a se stesso, a causa del comportamento dipendente
- ricaduta cioè la tendenza a ricominciare l'attività dopo averla interrotta.

L'Istituto è attento a tale aspetto tanto da definire confronti con gli alunni che dichiarano di trascorrere molto tempo online spesso scandito dal gioco virtuale che per alcuni studenti ne diventa quasi una dipendenza fino a perdere interesse verso le attività della vita reale.
In questo caso la Scuola ha predisposto la formazione di un docente referente in quest'area che si adopera per indicare strategie, tra cui la peer educazione, per un uso più consapevole delle tecnologie

per favorire il "*benessere digitale*", cioè la capacità di creare e mantenere una relazione sana con la tecnologia. Si è consapevoli che la tecnologia ha modificato gli ambienti che viviamo e ha un impatto sulla qualità della vita.
Gli elementi che contribuiscono al benessere digitale sono:

- la ricerca di equilibrio nelle relazioni anche online;
- l'uso degli strumenti digitali per il raggiungimento di obiettivi personali;
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile;
- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche).

Appare pertanto utile riflettere con gli studenti e le studentesse per fare in modo che la tecnologia sia strumento per raggiungere i propri obiettivi e non sia solo distrazione o addirittura ostacolo.
La scuola deve pertanto integrare la tecnologia nella didattica (per es. con le attività di coding), mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online. Allo stesso modo si può parlare di "*videogiochi*", da considerare non in termini negativi, ma di benessere digitale. Si è consapevoli che oramai sono parte del mondo degli alunni. Grazie anche al supporto del docente referente sono state predisposte attività specifiche che hanno condotto gli alunni a riflettere rispetto a quanto i videogiochi possano essere una risorsa. E' importante riflettere con i ragazzi e le ragazze rispetto all'uso della tecnologia in termini di qualità e tempo così che, se si controlla la tecnologia, è possibile usarne il pieno potenziale e trarne vantaggi nel rispetto di regole ben codificate.

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.

E' utile sapere che *sexting* (abbreviazione di *sex* – sesso e *texting* – messaggiare, inviare messaggi) indica l'invio e/o la ricezione di contenuti (video o immagini) sessualmente espliciti che ritraggono se stessi o gli altri che possono diventare materiale di ricatto assumendo la forma di "revenge porn" letteralmente "vendetta porno". Quest'ultimo è il fenomeno che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte. Oltre all'art.612 ter del codice penale rubricato *"Diffusione illecita di immagini o video sessualmente espliciti"*, 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.

La Scuola soprattutto nei percorsi di affettività-sessualità con i ragazzi e le ragazze della secondaria di I grado, avvalendosi anche di esperti esterni del COF – Centro Orientamento Famiglia, collegati all'ATS della provincia, organizza attività mirate che conducono gli alunni e le alunne alla consapevolezza che la diffusione di contenuti personali può danneggiare in termini psicologici e sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla**.** Due agiti che sono fra loro strettamente legati e che rappresentano veri e propri

comportamenti criminali con ripercussioni negative sulla vittima in termini di autostima, di credibilità, di reputazione sociale off e on line.

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 sono descritte le azioni che l'Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

Potenziali vittime dell'adescamento online possono essere sia bambini che bambine, sia ragazzi che ragazze. Il fenomeno, infatti, non conosce distinzione di genere. Gli adolescenti sono particolarmente vulnerabili, poiché si trovano in una fase della loro vita in cui è molto importante il processo di costruzione dell'identità sessuale. I docenti dell'Istituto devono essere attenti a valutare ogni possibile richiesta di aiuto degli alunni che potrebbe giungere in modo esplicito o mediato da altre modalità come ad es. testi individuali, disegni ...). Per questo si prevedono corsi si formazione specifici che conducano gli insegnanti a conoscere le fasi del processo di adescamento:

- la fase dell'amicizia iniziale: l'adescatore cerca i primi contatti con la vittima individuata, provando a socializzare con lei;
- la fase di risk-assessment: l'adescatore cerca di comprendere il contesto in cui si svolge l'interazione (es. i genitori lo controllano quando chatta?) L'adescatore ha l'obiettivo di rendere sempre più privato ed "esclusivo" il rapporto passando per esempio da una chat alle conversazioni al telefono, per carpirne il numero;
- la fase della costruzione del rapporto di fiducia nel corso della quale le confidenze e le tematiche affrontate divengono via via più private ed intime o comunque molto personali;
- la fase dell'esclusività: l'adescatore, ricorrendo anche a ricatti morali, 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;
- la 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. Il sapere quali siano le fasi del processo di adescamento deve essere collegato al sapere come fare ad intervenire nel caso si sospettasse o si avesse la certezza di un caso di adescamento online. È importante che l'adulto di riferimento non si sostituisca al minore nel rispondere all'adescatore e che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove. Casi di adescamento online richiedono infatti 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…). Oltre alla conoscenza delle fasi del processo di adescamento on line i docenti devono essere formati su come 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 essere 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?

Per prevenire casi di adescamento online l'Istituto organizza progetti per accompagnare ragazze e ragazzi in un percorso di educazione all'affettività e alla sessualità: ciò per aiutarli nel renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Per questo si affiancano incontri per i genitori, oltre alla formazione specifica per docenti. Gli adulti coinvolti, genitori e docenti, infatti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. E' necessario pertanto che gli adulti tengano sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e della sessualità. Nella società digitale, attraverso la Rete, i minori definiscono se stessi, si raccontano e sperimentano nuove forme di identità, socializzano, si emozionano e si relazionano con gli altri, scoprono la propria sessualità e giocano con essa. Tutto ciò risponde a bisogni assolutamente naturali e importanti, ma allo stesso tempo può esporre i ragazzi a possibili rischi come quello, appena approfondito, dell'adescamento online. Il desiderio di conferma sociale (da ottenere anche attraverso i social) e, talvolta, la scarsa consapevolezza degli adolescenti nel gestire la propria immagine online quando pubblicano sui loro profili social video e foto piuttosto intimi o sensuali, può aumentare il rischio di esporli ad un adescamento online. Con un'adeguata competenza digitale ed emotiva, Internet potrebbe essere un valido supporto per i/le ragazzi/e nel loro percorso di esplorazione della sessualità. La Rete, purtroppo, abbonda pure di contenuti inadeguati che offrono una rappresentazione distorta della sessualità e dei rapporti uomo-donna senza alcun richiamo alla dimensione affettiva ed emotiva dei soggetti. Il più delle volte, tali rappresentazioni ricalcano con forza stereotipi di genere come quello della "*donna oggetto*" e quello dell'"*uomo forte e virile*". In un contesto simile non c'è da stupirsi se riproducano tali modelli, talvolta, anche i comportamenti degli adolescenti in Rete nella gestione della propria sessualità o semplicemente della propria immagine online. Modelli che la società odierna sembra confermare in messaggi che quotidianamente ci arrivano attraverso i media. La problematica dell'adescamento online, come quella del *sexting*, quindi, si inquadra in uno scenario più ampio di scarsa educazione emotiva, sessuale e di assenza di competenza digitale, in riferimento al modo in cui i/le ragazzi/e vivono la propria sessualità e la propria immagine online, al loro desiderio di esprimersi e affermare se stessi. Fondamentale quindi è che la Scuola organizzi percorsi di educazione digitale che comprendano lo sviluppo di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online. E' importante sottolineare che l'adescamento ha ripercussioni psicologiche significative sul minore. Per questo i genitori in collaborazione con la scuola devono rivolgersi ai Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima un adeguato supporto di tipo psicologico o psichiatrico. I minori vittime di adescamento riferiscono, generalmente, di sentirsi traditi e di provare un senso di colpa per essere caduti in trappola ed essersi fidati di uno sconosciuto. È da considerarsi prioritario e urgente un sostegno psicologico esperto per il minore nei casi più estremi in cui l'adescamento porta ad un incontro fisico e ad un abuso sessuale. Per consigli e per un supporto i docenti possono rivolgersi alla Helpline di Generazioni Connesse. Operatori esperti sono sempre a disposizione degli insegnanti, del Dirigente Scolastico 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.

Studi in materia dimostrano come l'utilizzo di materiale pedopornografico possa essere propedeutico all'abuso sessuale agito ed è quindi fondamentale, in termini preventivi, intervenire per ridurre l'incidenza di tale possibilità.
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. La Scuola ha il compito di guidare i giovani ad acquisire competenze in grado di orientarli e guidarli nelle loro scelte anche online. Per questo motivo, come già sottolineato, l'educazione, compresa l'educazione all'affettività, riveste un ruolo fondamentale. 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. Risulta utilissima l'attività educativa sull'affettività e le relazioni, invitando i giovani nella necessità di rivolgersi ad un adulto quando qualcosa online mette loro a disagio. I docenti devono essere formati affinché possano capire che la pedopornografia è strettamente interconnessa agli aspetti legati alle conseguenze impreviste del *sexting*. La Scuola è disponibile ad organizzare attività di sensibilizzazione rivolta ai genitori.

Piano di azioni (*)
Numero Docenti da raggiungere (*): tutti i docenti in servizio sia nella Primaria che nella Secondaria di I grado**.**

AZIONI – 1 anno
- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

AZIONI - 3 ANNI

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.

Capitolo 5 - Segnalazione e gestione dei casi

5.1 - Cosa segnalare

Il personale docente del nostro Istituto ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica 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.
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;
- l'utilizzo di locandine da affiggere a scuola
- news nel sito della scuola
- durante i Collegi dei Docenti
- 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.

E' necessario che ciascun docente, venuto a conoscenza delle sopracitate situazioni, riferisca tempestivamente al Dirigente scolastico Mariagnese Trabattoni e al docente referente del bullismo e cyberbullismo (Antonella Casiraghi) e ai suoi collaboratori (Plesso Pietro Verri: Barbara Porro, Plesso Sant'Andrea: Clara Montecchio, Plesso Aldo Moro: Mariacristina Massari).

5.2. - Come segnalare: quali strumenti e a chi

Il professore è un pubblico ufficiale a tutti gli effetti nel momento in cui esercita la sua funzione. L'insegnante riveste pertanto 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 prevede la presenza in ogni plesso di un docente referente per le segnalazioni appositamente sensibilizzato e/o formato.
Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Nel caso A per aiutare gli studenti a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni si prevedono strumenti di segnalazione ad hoc messi a loro disposizione → lo studente si rivolge all' insegnante di classe, che a sua volta riferisce al docente referente per le segnalazioni. E' possibile avvisare l'intero consiglio di classe e, se si ravvisa la necessità e l'urgenza, coinvolgere il Dirigente Scolastico. Nel frattempo, il docente (e i docenti informati) ascolta gli studenti e prevede momenti laboratoriali, utilizzando anche la piattaforma

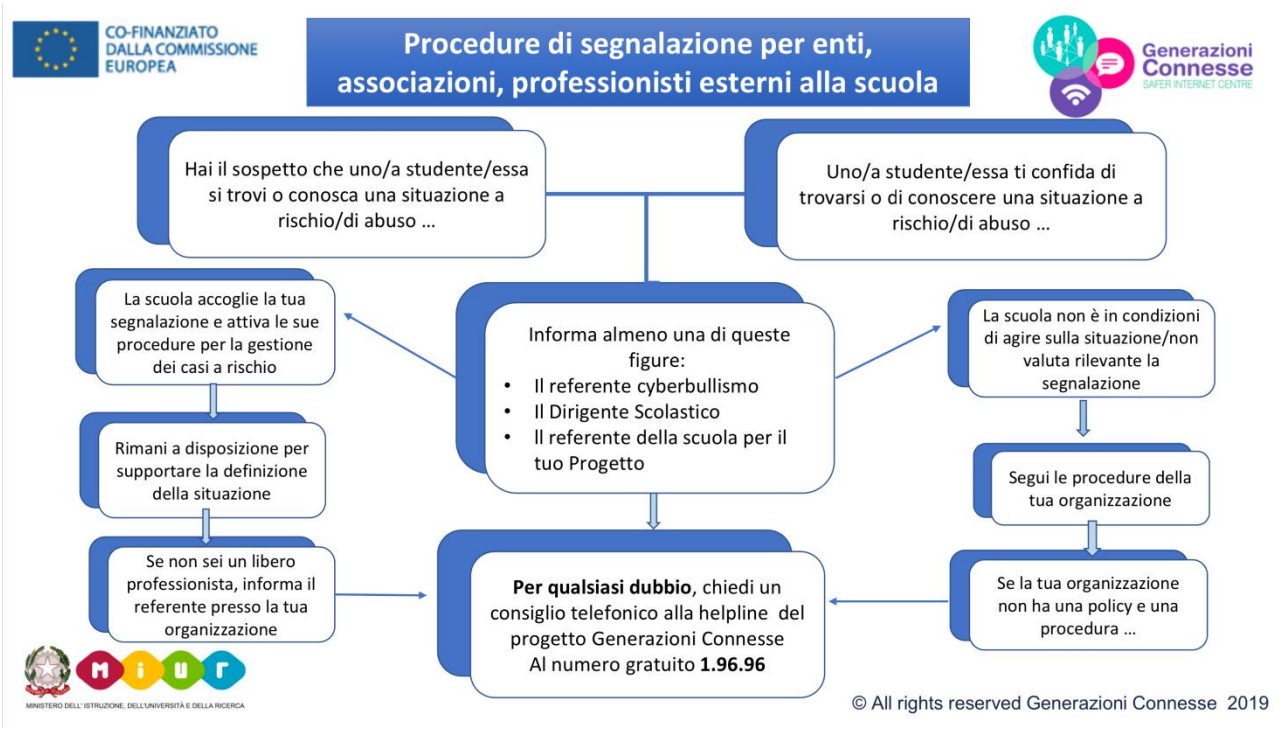
Generazioni Connesse nella parte dei contenuti e dei materiali, per stimolare il dialogo e la riflessione all'interno del gruppo classe.

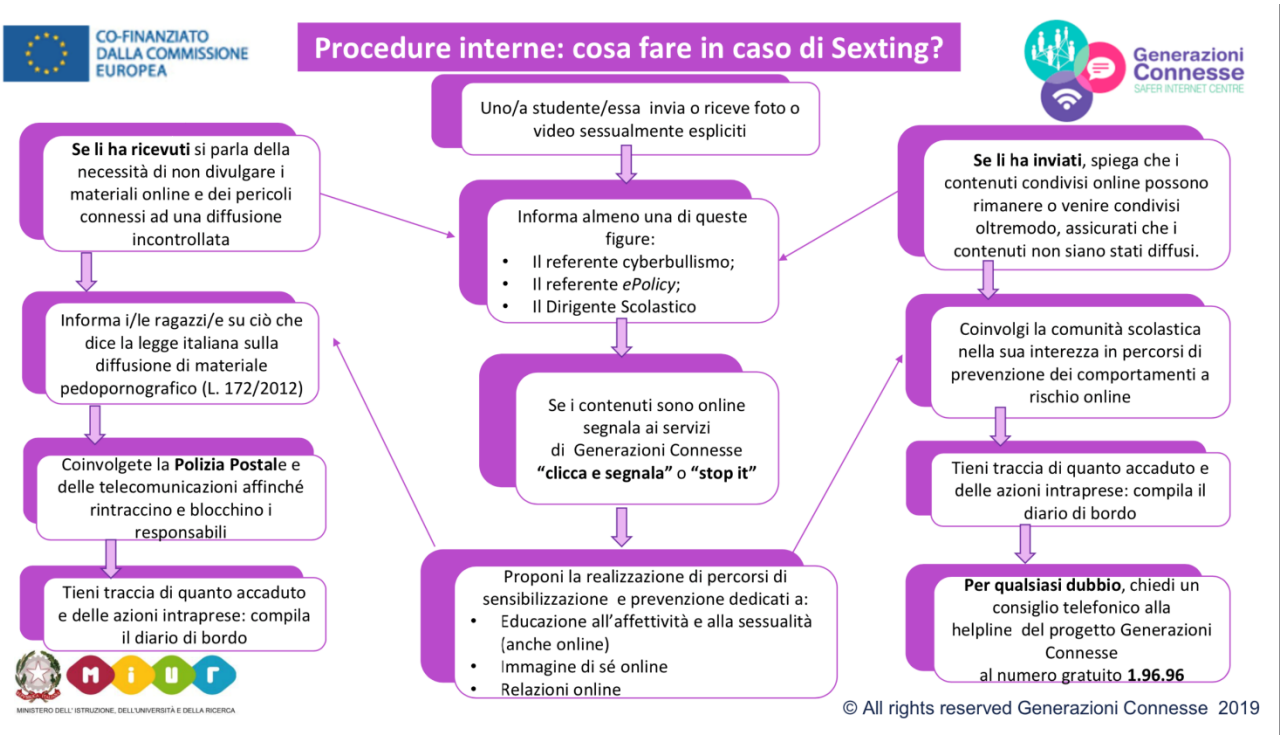
Nel caso B il docente deve condividere immediatamente quanto osservato con il referente per il bullismo e il cyberbullismo, valutando insieme le possibili strategie di intervento. Si avvisa anche il Dirigente Scolastico che convoca il consiglio di classe. Si informano i genitori (o chi esercita la responsabilità genitoriale) degli studenti direttamente coinvolti. E' possibile rivolgersi ai Servizi Sociali del Comune per condividere informazioni e strategie. E' necessario informare sia i genitori che gli studenti circa la possibilità di rimozione l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social.

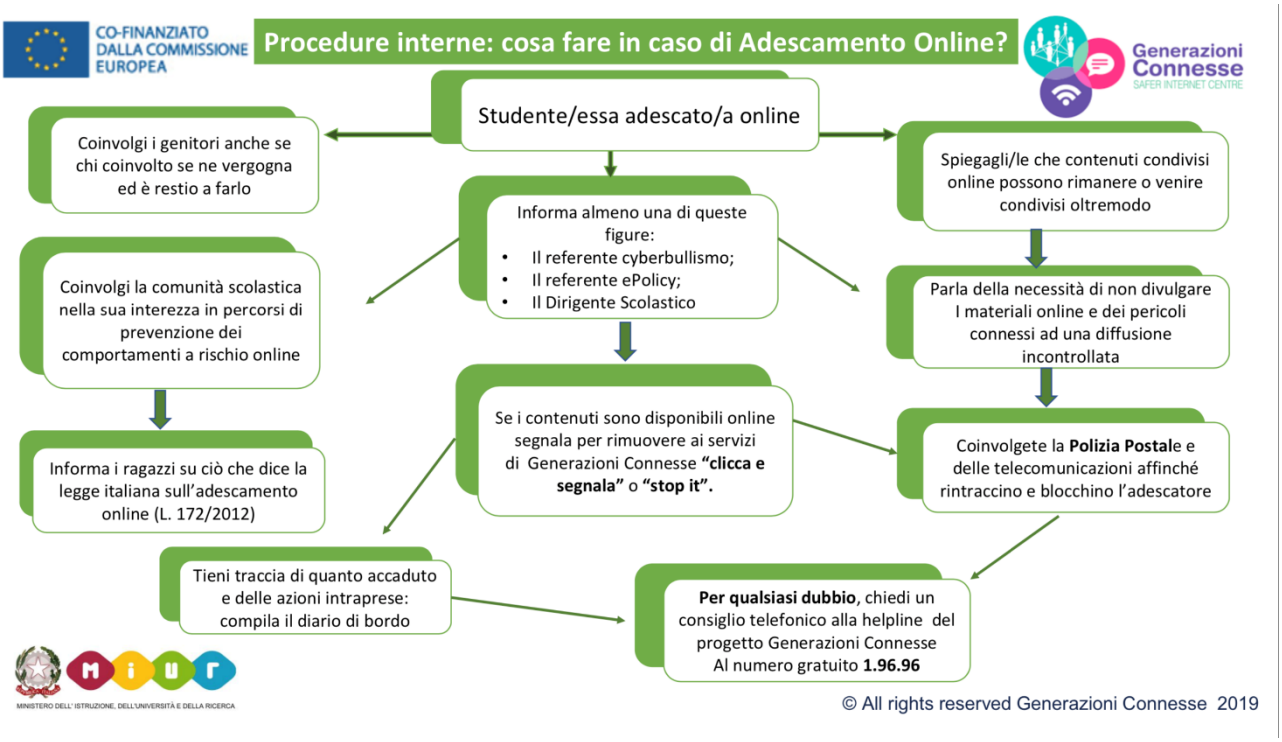
5.3. - Gli attori sul territorio

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.

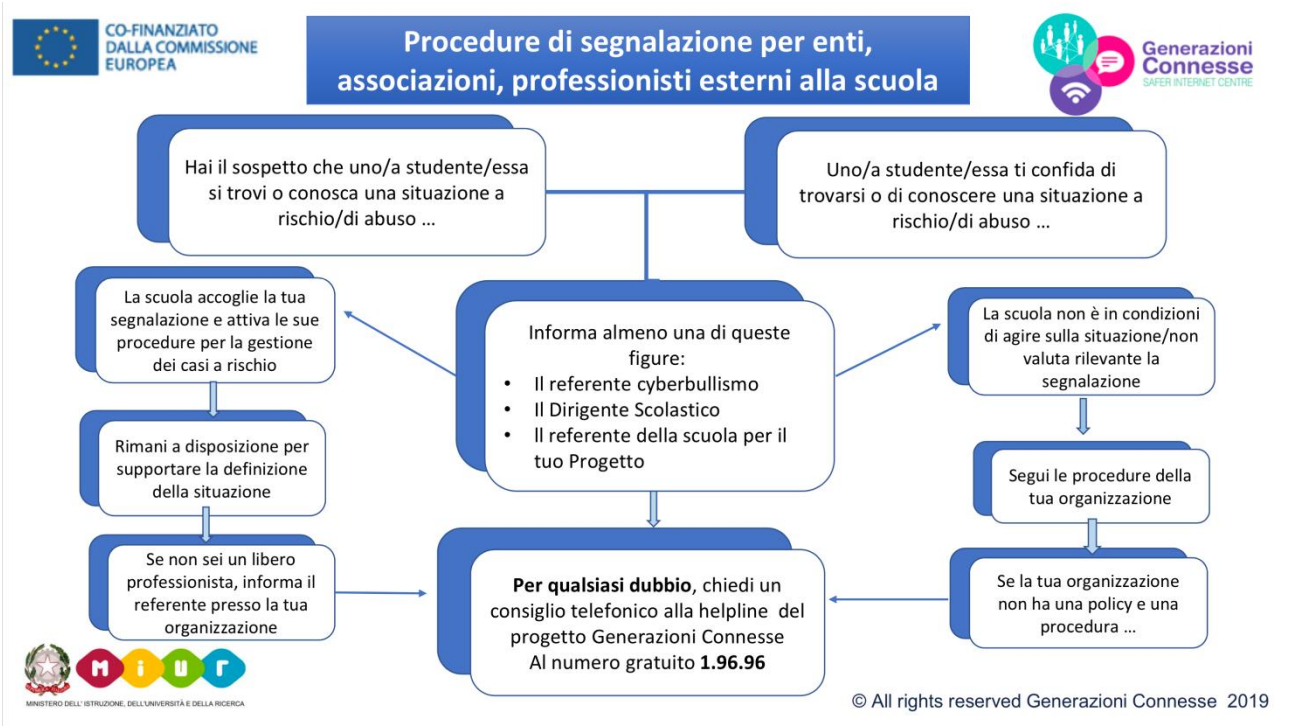
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare 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.


CO-FINANZIATO DALLA COMMISSIONE EUROPEA
Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola
Generazioni Connesse
SAFER INTERNET CENTRE
Hai il sospetto che uno/a studente/essa si trovi o conosca una situazione a rischio/di abuso …
Uno/a studente/essa ti confida di trovarsi o di conoscere una situazione a rischio/di abuso …
La scuola accoglie la tua segnalazione e attiva le sue procedure per la gestione dei casi a rischio
Rimani a disposizione per supportare la definizione della situazione
Se non sei un libero professionista, informa il referente presso la tua organizzazione
Informa almeno una di queste figure:
• Il referente cyberbullismo
• Il Dirigente Scolastico
• Il referente della scuola per il tuo Progetto
La scuola non è in condizioni di agire sulla situazione/non valuta rilevante la segnalazione
Segui le procedure della tua organizzazione
Se la tua organizzazione non ha una policy e una procedura …
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse Al numero gratuito 1.96.96
MINISTERO DELL' ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
© All rights reserved Generazioni Connesse 2019


CO-FINANZIATO DALLA COMMISSIONE EUROPEA
Procedure interne: cosa fare in caso di Sexting?
Generazioni Connesse
SAFER INTERNET CENTRE
Uno/a studente/essa invia o riceve foto o video sessualmente espliciti
Se li ha ricevuti si parla della necessità di non divulgare i materiali online e dei pericoli connessi ad una diffusione incontrollata
Informa i/le ragazzi/e su ciò che dice la legge italiana sulla diffusione di materiale pedopornografico (L. 172/2012)
Coinvolgete la Polizia Postale e delle telecomunicazioni affinché rintraccino e blocchino i responsabili
Tieni traccia di quanto accaduto e delle azioni intraprese: compila il diario di bordo
Informa almeno una di queste figure:
• Il referente cyberbullismo;
• Il referente ePolicy;
• Il Dirigente Scolastico
Se i contenuti sono online segnala ai servizi di Generazioni Connesse "clicca e segnala" o "stop it"
Proponi la realizzazione di percorsi di sensibilizzazione e prevenzione dedicati a:
• Educazione all'affettività e alla sessualità (anche online)
• Immagine di sé online
• Relazioni online
Se li ha inviati, spiega che i contenuti condivisi online possono rimanere o venire condivisi oltremodo, assicurati che i contenuti non siano stati diffusi.
Coinvolgi la comunità scolastica nella sua interezza in percorsi di prevenzione dei comportamenti a rischio online
Tieni traccia di quanto accaduto e delle azioni intraprese: compila il diario di bordo
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse al numero gratuito 1.96.96
MINISTERO DELL' ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
© All rights reserved Generazioni Connesse 2019



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
- https://www.iscobiassono.edu.it/bullismo-e-cyberbullismo/

Allegati dell’Istituto

- Privacy - Consenso immagini
- Privacy - Consenso generico
- Patto di corresponsabilità scuola Primaria
- Patto di corresponsabilità Scuola Secondaria
- Regolamento di disciplina scuola Primaria
- Regolamento di disciplina scuola Secondaria
- Piano Didattica Digitale
- Curriculum di Educazione Civica Primaria e Secondaria