Documento di ePolicy
ISTITUTO COMPRENSIVO DI ESINE

VIA CHIOSI N.4 - 25040 - ESINE
Brescia (BS) - Lombardia
Data di approvazione: 23/10/2024 - 14:14

Cap 1 - Lo scopo della ePolicy

1.1 Scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

1. Scopo dell'ePolicy
2. Ruoli e responsabilità nell'implementazione dell'ePolicy
3. Integrazione dell'ePolicy con regolamenti e normativa generale esistenti
4. Condivisione e comunicazione dell'ePolicy all'intera comunità educante
5. I piani di Azione dell'ePolicy

Capitolo 2 - Sensibilizzazione e prevenzione

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

1. Protezione dei dati personali e GDPR
2. Accesso ad Internet
3. Strumenti di comunicazione online (PUA)
4. Strumentazione personale (BYOD)

Capitolo 4 - Segnalazione e gestione dei casi

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

1.1 Scopo dell'ePolicy

(Questo paragrafo illustra lo scopo e gli obiettivi di questo documento programmatico per la cittadinanza digitale)

L' E-Policy ha come obiettivo principale quello di promuovere le competenze digitali per un uso delle tecnologie digitali positivo, critico e consapevole, da parte degli studenti e delle studentesse guidati dagli adulti coinvolti nel processo didattico-educativo.

La competenza digitale è una competenza chiave del cittadino europeo come indicato dal Consiglio Europeo (Raccomandazione del 2018) che permette ad ogni cittadino di esercitare i propri diritti all'interno degli ambienti digitali (ONU - Commento Generale 25: I diritti dei minori negli ambienti digitali).

L'ePolicy è un documento programmatico che permette di lavorare su quattro obiettivi:

1. Il piano di azioni triennale per promuovere nell'intera comunità scolastica l'uso sicuro responsabile e positivo della rete;
2. le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
3. le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
4. le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

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

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'ePolicy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati a un utilizzo scorretto degli strumenti.

Perché è importante dotarsi di una E-policy?

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

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

L'ePolicy è un documento programmatico elaborato nel primo quadrimestre dell'anno scolastico 2024/25, dai componenti del Team Antibullismo e dell'Emergenza composto dal Dirigente scolastico, dall'Animatore Digitale, dal Referente per il bullismo e il cyberbullismo, dai componenti del Team Digitale e da insegnanti che rappresentano ogni grado scolastico dell'Istituto: infanzia, primaria e secondaria di primo grado.

Esso mira a promuovere le competenze digitali e un uso delle tecnologie digitali positivo, critico e consapevole, sia da parte degli alunni/e che degli adulti coinvolti nel processo educativo.

L'Istituto Comprensivo di Esine, aderendo al progetto "Generazioni Connesse" promosso dal MIUR in collaborazione con l'Unione Europea, ha elaborato questo documento in conformità con le "Linee d'orientamento per la prevenzione e il contrasto dei fenomeni di Bullismo e Cyberbullismo del 2021 (D.M. 18/2021)" con l'obiettivo di educare e sensibilizzare tutta la comunità scolastica, alunni/e, insegnanti e genitori all'uso sicuro e consapevole di internet.

Si intende promuovere lo sviluppo della competenza digitale, che passa attraverso la conoscenza di procedure e competenze tecniche e di norme comportamentali, dettate da un uso consapevole e critico da parte degli alunni/e, delle tecnologie digitali e di internet. Lo scopo è di prevenire ed eventualmente rilevare e affrontare, situazioni derivanti da un uso pericoloso delle stesse. Il primo passo è informare gli alunni/e dei rischi cui si espongono nella navigazione in rete, mentre dal canto suo l'Istituto si attiva per limitare l'accesso a siti potenzialmente dannosi, i cui contenuti possano risultare illegali o inadeguati. Ai docenti spetta il ruolo di guidare le attività online a scuola, illustrare le regole di comportamento per la navigazione in rete anche a casa, informare gli alunni/e affinché imparino a usare consapevolmente i contenuti e i servizi della rete per conoscere gli effetti cognitivi, comportamentali delle sue potenzialità oltre alle informazioni utili a gestire gli strumenti tecnologici.

1.2 - ePolicy: ruoli e responsabilità nell'implementazione dell'ePolicy

- (In questo paragrafo vengono dettagliati ruoli e responsabilità nell'implementazione del documento all'interno dei contesti scolastici ivi inclusi rappresentanti genitori e studenti per secondaria II grado).

Affinché l'ePolicy 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 opportuno che nel documento vengano definiti con chiarezza ruoli, compiti e responsabilità di ciascuna delle figure all'interno dell'Istituto.

In questo paragrafo dell'ePolicy è importante specificare le figure professionali che, a vario titolo, si occupano di gestione e programmazione delle attività formative, didattiche ed educative dell'Istituto e tutte quelle figure appartenenti alla comunità educante.

IL DIRIGENTE SCOLASTICO

Il ruolo del Dirigente Scolastico nel promuovere l'uso consentito delle tecnologie digitali e di internet include i seguenti compiti:

- promuovere la cultura della sicurezza online e garantirla a tutti i membri della comunità scolastica, in linea con il quadro normativo di riferimento, le indicazioni del MIM, delle sue agenzie e attraverso il documento di ePolicy;
- promuovere la cultura della sicurezza online – anche attraverso il documento di ePolicy - integrandola ed inserendola nelle misure di sicurezza più generali dell'intero Istituto;
- ha la responsabilità di fornire sistemi per un uso sicuro delle TIC, internet, i suoi strumenti ed ambienti e deve garantire alla popolazione scolastica la sicurezza di navigazione tramite internet utilizzando adeguati sistemi informatici e filtri;
- ha la responsabilità della gestione dei dati e della sicurezza delle informazioni e garantisce che l'Istituto segue le pratiche migliori possibili nella gestione dei dati stessi;
- deve tutelare la scuola e garantire agli utenti la sicurezza di navigazione utilizzando adeguati sistemi informatici e servizi di filtri Internet;
- ha il compito di garantire a tutto il personale una formazione adeguata sulla sicurezza online per essere tutelato nell'esercizio del proprio ruolo educativo e non;
- deve essere a conoscenza delle procedure da seguire in caso di un grave incidente di sicurezza online;
- deve garantire adeguate valutazioni di rischio nell'usare strumenti e TIC, effettuate in modo che comunque quanto programmato possa soddisfare le istanze educative e didattiche dichiarate nel PTOF di Istituto;
- deve garantire l'esistenza di un sistema che assicuri il monitoraggio e il controllo interno della sicurezza online in collaborazione con le figure di sistema;
- deve essere a conoscenza ed attuare le procedure necessarie in caso di grave incidente di sicurezza online.

L'ANIMATORE DIGITALE E IL TEAM PER L'INNOVAZIONE DIGITALE

L'animatore digitale e il Team per l'Innovazione digitale sono co-responsabili, con il referente ePolicy, dell'attuazione dei

piani di azione in particolare in riferimento alla formazione dei docenti. Sono inoltre responsabili del controllo all'accesso da parte degli studenti delle Tic

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

Il referente cyberbullismo è co-responsabile, con il team ePolicy, dell'attuazione dei piani di azione e coordina le iniziative di prevenzione e contrasto del cyberbullismo.

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

In coerenza con le Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo del Ministero dell'Istruzione (D.M. n. 18 del 13/1/2021, agg. 2021 – nota prot. 482 del 18-02-2021), il Team ha le funzioni di coadiuvare il Dirigente Scolastico, coordinatore del Team nella scuola, nella definizione degli interventi di prevenzione e nella gestione dei casi di bullismo e cyberbullismo che si possono presentare. Promuove inoltre la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale e comunica ad alunni, famiglie e tutto il personale scolastico dell'esistenza del team, a cui poter fare riferimento per segnalazioni o richieste di informazioni sul tema.

Il Team ha il compito di:

- coadiuvare il Dirigente scolastico, coordinatore del Team, nella definizione degli interventi di prevenzione del bullismo (per questa funzione partecipano anche il presidente del Consiglio d'Istituto e i Rappresentanti degli studenti).
- Intervenire (come gruppo ristretto, composto da Dirigente e referente o referenti per il bullismo e il cyberbullismo, psicologo o pedagogista, se presente) nelle situazioni acute di bullismo.
- Promuovere la redazione e l'applicazione della ePolicy e monitorare le segnalazioni.

I/LE DOCENTI

I/le docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Possono, innanzitutto, integrare la propria disciplina con approfondimenti, promuovendo l'uso delle tecnologie digitali nella didattica. I docenti devono accompagnare e supportare gli/le studenti nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete. Inoltre, educano gli studenti alla prudenza, a non fornire dati ed informazioni personali, ad abbandonare un sito dai contenuti che possono turbare o spaventare e a non incontrare persone conosciute in Rete senza averne prima parlato con i genitori. Informano gli alunni sui rischi presenti in Rete, senza demonizzarla, ma sollecitandone un uso consapevole, in modo che Internet possa rimanere per bambini/e e ragazzi/e una fonte di divertimento e uno strumento di apprendimento.

I/le docenti osservano altresì regolarmente i comportamenti a rischio (sia dei potenziali bulli, sia delle potenziali vittime) e hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che veda coinvolti studenti e studentesse dandone tempestiva comunicazione al Dirigente Scolastico, al Referente per il Cyberbullismo e Bullismo e al Consiglio di Classe per definire strategie di intervento condivise.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Responsabile della protezione dei dati (RPD o DPO) conosce l'ePolicy di Istituto, fornisce la propria consulenza in merito agli obblighi derivanti dal GDPR e sorveglia sull'esatta osservanza della normativa in materia di tutela dei dati personali ed è co-responsabile delle azioni di informazione e formazione nell'Istituto sulla protezione dei dati personali

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

Il personale ATA, all'interno dei singoli regolamenti d'Istituto, è coinvolto nelle pratiche di prevenzione – ivi incluso il processo di definizione e implementazione dell'ePolicy di Istituto - ed è tenuto alla segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.

GLI STUDENTI E LE STUDENTESSE

Gli studenti e le studentesse devono, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti. Con il supporto della scuola dovrebbero imparare a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le. Affinché questo accada devono partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

I rappresentanti degli/delle studenti sono informati del documento di ePolicy e invitati a costruire i piani di azione, a partire dal secondo anno della secondaria di II grado,

I GENITORI/ADULTI DI RIFERIMENTO

I Genitori, in continuità con l'Istituto scolastico, sono attori partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile degli strumenti personali (pc, smartphone, etc). Come parte della comunità educante sono tenuti a relazionarsi in modo costruttivo con i/le docenti sulle linee educative che riguardano le TIC e la Rete e – ivi incluso il documento di ePolicy - comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet.

È estremamente importante che accettino e condividano quanto scritto nell'ePolicy d'Istituto e nel patto di corresponsabilità in un'ottica di collaborazione reciproca. Si promuove il coinvolgimento dei rappresentanti di genitori/adulti di riferimento all'interno del percorso di definizione e implementazione dell'ePolicy.

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

Enti esterni pubblici e privati, il mondo dell'associazionismo dovranno conformarsi alla politica della scuola riguardo all'uso consapevole delle TIC e della rete per la realizzazione di iniziative nelle scuole, finalizzate a promuovere un uso positivo e consapevole delle Tecnologie Digitali da parte dei più giovani, e/o finalizzate a prevenire e contrastare situazioni di rischio online e valutare la rispondenza delle proposte di attività di sensibilizzazione/formazione alle esigenze di qualità contenute nel documento di ePolicy. Dovranno inoltre promuovere comportamenti sicuri durante le attività che si svolgono con gli/le studenti e verificare di aver implementato una serie di misure volte a garantire la tutela dei minori nel caso di insorgenza di problematiche e ad assicurarne la tempestiva individuazione e presa in carico.

IL COLLEGIO DOCENTI

- promuove scelte didattiche ed educative, anche in collaborazione con altre scuole in rete, per la prevenzione del fenomeno.

IL CONSIGLIO DI CLASSE

- pianifica attività didattiche e/o integrative finalizzate al coinvolgimento attivo e collaborativo degli alunni/e e all'approfondimento di tematiche che favoriscano la riflessione e la presa di coscienza della necessità dei valori di convivenza civile;
- favorisce un clima collaborativo all'interno della classe e nelle relazioni con le famiglie propone progetti di educazione alla legalità e alla cittadinanza attiva.

DSGA

Il ruolo del DSGA include inoltre i seguenti compiti:

- vigilare sulla corretta applicazione della ePolicy da parte del personale ATA;
- suggerire modifiche e integrazioni alla ePolicy.

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).

L'Istituto predispone una informativa sintetica sull'ePolicy, comprensiva delle procedure di segnalazione, garantisce un migliore rapporto fiduciario fra scuola e famiglia, consente di distinguere i ruoli e le azioni da compiere e di attivare direttamente, a seconda della tipologia dei casi da segnalare, le autorità competenti collaborando con i servizi del territorio per la prevenzione e la gestione di quanto rilevato, in un'ottica di gestione condivisa degli interventi. È importante garantire che tutti i soggetti esterni che erogano attività in ambito scolastico siano sensibilizzati e resi consapevoli dei rischi online che possono correre gli alunni/e e dei comportamenti corretti che devono adottare a scuola.

Le organizzazioni/associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti e attività educative, dovranno prendere atto di quanto stilato nell'ePolicy del nostro Istituto e sottoscrivere un'informativa sintetica del documento in questione, presente nel contratto.

L'Istituto può richiedere agli attori esterni il casellario giudiziale come fattore ulteriormente protettivo verso i minori. L'obiettivo è quello di verificare l'esistenza (o meno) di condanne per alcuni reati previsti dal Codice Penale e nello specifico gli articoli 600-bis (prostituzione minorile), 600-ter (pornografia minorile), 600-quater (detenzione di materiale pornografico), 600-quinquies (iniziative turistiche volte allo sfruttamento della prostituzione minorile), 609-undecies (adescamento di minorenni), o l'irrogazione di sanzioni interdittive all'esercizio di attività che comportino contatti diretti e regolari con i minori.

All'interno della procedura disciplinare, che vale per qualsiasi comportamento contrario al Regolamento di Istituto, si inserisce una parte specifica per gli episodi di bullismo e cyberbullismo in base all'attuale normativa:

- attraverso la compilazione del modulo in formato cartaceo opportunamente predisposto, viene effettuata una segnalazione al Referente per il bullismo e il cyberbullismo che ne dà immediata comunicazione al Dirigente Scolastico, il quale valuta se ricorrono gli estremi per una denuncia; la segnalazione può essere anonima, ma va sempre riportata per iscritto anche se raccolta oralmente;
- nel caso in cui la segnalazione arrivi direttamente al Dirigente Scolastico, questi procederà come da prescrizioni normative;
- diverse ipotesi:
  - il fatto non costituisce reato o ipotizza un reato a querela di parte: il Dirigente Scolastico informa tempestivamente i soggetti esercenti la responsabilità genitoriale, ovvero i tutori dei minori coinvolti e attiva adeguate azioni di carattere educativo;
  - il Dirigente Scolastico ha notizia di reato: sporge subito denuncia per iscritto all'autorità giudiziaria (Questura, Carabinieri, ecc.), anche quando non sia individuata la persona alla quale il reato è attribuito (art. 331 cpp);
  - si evidenzia che sia la detenzione che la divulgazione di qualsiasi immagine di tipo sessuale o di esposizione di nudità (prodotto anche attraverso la pratica del "sexting") è considerato dalla legislazione vigente materiale pedopornografico; è, pertanto, necessario comunicarlo immediatamente al Dirigente Scolastico perché trasmetta la notizia tempestivamente, con relazione circostanziata, alla Polizia Postale o altra forza di Polizia.

Per quanto non espressamente indicato sui ruoli e sulle responsabilità delle figure presenti all'interno dell'Istituzione scolastica, si rimanda: all'art. 21, comma 8, Legge 15 marzo 1997, n. 59; all'art. 25 della Legge 30 marzo 2001, n. 165; al CCNL in vigore; al D.P.R. 8 marzo 1999, n. 275; alla Legge 13 luglio 2015, n. 107; al Piano Nazionale Scuola Digitale; a quanto stabilito in materia di culpa in vigilando, culpa in organizzando, culpa in educando.

Ricordiamo, inoltre, che esiste una corresponsabilità educativa e formativa che riguarda i genitori e la scuola nel percorso di crescita di alunni/e.

In particolare, il 2° comma dell'art. 2048 c.c. così recita: "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, invece, bisogna considerare: il 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"; il 1° comma dell'art. 2048 c.c. ai sensi del quale "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 a un profilo prettamente processuale anche in materia di bullismo e cyberbullismo, si può parlare di tre tipologie di "culpa":

- **culpa in vigilando**: concerne la mancata sorveglianza attiva da parte del docente responsabile verso il minore (così 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**: fa capo ai genitori i quali hanno instaurato una relazione educativa con il/la figlio/a, ritenuta inadeguata, insufficiente o comunque carente tale da metterlo/a nella situazione di poter recare danno a terzi.

1.3 Integrazione ePolicy nei documenti scolastici

(Il paragrafo spiega in che modo integrare il documento nel Regolamento dell'Istituto Scolastico da aggiornare con specifici riferimenti all'E-policy, così come nel RAV e all'interno del Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto).

La trasversalità dell'ePolicy rende necessaria una sua integrazione nell'ambito dei documenti che disciplinano il funzionamento dell'Istituto Scolastico.

Il Regolamento dell'Istituto scolastico, che rappresenta il principale punto di riferimento normativo, dovrà essere aggiornato in modo tale da dare contezza dell'adozione dell'ePolicy, e richiamare le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione in ambiente scolastico.

Anche il **Patto di Corresponsabilità educativa** tra scuola e famiglia dovrà essere integrato con gli opportuni riferimenti all'ePolicy, puntualizzando, da un lato l'impegno dell'Istituto ad organizzare eventi formativi/informativi a beneficio dei genitori, e dall'altro l'impegno di questi ultimi a partecipare in maniera proattiva a tali eventi.

Il **Piano Triennale dell'Offerta Formativa**, per la sua funzione di carta d'identità culturale e progettuale delle istituzioni scolastiche, nel quale si esplicita la progettazione curricolare, extracurricolare, educativa e organizzativa che le singole scuole adottano nell'ambito della loro autonomia, deve contenere anche le progettualità relative ad azioni media educative legate al percorso di ePolicy.

Così come il PTOF è il risultato di una consapevole concertazione fra le componenti delle istituzioni scolastiche (Dirigente Scolastico, docenti, alunni, genitori) e fra queste e il territorio, il patto di corresponsabilità rappresenta l'assunzione di responsabilità da parte di tutti coloro che svolgono un ruolo attivo nella Comunità educante.

Integrazione dell'ePolicy con Regolamenti esistenti

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

La ePolicy è coerente con quanto stabilito dalla Legge (Statuto delle studentesse e degli studenti della scuola secondaria DPR 24 giugno 1998 n. 249 modificato dal DPR 21 novembre 2007 n. 235; Legge 29 maggio 2017 n. 71 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo" novellata dalla legge 70 del 17 maggio 2024 "Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e cyberbullismo", in vigore dal 14 giugno 2024; Legge 31 dicembre 1996 n. 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali").

La ePolicy è coerente con quanto stabilito nei Regolamenti vigenti e nel Patto di Corresponsabilità, si integra pienamente con obiettivi e contenuti dei seguenti documenti, che specificano il contesto di attuazione delle politiche dell'Istituto Comprensivo per un uso efficace e consapevole del digitale nella didattica:

- PTOF, incluso il piano per l'attuazione del PNSD;
- Regolamento interno di Istituto;
- Regolamento per la DDI e relative Netiquette;
- Curricolo Digitale di Istituto.

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.

Il nostro Istituto Scolastico ritiene importante promuovere iniziative educative di sensibilizzazione, conoscenza e prevenzione, allo scopo di promuovere una maggiore consapevolezza circa l'utilizzo delle TIC e di internet e i rischi connessi.

È opportuno, inoltre, valutare la natura e la gravità di quanto accaduto, al fine di considerare la necessità di denunciare l'episodio (con il coinvolgimento ad es. della Polizia Postale) o di garantire immediato supporto psicologico all'alunno/a attraverso i servizi predisposti, qualora ciò fosse necessario.

Disciplina degli alunni/e

Sono oggetto di condotte sanzionabili, in relazione all'uso improprio delle TIC, dei dispositivi e della Rete a scuola da parte degli alunni/e, fermo restando il Regolamento d'Istituto:

- l'uso della RETE per giudicare, infastidire, offendere, denigrare, impedire a qualcuno di esprimersi o partecipare, esprimersi in modo volgare usando il turpiloquio;
- la condivisione incauta o senza permesso di foto o altri dati personali (indirizzo di casa, numero di telefono);
- la condivisione online di immagini o video di compagni/e e personale scolastico senza il loro esplicito consenso o che li ritraggono in pose offensive e denigratorie;
- la condivisione di scatti intimi e a sfondo sessuale;
- l'invio di immagini o video, volti all'esclusione di compagni/e;
- la comunicazione incauta e senza permesso con sconosciuti;
- il collegamento a siti web non adeguati e/o indicati e, dunque, non autorizzati dai docenti durante attività laboratoriali di qualsiasi genere.

L'azione educativa prevista per gli alunni/e è rapportata alla fascia di età e al livello di sviluppo e maturazione personale. Infatti in alcuni casi i comportamenti sanzionabili sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, di cui gli educatori devono tenere conto per il raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno/a.

Pertanto sono previsti interventi graduali in base all'età e alla gravità delle violazioni:

- richiamo verbale;
- richiamo verbale con particolari conseguenze;
- sanzioni estemporanee commisurate alla violazione commessa;
- richiamo scritto con annotazione sul diario e sul Registro Elettronico;
- convocazione dei genitori da parte dell'insegnante;
- convocazione dei genitori da parte del Dirigente Scolastico;
- rimozione temporanea dei diritti di accesso a internet;
- presa in custodia del dispositivo;
- sospensione con obbligo di frequenza;
- allontanamento temporaneo dalle lezioni;
- segnalazione alle autorità competenti.

Contestualmente sono previsti interventi educativi di rinforzo rispetto a comportamenti corretti e riparativi dei disagi causati,

di ri-definizione delle regole sociali di convivenza, di prevenzione e gestione positiva dei conflitti, di pro-socialità, di conoscenza e gestione delle emozioni.

E' inoltre importante intervenire su tutto il contesto classe con attività specifiche educative e di sensibilizzazione.

Disciplina del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono quelle potenzialmente atte a determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli allievi/e:

- utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni/e, estraneo all'attività di insegnamento o al proprio profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- utilizzo delle comunicazioni elettroniche con genitori e/o alunni/e non compatibile con il proprio ruolo professionale;
- trattamento dei dati personali e sensibili degli alunni/e, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- diffusione delle password assegnate e custodia incauta degli strumenti e degli accessi, di cui potrebbero approfittare terzi;
- vigilanza elusa dagli alunni/e, mancata o non attenta vigilanza, che potrebbe favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- insufficienti azioni di contrasto a terzi in situazioni critiche;
- carenza negli interventi correttivi o di sostegno ad alunni/e;
- mancata segnalazione al Dirigente Scolastico, all'Animatore Digitale e al Team di situazioni critiche.

Le infrazioni della ePolicy da parte del personale scolastico possono riguardare sia la mancata osservanza delle regole qui descritte sulla gestione della strumentazione, sia la mancata sorveglianza e pronto intervento nel caso di infrazione da parte degli alunni/e. Nel primo caso la gravità si valuta sull'esposizione al rischio procurata agli alunni/e, nel secondo caso sul danno per la non tempestiva attivazione delle azioni qui indicate. La gestione delle infrazioni in quest'ambito ricade nella disciplina contrattuale.

Il Dirigente Scolastico può disporre il controllo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola; può disporre la cancellazione di materiali non adeguati o non autorizzati dal sistema informatico della scuola, e se necessario ne conserva una copia per eventuali approfondimenti successivi.

Tutto il personale è tenuto a collaborare con il Dirigente Scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio dei procedimenti che possono avere carattere organizzativo-gestionale, disciplinare, amministrativo, penale, a seconda del tipo e della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

Disciplina dei genitori

In considerazione dell'età degli alunni/e e della loro dipendenza dagli adulti, anche talune condizioni e condotte dei genitori medesimi possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli allievi a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico.

Gli atteggiamenti da parte della famiglia meno favorevoli sono:

- la convinzione che se il proprio figlio/a rimane a casa a usare il computer è al sicuro e non corre rischi;
- una posizione del computer in una stanza o in postazione non visibile e controllabile dall'adulto;
- una piena autonomia concessa al proprio figlio/a nella navigazione sul web e nell'uso di cellulare o smartphone;
- un utilizzo del dispositivo digitale, cellulare e/o smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei a minori.

E' quindi dovere dei genitori supportare gli insegnanti e il personale scolastico nel riconoscimento e nella costruzione di azioni di contrasto efficaci contro i principali rischi rappresentati dalla navigazione in internet da parte dei minori. Nel caso di inadeguata vigilanza che comporti infrazioni da parte del minore, si prevedono interventi rapportati alla gravità dell'infrazione stessa, che vanno dalla semplice comunicazione del problema ai genitori, alla loro convocazione da parte degli insegnanti di classe o del Dirigente Scolastico.

I genitori degli alunni/e, pertanto, possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli/e, se dovessero risultare pericolosi per sé e/o dannosi per altri (culpa in educando e in vigilando).

Il Dirigente Scolastico:

- informa immediatamente e coinvolge i genitori (a eccezione che per i sospetti casi per i quali bisogna segnalare alle Forze dell'Ordine);
- nel caso di mancata collaborazione della famiglia o della sua inadeguatezza rispetto al caso, segnala il caso ai Servizi Sociali del Comune e/o alla Tutela Minori;
- organizza attività di formazione/informazione a favore della comunità scolastica;
- raccoglie le informazioni con l'apposito modulo e informa tempestivamente i genitori dei fatti;
- in presenza di un testimone e di un genitore in caso di alunno/a minore, procede a:
  - ascoltare i protagonisti dei fatti e i genitori al fine di acquisire testimonianze e versioni;
  - ricostruire i fatti alla luce di quanto emerso;
  - accogliere eventuali documenti o materiali utili anche scritti, consegnati alla scuola da interessati e controinteressati.

Per maggiori approfondimenti si rimanda a quanto riportato sul sito scolastico, alla sezione "Regolamento d'Istituto", ove sono presenti i vari Regolamenti che disciplinano l'Istituto Comprensivo di Esine e con essi anche quelli relativi alla concessione in uso dei dispositivi tecnologici, alla Didattica Digitale Integrata, alle Netiquette – regole di buona educazione per la DDI e all'utilizzo della piattaforma Google Workspace.

Procedure operative per la gestione delle infrazioni alla E-Safety Policy

Infrazioni lievi	**Sanzioni**	**Interventi educativi riparatori**	**Organo competente**
Collegamento a siti web non indicati dai docenti Utilizzare la rete per interessi privati e personali che esulano dalla didattica Scaricare file, video, musicali protetti da copyright	Richiamo verbale Annotazione sul Registro Elettronico Rapporto disciplinare sul Registro Elettronico	Riflessione sul comportamento che l'alunno/a ha adottato e sulle motivazioni che l'hanno determinate Richiesta di scuse verbali	Insegnante di classe
Infrazioni gravi	**Sanzioni**	**Interventi educativi riparatori**	**Organo competente**

		Riflessione sul comportamento che l'alunno/a ha adottato e sulle motivazioni che l'hanno determinato Richiesta di scuse pubbliche Produzione obbligatoria di un elaborato (da svolgere a casa in collaborazione coi genitori) sui fatti accaduti e riflessioni sulle conseguenza delle proprie azioni	Insegnante di classe Consiglio di Classe Referente per il bullismo e cyberbullismo Team Antibullismo e dell'Emergenza Dirigente Scolastico
Deridere, denigrare, umiliare, calunniare attraverso l'uso delle TIC	Comunicazione scritta alla famiglia sul Libretto Digitale Ammonimento del Dirigente Scolastico (se reiterate) Convocazione dei genitori		
Infrazioni gravi	**Sanzioni**	**Interventi educativi riparatori**	**Organo competente**
Non rispettare le regole d'accesso alle strumentazioni Non rispettare le regole d'accesso a internet Uso scorretto della strumentazione personale	Richiamo verbale Annotazione sul Registro Elettronico Comunicazione scritta alla famiglia sul Libretto Digitale Sequestro temporaneo della strumentazione utilizzata in modo scorretto e restituzione all'alunno/a al termine della giornata scolastica Sequestro temporaneo della strumentazione utilizzata in modo scorretto e restituzione al genitore al termine della giornata scolastica Convocazione dei genitori Sospensione dalle lezioni	Riflessione sul comportamento che l'alunno/a ha adottato e sulle motivazioni che l'hanno determinato Assegnazione di un lavoro in classe durante i momenti di riposo o a casa Assegnazione di un compito di rinforzo, da eseguirsi a casa, inerente l'attività svolta in classe al momento della mancanza disciplinare Studio delle regole di sicurezza non rispettate Studio e ricerca di danni conseguenti a episodi di violazione delle regole e presentazione relazione in classe Svolgimento di mansioni utili alla comunità scolastica	Insegnante di classe Consiglio di Classe Animatore Digitale Dirigente Scolastico Consiglio di Istituto
Infrazioni gravissime	**Sanzioni**	**Interventi educativi riparatori**	**Organo competente**

Isolare o emarginare attraverso l'uso delle TIC Non rispettare i diritti altrui in ambito di Cittadinanza digitale Minacciare attraverso l'uso delle TIC Attuare cyberstolking o altre forme di persecuzione e molestia attraverso l'uso delle TIC Pubblicare sui social network o inviare tramite messaggistica immagini, video o testi che: - siano offensivi della dignità personale violino le norme della Privacy - non siano rispettosi dei valori di uguaglianza e di pari opportunità - siano discriminanti (a sfondo etnico, religioso, sessuale...) - incoraggino, atteggiamenti di maschilismo o stereotipi di genere	Annotazione sul Registro Elettronico Ammonimento del Dirigente Scolastico Convocazione immediata dei genitori Sospensione dalle lezioni Segnalazione agli assistenti sociali (se reiterate) Segnalazione alle autorità competenti in caso di reati	Riflessione sul comportamento che l'alunno/a ha adottato e sulle motivazioni che l'hanno determinate Produzione obbligatoria di un elaborato (da svolgere a casa in collaborazione coi genitori) sui fatti accaduti e riflessioni sulle conseguenza delle proprie azioni Conversione della sospensione dalle lezioni con attività socialmente utili favorendo un reale e concreto confronto con i valori della solidarietà e l'assunzione di stili di comportamento positivo, che sviluppino la formazione di una coscienza responsabile e la crescita consapevole dei giovani	Insegnante di classe Consiglio di Classe Referente per il bullismo e cyberbullismo Team Antibullismo e dell'Emergenza Dirigente Scolastico Consiglio di Istituto Assistenti sociali Forze dell'Ordine

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

1. il curricolo sulle competenze digitali per la comunità educante (il DigComp2.2);
2. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative;
3. Come comunicare e condividere l'epolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

1. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative;

L'efficacia dell'ePolicy è direttamente proporzionale a livello di conoscenza e diffusione all'interno della comunità scolastica ivi comprese le famiglie. Il documento rappresenta il canale interno privilegiato per informare, responsabilizzare e collaborare sui temi della rete e delle tecnologie a scuola con l'intera comunità scolastica.

In tal senso, il documento è accompagnato da versioni, allegate e sintetiche, all'interno delle quali sono individuati gli elementi principali del documento; una versione è diretta agli studenti ed una è diretta alle famiglie con un linguaggio e una

presentazione dei contenuti adeguata, flessibile e chiara. La versione sintetica rivolta agli studenti è inserita all'interno delle attività didattiche dell'educazione alla cittadinanza mentre la versione per le famiglie è consegnata nel corso dei colloqui scuola-famiglia.

Il documento è altresì pubblicato sul sito della scuola ed inserito nel Patto di corresponsabilità.

2. Come comunicare e condividere l'ePolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

La presenza dell'ePolicy nell'Istituto scolastico è garanzia, per il territorio, della presenza di un presidio informato, sensibile e attento sulla rete e le tecnologie in relazione con i più giovani.

In questo senso l'Istituto può rappresentare per le Istituzioni del territorio, le aziende, e le realtà del Terzo Settore un luogo di confronto privilegiato e di sperimentazione per tutti coloro che intendono costruire progetti di cittadinanza digitale rivolte ai più giovani.

A tal fine l'adozione dell'ePolicy è comunicata all'USR di riferimento e al Municipio (servizi istruzione e servizi sociali) attraverso gli allegati sintetici progettati che indicano gli elementi del documento e le prospettive per la comunità.

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

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

- la pubblicazione del documento sul sito istituzionale della scuola sia in forma integrale che sintetica;
- il diario di Istituto nel quale vengono riportati il formato friendly dell'ePolicy e il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico.

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

L'Istituto Comprensivo di Esine si impegna a intraprendere una serie di azioni e iniziative per la condivisione e comunicazione all'intera comunità scolastica.

All'inizio del percorso scolastico di ogni ordine di scuola, la ePolicy verrà illustrata ai genitori e agli alunni/e insieme al Patto di Corresponsabilità Educativa.

Si potranno prevedere inoltre:

- per i docenti:
  - la linea di condotta adottata dalla scuola in materia di sicurezza nell'utilizzo del digitale saranno discusse in tutti gli organi collegiali e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito web della scuola;
  - per proteggere tutto il personale e gli alunni/e, la scuola metterà in atto una linea di condotta di utilizzo controllata e limitata alle esigenze didattiche;
  - il personale docente sarà reso consapevole del fatto che il traffico in internet può essere monitorato e si potrà risalire al singolo utente registrato;

- il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC sarà supervisionato dall'Animatore Digitale, che segnalerà al DS/DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici;
- l'Animatore Digitale metterà in evidenza online utili strumenti, calibrati in funzione dell'età e delle capacità, che il personale potrà utilizzare con gli alunni/e in classe;
- tutto il personale è consapevole che una condotta non in linea con il Codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile;
- il personale scolastico riceverà un'adeguata formazione/informazione sull'uso sicuro e responsabile di internet attraverso materiali resi disponibili anche sul sito web della scuola;
- discussione e confronto in ambito collegiale sui contenuti, sulle pratiche indicate e su come declinare nel curricolo le tematiche d'interesse della ePolicy, per l'elaborazione di protocolli condivisi di intervento;

- per gli alunni/e:
  - lettura, comprensione e sottoscrizione del "Patto di Corresponsabilità";
  - diffusione tra gli alunni/e di un estratto del protocollo di ePolicy, tenendo in doveroso conto del grado scolastico di appartenenza e dell'età;
  - nel corso dell'anno i docenti potranno dedicare alcune lezioni alle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta contro il cyberbullismo;
  - gli alunni/e sono informati delle regole dell'utilizzo dei laboratori di informatica e dei dispositivi digitali in generale, e i docenti sono tenuti a farle rispettare, monitorando le postazioni e facendo un controllo periodico della cronologia di navigazione. Ogni alunno/a è responsabile del dispositivo digitale che ha utilizzato ed eventuali violazioni verranno sanzionate secondo il Regolamento d'Istituto;
- per i genitori:
  - lettura e comprensione del "Regolamento d'Istituto" e sottoscrizione del "Patto di Corresponsabilità";
  - organizzazione di incontri al fine di favorire un approccio collaborativo nel perseguimento della sicurezza nell'uso delle TIC e di internet;
  - l'Animatore Digitale fornirà suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di internet, mediante materiale informatico pubblicato sul sito web scolastico;
  - i docenti di classe forniranno eventuali indirizzi web relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni/e.

Riteniamo che nella comunicazione e condivisione dell'ePolicy sia importante valutare i vari target di riferimento (alunni/e, docenti, genitori, personale amministrativo, collaboratori scolastici etc.) individuando di conseguenza i linguaggi, le modalità e i canali di comunicazione e condivisione più adatti, definiti in itinere, per la predisposizione della versione child friendly del documento.

La ePolicy, redatta dal Team Antibullismo e dell'Emergenza e approvata dal Collegio Docenti e dal Consiglio di Istituto, sarà inserita all'interno del PTOF.

1.5 - I Piani di Azione dell'ePolicy

I piani di azione rappresentano il **programma triennale** di obiettivi che la scuola intende realizzare per promuovere la conoscenza delle regole e dei protocolli di intervento che sono stati adottati con il documento di ePolicy nella comunità

scolastica.

Nei Piani di Azione sono riportati **gli impegni e le responsabilità** che la scuola si assume per promuovere sui temi dell'educazione civica digitale e dell'utilizzo sicuro e consapevole delle tecnologie e della rete:

- la rilevazione dei bisogni
- le iniziative informative e formative,
- la formazione di docenti, studenti e studentesse, e famiglie,
- il monitoraggio e la valutazione delle azioni (laddove possibile, anche all'interno del RAV);

I Piani di Azione si distinguono tra standard, comuni ad ogni scuola che ha adottato l'ePolicy, e autoprodotti ovvero definiti dalla scuola sulla base del proprio contesto territoriale e delle collaborazioni in essere con Istituzioni, associazioni e aziende.

1° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

- Realizzare un evento di presentazione dell'ePolicy ai docenti dell'Istituto;
- Realizzare un evento di diffusione dell'ePolicy in occasione degli Open Day e/o in occasione del SID dell'Istituto dedicato alle famiglie ed a studenti/esse;
- Diffondere l'ePolicy negli ambienti scolastici, a studenti e studentesse, docenti e famiglie attraverso le versioni friendly dell'ePolicy;

MODULO II

- Effettuare una rilevazione del fabbisogno formativo dei docenti sui temi dell'educazione civica digitale;
- Effettuare una rilevazione di interessi, bisogni e comportamenti delle famiglie sull' uso positivo del digitale;
- Avviare l'introduzione dell kit didattico come metodo e risorsa di lavoro in alcune classi pilota;

MODULO III

- Integrare l'ePolicy (norme, regolamenti e procedure) nei documenti dell'Istituto;
- Aggiornare la Politica d'Uso Accettabile (PUA) della scuola ed il regolamento BYOD dell'Istituto;

MODULO IV

- Definizione, a partire da quanto definito nell'ePolicy, delle procedure di segnalazione anche con linguaggio child/youth friendly perché possano essere accessibili a studenti e studentesse;
- Realizzare una reportistica delle segnalazioni ricevute e dei relativi esiti.

2° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

- Realizzare una formazione rivolta ai docenti dell'Istituto, sulla base dei risultati della rilevazione svolta nel corso del

primo anno, anche attraverso il supporto di esperti/associazioni esterne o avvalendosi del percorso disponibile sul sito di Generazioni Connesse. La formazione deve coprire almeno il 60% del corpo docente.

MODULO II

- L'istituto utilizza il kit didattico come pratica metodologica e risorse a disposizione dei docenti per i percorsi di ECD attraverso la formazione specifica sviluppata per i docenti attraverso il sito di Generazioni Connesse;
- Effettuare una rilevazione di interessi, bisogni, comportamenti, abitudini di studenti e studentesse sui temi dell'educazione civica digitale;
- Realizzare una formazione rivolta agli studenti e alle studentesse attraverso il percorso previsto sulla piattaforma di Generazioni Connesse;
- Realizzare una formazione rivolta alle famiglie attraverso il percorso previsto sulla piattaforma di Generazioni Connesse

Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

L'aggiornamento e l'implementazione della ePolicy avverrà contestualmente al "Rapporto di Autovalutazione" sulla base dei casi problematici riscontrati e della loro gestione, eventualmente in caso di insorgenza di nuove necessità, ogni qualvolta si verifichino cambiamenti significativi nelle normative o nell'utilizzo delle nuove tecnologie digitali all'interno dell'Istituto. Il monitoraggio, la revisione, l'aggiornamento e l'implementazione dell'ePolicy saranno a carico del gruppo di lavoro che ha redatto il documento.

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

- Kit Didattico
- Area formazione (per docenti, famiglie, studenti/sse con ePolicy)
- Canale Youtube (webinar, video-stimolo, serie per target differenti)
- Canale TikTok
- Canale Instagram
- Canale Facebook

Cap 2 - Sensibilizzazione e prevenzione

2.1 - Sensibilizzazione e prevenzione

(Il capitolo raccoglie indicazioni su azioni formative per studenti/esse, famiglie e docenti con obiettivi a breve e lungo termine e riferimenti normativi (es legge 92 2019 su ECD). I rischi online andranno in appendice come glossario, sul sito come approfondimenti, sul kit didattico come attività.

La quotidianità in rete di ciascuno dei componenti della comunità scolastica - docenti, studenti e famiglie - deve essere caratterizzata da una consapevolezza critica delle caratteristiche degli ambienti e dei servizi online affiancata alle competenze per vivere al meglio il mondo connesso.

In questa direzione l'ePolicy è un documento che sviluppa azioni e interventi con l'obiettivo di raggiungere l'intera comunità scolastica e promuovere, ciascuno secondo il proprio ruolo, una cittadinanza digitale composta dalla conoscenza dei diritti in rete, dei rischi e delle opportunità per una partecipazione attiva e responsabile nella rete.

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 - Il Curricolo Digitale

Per realizzare questo obiettivo l'istituto utilizza le risorse messe a disposizione a livello nazionale e internazionale.

Il DigComp 2.2, framework europeo sulle competenze digitali, permette di costruire una cornice precisa in cui inquadrare i temi e le corrispondenti competenze da proporre nell' Istituto non solo per gli studenti.

Al suo interno vengono identificati alcuni temi sui quali è costruita una proposta specifica per le famiglie e gli studenti (formazione). Tale cornice trova poi sviluppo specifico, per gli studenti, nel curricolo di educazione alla Cittadinanza Digitale previsto dalla L. 92/2019. Il curricolo prende forma attorno all'ePolicy e le attività didattiche sono legate al documento ed alle scelte dell'Istituto al suo interno.

Nel curricolo va previsto in ogni classe un appuntamento didattico specifico, calibrato sull'età degli alunni, e l'utilizzo dei kit didattici per favorire da parte degli studenti una maggiore conoscenza e consapevolezza delle finalità del presente documento.

I regolamenti e le attività sviluppate sul tema della prevenzione presenti nell'ePolicy sono parte, costante ma non esclusiva, delle azioni di disseminazione e sensibilizzazione descritte ed attuate dall'Istituto.

Tenendo conto del Piano Scuola Digitale (PNSD), in particolar modo il paragrafo 4.2. "Competenze e contenuti", il Sillabo sull'Educazione Civica Digitale, il DigComp 2.1 e la Raccomandazione del Consiglio Europeo relativa alle competenze chiave per l'apprendimento permanente (C189/9, p. 9), l'Istituto Comprensivo di Esine si è dotato di un curricolo digitale che prevede il coinvolgimento di tutti gli alunni/e dell'Istituto della scuola dell'Infanzia, Primaria e Secondaria di primo grado.

La scuola fornisce agli alunni/e l'accesso alle TIC e alla rete, aiutandoli a maturare competenze e strumenti per una consapevole cittadinanza digitale.

E' importante ricordare che le competenze digitali richiamano diverse dimensioni sulle quali è possibile lavorare in classe, in un'ottica che integra la dimensione tecnologica con quella cognitiva ed etica:

- la dimensione tecnologica, inserita tra le otto competenze chiave a livello Europeo, prevede, oltre al raggiungimento delle abilità di base delle TIC, anche implicazioni cognitive e relazionali. E' importante far riflettere i più giovani sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana, onde evitare automatismi che abbiano conseguenze incerte, attraverso un'adeguata comprensione della "grammatica" dello strumento.
- La dimensione cognitiva, comprende abilità legate al trattamento dell'informazione. Fa riferimento alla capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità.
- La dimensione etica e sociale: la prima fa riferimento alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui, di usare le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri, comprendendo alcune tematiche attuali, dalla tutela della privacy al contrasto del fenomeno del cyberbullismo. La seconda pone l'accento sulle pratiche sociali e sullo sviluppo di particolari abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui doveri nei riguardi di coloro con cui comunichiamo online.

Dall'integrazione di queste dimensioni emerge un concetto di competenza digitale denso, che fa riferimento alla capacità di comprendere e sfruttare l'effettivo potenziale delle tecnologie come costruzione di conoscenza e di promozione della partecipazione e dell'inclusione. La competenza nell'uso consapevole, critico e creativo delle nuove tecnologie diventa quindi una componente fondamentale nell'ottica della Cittadinanza digitale, trasversale al curricolo scolastico di ogni alunno/a.

Competenze digitali declinate secondo le cinque aree del quadro di riferimento DIGCOM (Quadro comune di riferimento europeo per le competenze digitali):

1. INFORMAZIONE: identificare, localizzare, recuperare, conservare, organizzare e analizzare le informazioni digitali, giudicare la loro importanza e scopo;

2. COMUNICAZIONE: comunicare in ambienti digitali, condividere risorse attraverso strumenti online, collegarsi con gli altri e collaborare attraverso strumenti digitali, interagire e partecipare alle comunità e alle reti;

3. CREAZIONE DI CONTENUTI: creare e modificare nuovi contenuti (da elaborazione testi a immagini e video); integrare e rielaborare le conoscenze e i contenuti; produrre espressioni creative, contenuti media e programmare; conoscere e applicare i diritti di proprietà intellettuale e le licenze;

4. SICUREZZA: protezione personale, dei dati e dell'identità digitale, misure di sicurezza, uso sicuro e sostenibile;

5. PROBLEM-SOLVING: identificare i bisogni e le risorse digitali; valutare appropriati strumenti digitali secondo lo scopo o necessità; risolvere problemi concettuali attraverso i mezzi digitali; utilizzare creativamente le tecnologie; risolvere problemi tecnici; aggiornare la propria competenza.

2.3 - Il Kit Didattico

L'e-Policy prevede, a livello macro, un lavoro di lettura e d'intenti condivisi dall'intera comunità scolastica, a livello micro, invece, immagina che la singola classe lavori anche su tematiche direttamente collegate alla sicurezza in rete, ma complesse e di non immediata ricaduta nelle programmazioni scolastiche (etica e digitale, algoritmi, datafication). A tal fine si è progettato e predisposto del materiale che possa funzionare sia da attivatore, sia d'accompagnamento ai docenti e agli studenti nella fase più delicata ed incisiva del processo di prevenzione: la lezione in classe.

Pertanto, il progetto Generazioni Connesse, a supporto del lavoro dell'e-Policy ha previsto per i docenti e studenti di ogni segmento scolare un nuovo Kit Didattico che contiene materiali per le lezioni e per il proprio aggiornamento, a partire dalla scuola d'infanzia fino alla secondaria di secondo grado. Il Kit può essere usato nella sua interezza oppure può essere oggetto di selezione e scelta, sulla base di quanto fatto dal docente.

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

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

La professione docente è complessa e pertanto richiede competenze diverse e integrate, fra queste anche quelle di tipo digitale. Le TIC, infatti, dovrebbero essere usate dagli insegnanti per l'integrazione della didattica al fine di progettare, sviluppare, utilizzare, gestire e valutare i processi di insegnamento e apprendimento di tutti gli alunni/e della classe.

Di conseguenza la competenza digitale, oggi, è imprescindibile per i docenti così come per alunni/e 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.

Pertanto l'Istituto riconosce e favorisce la partecipazione del personale a iniziative promosse sia direttamente dalla scuola, dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti (anche online).

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 può avvenire tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

La scuola, nelle persone del Dirigente Scolastico, del Referente del bullismo/cyberbullismo, dell'Animatore Digitale e dei componenti del Team Digitale, promuove all'interno degli organi collegiali, momenti di confronto e condivisione finalizzati a mettere a disposizione di tutto il corpo docente conoscenze e competenze acquisite dai singoli partecipanti nei diversi corsi. In presenza di appositi fondi la scuola si impegna altresì a organizzare percorsi formativi specifici.

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

Formare i docenti sulle tematiche in oggetto vuol dire non pensare esclusivamente all'alfabetizzazione ai media ma anche considerare la sfera emotiva e affettiva degli alunni/e che usano le nuove tecnologie. Essi, infatti, comunicano, esprimono se stessi e sviluppano l'identità personale e sociale, attraverso i dispositivi tecnologici che sempre di più consentono loro di poter entrare in contatto con il mondo che li circonda.

Prestare attenzione a questi aspetti significa dare loro gli strumenti per educarli alle emozioni in un contesto online e quindi modulare e gestire i propri e altrui comportamenti, favorendo e promuovendo forme di convivenza civile.

I momenti di formazione e aggiornamento sono pensati e creati a partire dall'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica; dall'analisi del fabbisogno conoscitivo circa particolari argomenti che i docenti sentono come più urgenti; dall'analisi delle richieste che provengono dagli alunni/e in modo da utilizzare (attraverso le modalità che il docente indica e ritiene più confacente alla classe) quanto appreso durante la formazione ricevuta.

Saranno previsti momenti formativi di approfondimento (progetti specifici, laboratori, eventi, giornate, etc, ...) con la famiglia e gli alunni/e in modo da sensibilizzare l'intera comunità educante sia sul corretto uso delle tecnologie digitali che sulle potenzialità della Rete.

Verrà elaborato un cronoprogramma che consideri il triennio scolastico, nell'ottica di una vera e propria programmazione con azioni specifiche:

- analizzare il fabbisogno formativo degli insegnanti sull'uso sicuro della Rete;
- promuovere la partecipazione dei docenti a corsi di formazione che abbiano in oggetto i temi del progetto Generazioni Connesse;
- monitorare le azioni svolte per mezzo di specifici momenti di valutazione;
- organizzare incontri con professionisti della scuola o con esperti esterni, enti, associazioni.

L'avvio del progetto Generazioni Connesse rappresenta una reale opportunità di rendere coesa e unitaria la formazione online sull'uso consapevole e sicuro della rete e delle tecnologie digitali, pertanto sono state predisposte aree apposite nel sito di Istituto dedicate alla condivisione di materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di internet (guide in pdf, video, manuali a fumetti, link a siti specializzati e contributi della Polizia Postale, del Co.Re.Com Lombardia, di Telefono Azzurro, dal sito "Generazioni connesse", ecc...), dove il personale scolastico, gli alunni/e e le famiglie potranno trovare materiali informativi per l'approfondimento personale e/o collettivo.

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.

Negli ultimi anni, con l'uso diffuso del Registro Elettronico, delle piattaforma elearning e della costante comunicazione tra la

commissione digitale, i docenti e le famiglie, sono stati elaborati e diffusi tutti i Regolamenti concernenti l'utilizzo della rete, delle tecnologie e i Regolamenti disciplinari con le sanzioni ammesse. Tutte le informazioni per i genitori sono pubblicate periodicamente sul sito della scuola e inviate tramite Registro Elettronico.

Gli alunni/e devono attenersi a quanto previsto dai Regolamenti scolastici e dalle Circolari interne emanate dal Dirigente Scolastico. I genitori, nell'azione di corresponsabilità didattico-educativa, rappresentano un punto di forza per l'implementazione dei rapporti "scuola-famiglia", quale garanzia e rispetto degli impegni, di natura anche pedagogica, sottoscritti e condivisi nello stesso Patto di Corresponsabilità, impegnandosi pertanto nell'accompagnare e supervisionare i figli/e durante la navigazione in rete.

La scuola sostiene i genitori organizzando incontri ed eventi sui temi dell'uso consapevole della rete e delle tecnologie dell'informazione, impegnandosi a mettere in atto azioni continue di consulenza, orientamento e formazione per i genitori, tra cui:

- presentare l'ePolicy di Istituto, al fine di far conoscere e divulgare i principi di comportamento sicuro online;
- informare l'utenza con e-mail, assemblee di classe, formazione specifica, pubblicazioni sul sito della scuola e divulgazione del Vademecum di Generazioni Connesse;
- organizzare incontri di consulenza con esperti;
- fornire informazioni sui siti nazionali di supporto per i genitori.

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

3.1 - Protezione dei dati personali e GDPR

La protezione dei dati personali delle persone fisiche costituisce un diritto fondamentale. L'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea e l'art. 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Le principali normative di riferimento sono il Regolamento Generale sulla Protezione dei Dati 2016/679 noto anche come GDPR, e il Dlgs 196/2003 conosciuto come Codice Privacy.

Il settore dell'istruzione è particolarmente impattato dalla tematica privacy in considerazione del fatto che gli Istituti Scolastici sono chiamati, necessariamente, a trattare un'enorme mole di dati personali.

Con l'entrata in vigore del GDPR è stato introdotto l'obbligo per ciascun Istituto scolastico di provvedere alla designazione di un Responsabile della protezione dei dati personali (RPD o DPO).

I principali obblighi in materia di protezione dei dati personali consistono nella definizione di un "organigramma privacy", nel rilascio dell'informativa al momento della raccolta dei dati e nella tenuta di un registro dei trattamenti.

"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. https://www.garanteprivacy.it/temi/scuola).

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

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

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

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i

soggetti coinvolti nel processo educativo, con particolare attenzione ai minori. A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali.

L'Istituto ospita alunni/e dai 3 ai 14 anni, per questo è fondamentale fare tutto il possibile per evitare che siano esposti a contenuti inappropriati. In fase di iscrizione degli alunni/e alla scuola i genitori sottoscrivono un'informativa sul trattamento dei dati personali in ottemperanza all'art. 13 D.Lgs 30 giugno 2003, n. 196 modificato dal D.Lgs 101 del 2018 (Codice in materia di protezione dei dati personali).

All'inizio di ogni anno scolastico i genitori rilasciano il consenso all'utilizzo di materiale fotografico e audiovisivo e all'esposizione degli elaborati degli alunni/e anche in sedi diverse da quelle dell'Istituto. I dati sensibili sono a esclusivo uso della dirigenza e della segreteria. I computer che contengono queste informazioni sono protetti da un ingresso con nome utente e password noti solo al personale preposto.

L'accesso ai dati riportati nel Registro Elettronico (ritardi, assenze, note e valutazioni) è riservato ai genitori dell'Istituto, tramite l'invio di una password di accesso strettamente personale.

All'interno dell'istituzione scolastica, il responsabile della gestione del trattamento dei dati personali è il Dirigente Scolastico, il quale indica nella persona del DSGA e nel personale amministrativo gli incaricati al trattamento dei dati.

La segreteria utilizza password nelle postazioni informatiche di lavoro, individua soggetti preposti alla gestione delle password, ha un codice identificativo personale per ogni utente, utilizza programmi antivirus, protegge e regolamenta gli accessi locali che ospitano le informazioni riservate o in cui si trovano le postazioni di lavoro che ne consentono l'accesso, definisce i criteri per garantire l'integrità e la trasmissione sicura dei dati e si dota di mezzi elettronici adeguati per impedire l'accesso dall'esterno alla propria rete.

Le fotografie e i video da pubblicare sul sito che includano gli alunni/e sono selezionati con cura e non permettono l'identificazione dei singoli attraverso l'indicazione del nome, a meno che non si tratti di eventi particolari per cui le famiglie potranno concedere opportuna autorizzazione.

Nella Guida del Garante per la protezione dei dati personali "La scuola a prova di privacy" sono specificate le linee guida da seguire riguardo il trattamento dei dati personali all'interno della comunità scolastica. Tutte le scuole hanno l'obbligo di far conoscere agli alunni/e, alle famiglie e ai docenti le modalità di trattamento dei loro dati personali. Ogni persona ha diritto di conoscere se sono conservate informazioni che la riguardano, di apprenderne il contenuto, di farle rettificare se erronee, incomplete o non aggiornate. Per esercitare questi diritti è possibile rivolgersi direttamente al "titolare del trattamento", anche tramite i suoi incaricati o responsabili del trattamento dei dati. Se non si ottiene risposta o se il riscontro non risulta adeguato è possibile rivolgersi al Garante o alla magistratura ordinaria.

L'accesso agli atti è regolato dall'amministrazione che deve valutare l'esistenza di presupposti normativi che permettano la presa visione o estratto/copia conforme dei documenti ai soggetti con un "interesse diretto, concreto e attuale" alla conoscibilità degli atti.

L'utilizzo del telefono cellulare e di apparecchi per la registrazione di suoni e immagini è disciplinato dal Regolamento di Istituto pubblicato sul sito della scuola. Nessun membro della comunità scolastica, in alcuna occasione (ad esempio, all'interno della scuola o durante un'uscita didattica), può diffondere o comunicare sistematicamente i dati di altre persone (ad esempio pubblicandoli su internet).

Le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici non violano la privacy. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare e non alla diffusione. Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su internet. In caso di comunicazione sistematica o diffusione diventa infatti necessario, di regola, ottenere il consenso scritto informato delle persone presenti nelle fotografie e nei video dei genitori (o di chi ne fa le veci) nel caso di minori.

Le scuole di ogni ordine e grado sono soggette a un regime di pubblicità e trasparenza. L'Istituto scolastico presta

particolare attenzione a non rendere accessibili informazioni che dovrebbero restare riservate o a mantenerle online oltre il tempo consentito.

Inoltre, la scuola non ha solo il compito di tutelare la privacy degli alunni/e e delle loro famiglie, ma anche quello di informare e rendere consapevoli gli alunni/e di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri.

Cosa sono i "dati personali"

I dati personali sono tutte quelle informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc.

Fra questi, particolarmente importanti sono:

- i dati che permettono l'identificazione diretta di una persona, come i dati anagrafici (ad es. nome e cognome);
- i dati che permettono l'identificazione indiretta di una persona, come un numero di identificazione (ad es. il codice fiscale, l'indirizzo IP, ...);
- i dati sensibili, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale e dati relativi alla salute o alla vita sessuale di una persona. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;
- i dati giudiziari, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti a iscrizione nel casellario giudiziale (ad es. i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto o obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) comprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
- altri dati personali che hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via internet o telefono) e quelli che consentono la geo-localizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti di una persona.

I protagonisti dei "dati personali"

- L'interessato è la persona fisica alla quale si riferiscono i dati personali (art. 4, paragrafo 1, punto 1 del Regolamento UE 2016/679);
- il titolare è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico, privato o l'associazione che adotta le decisioni sugli scopi e sulle modalità del trattamento (art. 4, paragrafo 1, punto 7 del Regolamento UE 2016/679);
- il responsabile è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo del trattamento dei dati (art. 4, paragrafo 1, punto 8 del Regolamento UE 2016/679). Il Regolamento medesimo ha introdotto la possibilità che un responsabile possa, a sua volta e secondo determinate condizioni, designare un altro soggetto c.d. sub-responsabile (art. 28, paragrafo 2).

Il trattamento dei "dati personali"

Trattamento è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o insiemi di dati personali.

Ad esempio: la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, par. 1, punto 2, del Regolamento (UE) 2016/679).

I soggetti che procedono al trattamento dei dati personali altrui devono adottare particolari misure per garantire il corretto e sicuro utilizzo dei dati.

Gli obblighi delle scuole in merito alla protezione dei "dati personali"

Le istituzioni scolastiche pubbliche possono trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali, oppure quelli espressamente previsti dalla normativa di settore.

In caso di violazione del trattamento dei dati la persona interessata può presentare al Garante per la Protezione dei dati personali un'apposita "segnalazione" gratuita o un "reclamo" (più circostanziato rispetto alla semplice segnalazione e con pagamento di diritti di segreteria).

Le scuole, sia pubbliche che private, hanno l'obbligo di informare tramite apposita informativa gli interessati delle caratteristiche e modalità del trattamento dei loro dati, indicando i responsabili del trattamento. Gli interessati non sono solo gli alunni/e, ma anche le famiglie e gli stessi docenti. È importante, inoltre, che le scuole verifichino i loro trattamenti, controllando se i dati siano eccedenti rispetto alle finalità perseguite.

Nel 2016 il Garante per la protezione dei dati personali ha pubblicato un utile vademecum "La scuola a prova di privacy" che offre agli insegnanti e ai dirigenti una guida per gestire correttamente le questioni legate alla diffusione e al trattamento dei dati personali degli alunni/e e delle famiglie. Il documento è stato elaborato prima dell'applicazione del Regolamento UE 679/2016, avvenuta il 25 maggio 2018, ma rimane un riferimento molto utile per aiutare docenti, famiglie, alunni/e e la stessa amministrazione scolastica a muoversi più agevolmente nel delicato mondo della protezione dei dati personali.

La liberatoria

La scuola non è tenuta a richiedere alle famiglie l'autorizzazione alle riprese fotografiche e video (ad es. in caso di gite scolastiche o recite) solo se esse sono realizzate a fini personali e non a fini di pubblicazione o divulgazione.

Famiglie e alunni/e hanno il diritto di conoscere quali informazioni sono trattate dall'Istituto scolastico, farle rettificare se inesatte, incomplete o non aggiornate.

3.2 - Strumenti di comunicazione online (PUA)

La Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) è un documento che racchiude una serie di regole legate all'utilizzo della rete a scuola e a casa da parte di studenti e di tutto il personale (compresi i professionisti esterni che lavorano in contesto scolastico), integrante il DPS (Documento programmatico sulla Sicurezza). Il documento, che funge da raccordo, si compone di punti strategici riguardanti non solo i vantaggi di internet a scuola ma anche i rischi connessi all'online, nella valutazione di quei contenuti presenti in rete e di quelle azioni negative che possono comprometterne l'uso positivo. Fra queste attività: ricercare materiale non consono allo stile educativo della scuola; produrre vere e proprie azioni illecite; giocare online con la rete scolastica; violare la privacy e i diritti d'autore, etc... Nella Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) vengono definite, dunque, le regole di utilizzo fra tutti gli attori in gioco, nel rispetto dei dati sensibili di ciascuno, in particolar modo degli alunni e delle alunne.

Accesso a 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.

Infrastruttura tecnologica dell'Istituto

La scuola è presente sulla rete con un portale web costantemente aggiornato contenente le informazioni utili per il personale scolastico e per le famiglie.

In ottemperanza alle leggi tutti i plessi dell'Istituto Comprensivo di Esine sono dotati di accesso alla Rete internet tramite wi-fi, rete protetta da password. E' possibile accedere alla rete da tutti i dispositivi digitali scolastici. I docenti e il personale ATA possono accedere alla rete anche con i propri dispositivi personali facendo richiesta della password di accesso al Referente informatico di plesso. L'accesso a internet degli alunni/e è ammesso in presenza del/i docente/i ed esclusivamente per motivi didattici. L'accesso è per tutti schermato da filtri che dal server impediscono il collegamento a siti appartenenti a black list o consentono il collegamento solo a siti idonei alla didattica, secondo le impostazioni date dall'amministrazione che periodicamente provvede alla manutenzione e aggiornamento del sistema informatico di Istituto, ove necessario richiedendo l'intervento di tecnici esterni.

Tutte le classi, laboratori, corridoi e spazi comuni sono dotati di accesso internet, di una rete wi-fi adeguata al numero di alunni/e, in grado di supportare il traffico dati generato da un numero elevato di utenti e permettere, ad esempio, l'uso di soluzioni cloud per la didattica e l'uso di contenuti di apprendimento multimediali.

Opportunità rese tali dal monitoraggio costante avvenuto negli anni, dalla partecipazione a bandi PON o europei, ma anche dalla collaborazione con le amministrazioni locali.

Per la DAD e la DDI si utilizza il Registro Elettronico al quale i docenti, gli alunni/e, i genitori accedono con credenziali personali, la piattaforma Google Workspace for Education tramite account istituzionale (.....@icesine.edu.it) e tutte le altre piattaforme in uso nell'Istituto. In essi è consentito caricare materiale didattico e scambiare messaggi tra docenti e alunni/e

e tra docenti e famiglie, ma il loro utilizzo è vincolato al possesso delle credenziali fornite dalla scuola e all'utilizzo della posta istituzionale.

Un ambiente sicuro anche online

In inglese esistono due termini per parlare di sicurezza:

- "**safety**": riguarda la prevenzione dei rischi, a partire dalla consapevolezza, conoscenza e preparazione per un uso consapevole delle tecnologie digitali (è questo l'approccio del progetto "Generazioni Connesse");
- "**security**" che, in relazione a internet e ai media, si riferisce a tutte quelle risorse tecnologiche che rendono sicuro l'ambiente digitale, dall'antivirus al firewall, da un protocollo di trasmissione dei dati sicuro (https) all'aggiornamento di software e sistemi operativi.

Il nostro Istituto Scolastico considera l'ambiente online alla stregua dell'ambiente fisico e ne valuta, quanto più possibile, tutti gli aspetti legati alla sicurezza.

In riferimento alla security, si presta attenzione non solo all'infrastruttura hardware e alla rete (wireless e non), ma si considera anche:

- la sicurezza di tutti gli aspetti che riguardano la gestione degli account degli utenti (in modo differenziato tra alunni/e, famiglie, insegnanti, personale scolastico/amministrativo);
- il filtraggio dei contenuti e gli aspetti legali in relazione prevalentemente alla privacy. L'accesso alla rete è protetto da apposito Firewall e l'Istituto conserva i log di accesso che verranno forniti, in caso di richiesta, alle Forze dell'Ordine.

Sono presenti reti separate per la segreteria e per la didattica. Le reti non comunicano tra loro al fine di garantire la riservatezza dei dati di segreteria.

Interventi tecnici

La scuola provvede a pianificare interventi periodici di manutenzione, segnalando eventuali problematiche riscontrate ai Referenti informatici di plesso e al Team Digitale, i quali provvedono tempestivamente a porre rimedio formando sul campo i docenti in difficoltà, permettendo loro, qualora le problematiche si ripresentino, di affrontare e risolvere in autonomia tutte quelle situazioni e casistiche di malfunzionamento dei dispositivi che si possono presentare nella quotidianità.

Le operazioni di gestione, configurazione, backup e ripristino sono affidate alla funzione strumentale e a risorse tecniche interne presenti nell'Istituto, affiancate a ditte esterne.

Il regolamento sull'uso delle tecnologie a scuola

L'accompagnamento da parte degli adulti è fondamentale nel percorso di crescita degli alunni per aiutarli a sviluppare le competenze digitali necessarie alla convivenza civile e al futuro lavorativo di alunni/e.

A tal proposito l'Istituto scolastico si è dotato di Regolamenti appositi che disciplinano la concessione in uso dei dispositivi tecnologici, la Didattica Digitale Integrata, le Netiquette – regole di buona educazione per la DDI, l'utilizzo della piattaforma Google Workspace for Education e del Registro Elettronico.

Il personale scolastico è tenuto a seguire le seguenti regole di accesso a internet:

- è possibile accedere a internet attraverso strumentazioni in dotazione all'Istituto;
- l'accesso a internet e la navigazione attraverso le strumentazioni scolastiche è riservato a un uso strettamente didattico;
- è possibile accedere ad account personali durante l'uso di internet, ma è obbligatorio il logout al termine;

- non è consentito il salvataggio di dati personali (nomi utenti, account e password) nei browser delle strumentazioni scolastiche;
- è vietato scaricare o installare da internet materiale potenzialmente dannoso, di provenienza non sicura o non legale.

Gli alunni/e sono tenuti a rispettare le seguenti regole di accesso a internet:

- è vietato l'accesso a internet senza autorizzazione da parte del personale docente;
- è vietata la navigazione in assenza del docente;
- l'accesso a internet e la navigazione attraverso le strumentazioni scolastiche è riservato a un uso strettamente didattico e nel rispetto di diritti della cittadinanza digitale e delle norme vigenti di utilizzo legale della rete;
- è vietato il salvataggio di dati personali (nomi utenti, account e password) nei browser delle strumentazioni scolastiche;
- è vietato scaricare da internet materiale senza l'autorizzazione del docente.

Tutti gli operatori presenti a qualsiasi titolo nella scuola (esperti esterni, collaboratori, ditte esterne...) dovranno attenersi alle regole generali previste per il personale.

Checklist per la cybersecurity

- **Reti separate di didattica e segreteria**: importante per garantire maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le reti grazie al firewall.
- **Aggiornamento periodico di software e Sistema Operativo**: garantire che il sistema sia aggiornato lo protegge dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo.
- **Programmazione di backup periodici**: copiare e mettere in sicurezza i dati del sistema scolastico per prevenire la perdita degli stessi.
- **Formazione adeguata al personale scolastico**: la formazione deve riguardare in particolare la gestione dei dispositivi e la conoscenza delle regole basilari sulla sicurezza.
- **Disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo**: prevedere l'accesso ai dispositivi tramite inserimento di password, anche in seguito a stand-by, per evitare il rischio potenziale di accesso da parte di persone non autorizzate.
- **Indicazioni sulle password:**
  - sensibilizzare rispetto all'uso di password difficilmente identificabili;
  - non memorizzare le password nei dispositivi scolastici;
  - non condividere le password con nessuno.

3.3 - BYOD

La presente ePolicy conterrà 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 infatti 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.

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.

I dispositivi digitali dell'Istituto sono monitorati e tenuti aggiornati dai docenti di riferimento affiancati da tecnici esterni specializzati.

In tutti i plessi è stato attivato un firewall di Istituto per bloccare l'accesso a siti e contenuti inappropriati per il contesto scolastico.

La connessione alla rete wi-fi d'Istituto è accessibile solo in seguito all'inserimento di una password comune.

I dispositivi digitali a disposizione degli insegnanti sono protetti da password di accesso, a tutela dei dati sensibili, mentre i computer destinati agli alunni/e sono privi di password e vengono utilizzati esclusivamente sotto la supervisione di un insegnante.

Strumenti di comunicazione online utilizzati a scuola

Fra gli strumenti di comunicazione troviamo:

1. il sito web della scuola raggiungibile all'indirizzo (www.icesine.edu.it), utilizzato per fornire informazioni di servizio rivolte ad alunni/e e genitori a integrazione delle comunicazioni, circolari e avvisi trasmessi mediante il Registro Elettronico e per trasmettere all'esterno l'identità, i valori, le azioni, i progetti e l'idea di educazione che l'Istituto porta avanti;
2. il Registro Elettronico con tutte le sue funzionalità: utilizzato per facilitare e rendere più partecipata la didattica e la comunicazione scuola-famiglia;
3. la piattaforma Google Workspace for Education, con le sue app incluse: e-mail, drive, meet, classroom, etc. A ogni docente e alunno/a è assegnato un indirizzo e-mail istituzionale (……@icesine.edu.it) utilizzato per scopi didattici.

La sicurezza e la privacy, nonché le prerogative di accesso, sono garantite mediante password individuali, generate da un'apposita procedura interna e comunicate ai destinatari a mezzo posta elettronica o cartacea, in presenza.

Ogni utente è responsabile delle proprie credenziali (username e password); in caso di smarrimento o dimenticanza è necessario compilare l'apposito modulo presente nel sito d'Istituto.

Si sollecita la custodia responsabile di tutte le credenziali personali.

In riferimento all'uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne è importante ricordare quello che si può definire "diritto alla disconnessione". L'art. 22 (Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola) del CCNL 2016/2018, infatti, fa riferimento ai criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione tra vita lavorativa e vita familiare.

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.

Di seguito sono analizzate le disposizioni ministeriali e infine le strategie che sono state messe in atto in classe con consapevolezza e responsabilità anche alla luce del quadro normativo e di indirizzo di riferimento.

Nel DPR 24 giugno 1998, n. 249 “Regolamento recante lo Statuto delle studentesse e degli studenti della scuola secondaria” (in GU 29 luglio 1998, n. 175), all’art. 2 (sezione Diritti), punto 8 lettera e si sottolinea “la disponibilità di un’adeguata strumentazione tecnologica” di cui la scuola deve dotarsi per offrirla ai propri alunni/e che, d’altra parte, “sono tenuti ad avere nei confronti del Dirigente Scolastico d'Istituto, dei docenti, del personale tutto della scuola e dei loro compagni/e lo stesso rispetto che chiedono per se stessi” (Art. 3, punto 2 sezione Doveri).

Più specificatamente, è nel Decreto del Presidente della Repubblica 21 Novembre 2007, n. 235 “Regolamento recante modifiche e integrazioni al decreto del Presidente della Repubblica 24 giugno 1998, n. 249”, concernente lo statuto degli alunni/e della scuola secondaria, che si introduce il Patto Educativo di Corresponsabilità e giornata della scuola (Art. 3) che definisce, attribuendole, le responsabilità fra istituzione scolastica e famiglia. Oggi, il Patto va letto anche in riferimento all’educazione degli alunni/e all’uso dei nuovi dispositivi tecnologici, inclusi tablet e smartphone sia a scuola che a casa.

All’interno di tale cornice normativa, si inserisce la circolare n° 362 del 25 agosto 1998 “Uso del telefono cellulare nelle scuole” che ha come oggetto particolare l’uso del cellulare a scuola da parte dei docenti anche durante le ore di lezione. La circolare contiene tali orientamenti: “è chiaro che tali comportamenti - laddove si verifichino - non possono essere consentiti in quanto si traducono in una mancanza di rispetto nei confronti degli alunni/e e recano un obiettivo elemento di disturbo al corretto svolgimento delle ore di lezione che, per legge, devono essere dedicate interamente all’attività di insegnamento e non possono essere utilizzate - sia pure parzialmente - per attività personali dei docenti”. Un orientamento, dunque, volto a punire l’uso personale del dispositivo solo per il corpo docente.

La DM n. 30 del 15/03/2007 “Linee di indirizzo e indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l’attività didattica, irrogazione di sanzioni disciplinari, doveri di vigilanza e di corresponsabilità dei genitori e dei docenti”, invece, si concentra su più elementi che interessano, questa volta, anche gli alunni/e in un’ottica non punitiva ma risarcitoria e riparatoria.

Per ciò che concerne la gestione degli strumenti personali (cellulari, tablet, pc) da parte di alunni/e, docenti, personale scolastico e ogni altro operatore presente a qualsiasi titolo nella scuola si fa riferimento a quanto riportato nel Patto di Corresponsabilità e nei Regolamenti di Istituto.

Cap 4 - Segnalazione e gestione dei casi

4.1 - Cosa Segnalare

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. Queste, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola.

Nelle procedure sono indicate le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso, nonché le modalità di coinvolgimento del Dirigente Scolastico e del Referente per il contrasto al bullismo e al cyberbullismo. 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. La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

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

Cyberbullismo: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).

Adescamento online: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

Sexting: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere, per quanto possibile, la rimozione del materiale on-line e il blocco della sua diffusione per mezzo dei 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.

Nel nostro Istituto è stato individuato un docente Referente per il contrasto al bullismo e al cyberbullismo che in collaborazione ai membri del Team Antibullismo e dell'emergenza e il Dirigente Scolastico si occupa di sostenere gli altri docenti nelle attività di prevenzione e di monitoraggio. I docenti del Team unitamente all'Animatore Digitale hanno seguito un percorso di formazione specifico su varie piattaforme, tra le quali Generazioni Connesse e Piattaforma Elisa.

Il personale docente del nostro Istituto, qualora abbia il sospetto o la certezza che un alunno/a possa essere vittima o responsabile di una situazione di bullismo o cyberbullismo, sexting o adescamento online, è tenuto, in particolare, a segnalare casi in cui viene a conoscenza dei seguenti fatti:

- **violenza** fisica, psicologica o intimidazione del gruppo, specie se reiterata;
- **intenzione** di nuocere;
- **isolamento** della vittima;
- **flaming**: litigi online nei quali si fa uso di un linguaggio violento e volgare;
- **harassment**: molestie attuate attraverso l'invio ripetuto di linguaggi offensivi;
- **cyberstalking**: invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità;
- **denigrazione**: pubblicazione all'interno di comunità virtuali, quali newsgroup, blog, forum di discussione, messaggistica immediata, siti internet, ecc., di pettegolezzi e commenti crudeli, calunniosi e denigratori. Sparlare di qualcuno per danneggiare gratuitamente e con cattiveria la sua reputazione;
- **outing estorto**: registrazione di confidenze – raccolte all'interno di un ambiente privato - creando un clima di fiducia e poi inserite integralmente in un blog pubblico;
- **trickery**: spinta, attraverso l'inganno, a rivelare informazioni imbarazzanti e riservate per renderle poi pubbliche in rete;
- **impersonificazione**: insinuazione all'interno dell'account di un'altra persona con l'obiettivo di inviare dal medesimo messaggi ingiuriosi che screditino la vittima;
- **esclusione**: estromissione intenzionale dall'attività di un gruppo online;
- **happy slapping**: ripresa, con il videotelefono, macchina fotografica o videocamera, di scene violente al fine di mostrarle ad amici o di diffonderle in Rete;
- **exposure**: pubblicare informazioni private e/o imbarazzanti su un'altra persona;
- **sexting**: invio di messaggi via smartphone e internet, corredati da immagini a sfondo sessuale.

Gli alunni/e possono mostrare segni di tristezza, ansia o risentimento nei confronti di compagni/e o di altri e riferire spontaneamente o su richiesta l'accaduto ai docenti, ma i minori potrebbero, confrontandosi periodicamente con i docenti sui rischi delle comunicazioni online, anche riferire fatti o eventi personali o altrui, accaduti anche al di fuori dell'ambito scolastico, che potrebbero mettere in allarme il docente.

Una "prova" di quanto riferito può essere presente nella memoria degli strumenti tecnologici utilizzati, può essere mostrata spontaneamente dall'alunno/a, può essere presentata da un reclamo dei genitori, può essere notata dall'insegnante che si accorge dell'infrazione in corso. Il docente è autorizzato a controllare le strumentazioni della scuola, mentre per controllare l'uso del telefono cellulare di un alunno/a, egli si rivolge al genitore.

Pertanto i contenuti "pericolosi" comunicati/ricevuti a/da altri, messi/scaricati in rete, ovvero le tracce che possono comprovare l'utilizzo incauto, scorretto o criminoso degli strumenti digitali utilizzabili anche a scuola attualmente dai minori (l'eventuale smartphone personale e il pc collegato a internet) per gli alunni/e, da segnalare dovranno essere riportati su apposita scheda (allegata al paragrafo 3) sono:

- contenuti afferenti la violazione della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati etc.);
- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto etc.);
- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia etc.).

La gestione dei casi rilevati verrà differenziata a seconda della loro gravità.

Si rinvia al "Protocollo intervento gestione emergenza bullismo e cyberbullismo".

Alcuni avvenimenti di lieve rilevanza (ad esempio silenziare il microfono del compagno/a durante una videolezione o estrometterlo dalla stessa) possono essere affrontati e risolti con la discussione collettiva in classe.

Altri casi di rilevanza maggiore (ad esempio insulti occasionali in chat, invio di immagini improprie) verranno segnalati al Referente del bullismo e cyberbullismo e poi al Dirigente Scolastico, il quale potrà affrontarli convocando genitori e alunni/e, alla presenza di tutti gli attori in campo, per riflettere insieme sull' accaduto e individuare strategie comuni d'intervento.

Nei casi più gravi (ad esempio sexting, grooming) e in ogni ipotesi di reato, occorre valutare tempestivamente con il Dirigente Scolastico come intervenire, convocando con urgenza i genitori. Tutte le segnalazioni dei docenti devono essere messe a verbale e protocollate.

Sensibilizzazione e Prevenzione

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

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

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

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

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

rischi per la sicurezza di bambine/i e ragazze/i.

La diffusione delle tecnologie digitali e dell'accesso alla Rete già nei primissimi anni di vita sta portando profondi cambiamenti nelle dinamiche relazionali e in quelle identitarie, trasformando linguaggi, modalità di comunicazione, abitudini e stili di vita e offrendo inedite potenzialità di crescita.

Se, dunque, le Tecnologie dell'Informazione e della Comunicazione (TIC) sono parte integrante della vita quotidiana dei più giovani, in quanto strumenti privilegiati di comunicazione e di relazione, ma anche di informazione, studio, creatività e partecipazione, esse pongono però delle questioni associate alla "sicurezza" e al comportamento sociale. Non bisogna, infatti, cadere nello stereotipo di una categoria uniforme di bambini/e e adolescenti "competenti", sollevando gli adulti dal proprio ruolo educativo e dalla responsabilità di promuovere presso i più giovani un uso consapevole e quindi anche un uso integrativo (e non sostitutivo) delle tecnologie digitali. Siamo di fronte a una realtà complessa, pensata prevalentemente per un mondo adulto e nella quale trovano spazio contenuti e comportamenti potenzialmente dannosi.

I rischi online rappresentano tutte quelle situazioni problematiche derivanti da un uso non consapevole e non responsabile delle tecnologie digitali da parte di bambini/e, ragazzi/e: adescamento online, cyberbullismo, sexting, violazione della privacy, pornografia, pedopornografia, gioco d'azzardo o gambling, internet addiction, videogiochi online, esposizione a contenuti dannosi o inadeguati (es. contenuti razzisti, che inneggiano al suicidio, che promuovono comportamenti alimentari scorretti, etc.), etc.

Partendo da questo punto di vista, vanno promosse nei più giovani le necessarie competenze e capacità, al fine di una protezione adeguata, ma anche al fine di un utilizzo consapevole che sappia sfruttare le potenzialità delle tecnologie digitali e gestirne le implicazioni.

A tal proposito i docenti dell'Istituto si formano per coinvolgere e avviare gli alunni/e verso le buone pratiche dell'uso consapevole della Rete e degli strumenti digitali, rendendoli consapevoli dei rischi e i pericoli di comportamenti e atteggiamenti non corretti sia nella Rete che nella quotidianità.

I genitori devono impegnarsi nel prendere visione della e-Safety Policy e nel seguire le azioni promosse dalla scuola per l'utilizzo consapevole della rete.

Gli alunni/e devono rispettare i Regolamenti e partecipare attivamente alle occasioni di confronto sul tema organizzate dalla scuola.

In presenza di appositi fondi la scuola si impegna altresì a organizzare percorsi formativi su tematiche specifiche mediante incontri con la Polizia di Stato, la Polizia Postale e/o figure specializzate.

Interventi di sensibilizzazione

La sensibilizzazione può costituire il primo passo verso un cambiamento positivo, ma per far sì che l'intervento sia efficace, è importante che sia chiara l'azione verso cui i soggetti devono impegnarsi. Due sono gli aspetti che bisogna tenere in considerazione:

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

Per far sì che un intervento di sensibilizzazione sia efficace si forniscono ai beneficiari informazioni chiare su quello che è lo stato attuale del tema che vogliamo trattare. In questo modo gli utenti avranno tutte le informazioni necessarie per avere una fotografia chiara del contenuto che stiamo trattando e del perché è necessario impegnarsi verso un cambiamento.

In sintesi, è opportuno tenere in considerazione i seguenti aspetti:

- spingere le persone a desiderare un cambiamento;

- porre in evidenza la possibilità di generare un cambiamento;
- individuare le azioni che consentono di produrre il cambiamento.

Un'attività di sensibilizzazione fornisce non solo le informazioni necessarie, ma illustra anche le possibili soluzioni o comportamenti da adottare.

Interventi di prevenzione

Il concetto di prevenzione nasce in ambito epidemiologico e seguendo quanto riportato dal Ministero della Salute si può sintetizzare come un insieme di attività, azioni e interventi attuati con il fine prioritario di promuovere e conservare lo stato di salute ed evitare l'insorgenza di malattie.

Se il problema della "sicurezza" è difficilmente riconducibile esclusivamente all'esistenza in sé di alcuni rischi, più o meno gravi e insidiosi, appare chiaro dunque come le migliori strategie di intervento siano di carattere prevalentemente preventivo.

L'Institute of Medicine distingue la prevenzione in tre livelli:

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

Il modello diviso in tre livelli è un'utile guida per affrontare e prevenire ogni possibile situazione di disagio.

I programmi che possono essere realizzati con maggiore frequenza ricadono nel primo livello di Prevenzione Universale e sono sicuramente consigliati proprio perché vanno a formare e consolidare quelle competenze educative di base necessarie a poter gestire le situazioni di vita che alunni/e sperimentano online.

Come sappiamo, le dimensioni che il fenomeno coinvolge sono molteplici e non puramente tecniche e si rifanno alla capacità dei più giovani di gestire situazioni complesse che richiedono:

- la capacità di gestire la relazione con l'altro/a diverso/a da sé,
- le dimensioni dell'affettività e della sessualità,
- il riconoscimento di un limite, anche, ma non solo, legato a una dimensione di legalità,
- l'utilizzo sicuro e consapevole delle tecnologie digitali.

Per questo motivo la scuola rafforza la sua capacità di rispondere anche a questi bisogni attraverso strumenti e misure specifiche. Allo stesso modo quando un evento problematico connesso ai rischi online coinvolge il contesto scolastico, è fondamentale dare una risposta il più possibile integrata, che trovi la sua espressione di indirizzo in procedure chiare di cui

deve dotarsi e che includano la collaborazione (prevedendo accordi specifici) con la rete dei servizi locali (in primis le ATS e la Polizia Postale).

Inoltre, la responsabilità dell'azione preventiva ed educativa chiama in campo diverse agenzie che sono chiamate a collaborare a un progetto comune, nell'ambito di funzioni educative condivise (scuola, famiglia, istituzioni, associazioni, società civile, etc.).

I comportamenti a rischio possono essere molteplici ma afferiscono, in base alla fascia di età, a uno sviluppo cognitivo, affettivo e morale incompleto oppure a fasi critiche transitorie o alla capacità di gestione di dinamiche complesse (confronto/relazione con il Sé e l'altro, empatia, socialità, affettività e sessualità, legalità e utilizzo sicuro delle tecnologie digitali).

Per questo motivo nel nostro Istituto è attivo da anni il progetto Life Skills Training rivolto agli alunni/e della Scuola Secondaria di primo grado e alle classi terze, quarte e quinte della Scuola Primaria.

Azioni di contenimento per la prevenzione dei rischi online:

- se la condotta incauta dell'alunno/a consiste nel fare circolare immagini imbarazzanti, di natura sessuale, su internet, è necessario rimuoverle: contattare il service provider e se il materiale postato viola i termini e le condizioni d'uso del sito chiedere di rimuoverle;
- se l'alunno/a viene infastidito od offeso, suggerirgli di modificare i dettagli del proprio profilo sistemandolo su "privato", in modo tale che solo gli utenti autorizzati siano in grado di vederlo (MSN messenger, siti social network, Skype etc.), o suggerirgli di bloccare o ignorare particolari mittenti, di cancellare il loro nominativo dalla lista degli amici con i quali regolarmente chatta, di inserire il compagno o la persona che offende, per quanto riguarda l'e-mail, tra gli indesiderati;
- consigliare di cambiare il proprio indirizzo e-mail, contattando l'e-mail provider, di scaricare un'applicazione che blocchi chiamate e messaggi da numeri indesiderati o, se necessario, cambiare il numero di cellulare contattando l'operatore telefonico;
- far cancellare il materiale offensivo dal cellulare, facendo intervenire i genitori, e chiedere agli alunni/e di indicare a chi e dove lo hanno spedito, conservare una copia di detto materiale se necessario per ulteriori indagini;
- contattare la Polizia se si ritiene che il materiale offensivo sia illegale. In caso di foto e video pedopornografici, confiscare il cellulare o altri dispositivi ed evitare di eseguire download, produrne copie, condividerne link o postarne il contenuto, poiché ciò è reato per chiunque.

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, novellata della legge 70 del 17 maggio 2024 *"Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e cyberbullismo"*, in vigore dal 14 giugno 2024 e le relative **Linee di orientamento per la prevenzione e il contrasto dei fenomeni di Bullismo e cyberbullismo** del 2021 (D.M. 18/2021) 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).

Definizione del fenomeno e caratteristiche

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 vengono usati impropriamente e si riconducono a 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.

Il termine cyberbullismo viene coniato dall'educatore canadese Bill Belsey nel 2002, ma una prima vera definizione del fenomeno viene elaborata solo qualche anno dopo.

Nel 2006 Smith e collaboratori definirono il cyberbullismo come:

"Un atto aggressivo e intenzionale perpetrato da un individuo o da un gruppo, attraverso l'uso delle nuove tecnologie della comunicazione, in modo ripetuto e continuato nel tempo, contro una vittima che non può facilmente difendersi" (in Smith P.K., Mahdavi J., Carvalho C., e Tippett N., An investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying. A Report to the Anti-Bullying Alliance, 2006, p.6).

Nel bullismo tradizionale, solitamente, la vittima che viene presa di mira è percepita come più debole e incapace di difendersi.

Il più forte, quindi, assume atteggiamenti prevaricatori nei confronti del più debole, a partire da una certa "asimmetria di potere".

Ciò, naturalmente, può accadere anche nel caso del cyberbullismo. Mentre nel bullismo tradizionale, però, il potere presenta connotati ben precisi, potrebbe essere, ad esempio, di tipo fisico (legato alla forza o alla statura) o sociale (legato alla popolarità), il potere online può derivare semplicemente dal possesso di specifiche competenze o di alcuni contenuti (immagini, video, confessioni) che potrebbero essere utilizzati per danneggiare la vittima.

Solitamente, quando si parla di cyberbullismo o di bullismo è necessario che vittima e bullo/cyberbullo siano minori o comunque adolescenti (sono esclusi, quindi, dalla definizione episodi di prevaricazione che avvengono fra adulti o fra un adulto e un minore).

Le caratteristiche specifiche del cyberbullismo rispetto al bullismo cosiddetto tradizionale sono:

- **l'impatto**: la diffusione di materiale tramite internet è incontrollabile e non è possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online e continuare a diffondersi). Un contenuto offensivo e denigratorio online può, quindi, diventare virale e distruggere in alcuni casi la reputazione della vittima.

Nelle situazioni più gravi, le vittime di cyberbullismo si trovano costrette a dover cambiare scuola o addirittura città, ma questo spesso non le aiuta. La Rete, si sa, è ovunque;

- **la convinzione dell'anonimato**: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile. Sentendosi protetti dall'anonimato ci si sente liberi e più forti nel compiere atti denigratori, senza il timore di essere scoperti. È importante tenere bene a mente, però, che quello dell'anonimato è un "falso mito della Rete". Ogni nostra azione online è, infatti, rintracciabile e riconducibile a noi con gli strumenti opportuni o con l'intervento della Polizia Postale. L'anonimato del cyberbullo, inoltre, è anche uno dei fattori che stanno alla base del forte stress percepito dalla vittima, la quale molte volte non può dare né un nome e né un volto al proprio aggressore;
- **l'assenza di confini spaziali/temporali**: il cyberbullismo può avvenire ovunque e in ogni ora del giorno e della notte, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio. La vittima può essere raggiungibile anche a casa e vive nella costante percezione di non avere vie di fuga. Spegnere il cellulare o il computer non basta, così come cancellare tutti i propri profili social. Il solo pensiero che eventuali contenuti denigratori continuino a diffondersi online è doloroso e si accompagna a un senso costante di rabbia e impotenza;
- **l'indebolimento dell'empatia**: esistono cellule chiamate neuroni specchio che ci permettono di "leggere" gli altri quando li abbiamo di fronte, capirli e di provare emozioni simili a quelle che loro provano, proprio come se fossimo di fronte a uno specchio. Tale sensazione è data dall'attivazione di una particolare area del cervello. Quando le interazioni avvengono prevalentemente online la funzione speciale di questi neuroni viene meno (mancando la presenza fondamentale dell'altro che è sostituito dal dispositivo). La riduzione di empatia che ne consegue può degenerare nei comportamenti noti messi in atto dai cyberbulli;
- **il feedback non tangibile**: il cyberbullo non vede in modo diretto le reazioni della vittima e, ancora una volta, ciò riduce fortemente l'empatia e il riconoscimento del danno provocato.

Per questo non è mai totalmente consapevole delle conseguenze delle proprie azioni. L'impossibilità di vedere con i propri occhi l'eventuale sofferenza e umiliazione provata dalla vittima fa sì che il tutto venga percepito come "uno scherzo" divertente a cui partecipare, di cui ridere o a cui essere indifferenti. Inoltre, il cyberbullismo non lascia segni fisici evidenti sulla vittima e si consuma in un contesto virtuale che spesso viene percepito dai ragazzi/e come non "reale", come un mondo ludico a sé stante.

Per questo il fenomeno viene talvolta sottovalutato anche dal mondo adulto, familiare e scolastico.

La mediazione tecnologica, infatti, porta a un certo distanziamento fra aggressore e vittima, causando quello che Bandura ha definito come "disimpegno morale". Si tratta di un indebolimento del controllo morale interno dell'individuo, con la conseguente minimizzazione delle responsabilità individuali. Tale fenomeno vale non solo per il cyberbullo, ma anche per i cosiddetti bystander, ossia coloro che sono spettatori dei fatti.

A ciò si aggiungono altre convinzioni o tendenze frequenti nell'uso della Rete sia da parte dei giovani che degli adulti:

- percezione che online non ci siano norme sociali da rispettare: fra i giovani spesso vige la falsa convinzione secondo cui la Rete sia uno spazio virtuale lontano dalla realtà, in cui vige libertà assoluta e in cui regole e norme sociali della vita quotidiana non valgono;
- la sperimentazione online di identità e personalità multiple: la Rete è per i minori il luogo virtuale per eccellenza in cui mettersi in gioco "fingendo di essere ciò che non si è" per il semplice gusto di sperimentare nuove forme di identità e comportamento;
- il contesto virtuale come un luogo di simulazione e giochi di ruolo: "la vita sullo schermo" e tutti i comportamenti messi in atto online vengono percepiti solo come un gioco;
- diffusione di responsabilità: tutti quelli che partecipano anche solo con un like o un commento diventano, di fatto, corresponsabili delle azioni del cyberbullo facendo accrescere la portata dell'azione; mettere un "like" su un social

network, commentare o condividere una foto o un video che prende di mira qualcuno o semplicemente tacere pur sapendo, mette ragazzi/e nella condizione di avere una responsabilità.

D'altro canto sono proprio loro che possono "fare la differenza" perché la responsabilità è condivisa: il gruppo "silente" che partecipa senza assumersi la responsabilità, rappresenta, in realtà, anche l'elemento che può fermare una situazione di cyberbullismo. Questo appunto costituisce un gancio educativo.

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

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

Le molestie che sono attuate attraverso strumenti tecnologici possono essere di vario tipo:

- litigare nei forum di discussione, con l'uso di un linguaggio violento e volgare;
- molestare attraverso l'invio ripetuto di messaggi offensivi;
- inviare ripetutamente messaggi che includono esplicite minacce fisiche;
- sparlare di qualcuno per danneggiare gratuitamente e con cattiveria la sua reputazione;
- registrare confidenze per poi inserirle integralmente in un blog pubblico;
- convincere, attraverso l'inganno, a rivelare informazioni imbarazzanti e riservate per renderle poi pubbliche in rete;
- insinuarsi all'interno dell'account di un'altra persona;
- estromettere intenzionalmente una persona da un gruppo online;
- riprendere, con il cellulare, macchina fotografica o videocamera, scene violente al fine di mostrarle ad amici o di diffonderle sulla Rete;
- pubblicare informazioni private e/o imbarazzanti su un'altra persona;
- inviare messaggi via smartphone e internet, corredati da immagini a sfondo sessuale.

Come riconoscere casi di cyberbullismo?

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

- appare nervosa quando riceve un messaggio o una notifica;
- sembra a disagio nell'andare a scuola o finge di essere malata;
- cambia comportamento e atteggiamento in modo repentino;
- mostra ritrosia nel dare informazioni su ciò che fa online;
- soprattutto dopo essere stata online, mostra rabbia o si sente depressa;
- inizia a utilizzare sempre meno Pc e smartphone (arrivando a evitarli);
- perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;
- il suo rendimento scolastico peggiora.

Finalità condivisa tra scuola e famiglia è intervenire preventivamente ed efficacemente, al fine di evitare, arginare ed

eliminare possibili manifestazioni di comportamenti antisociali. Valutare i comportamenti che sfociano in disagio sociale è precursore di un lavoro in rete, con la possibilità di coinvolgere anche un servizio specialistico socio-sanitario (psicologo della scuola, consultorio familiare, servizi di neuropsichiatria, etc.), quale supporto e/o forme di mediazione.

Il cyberbullismo è un fenomeno complesso che si manifesta con modalità articolate e si può distinguere in:

- **flamming**: invio di messaggi violenti e volgari allo scopo di suscitare conflitti verbali fra due o più utenti della rete;
- **harassment**: molestie attuate attraverso l'invio ripetuto di messaggi offensivi indirizzati verso la singola persona, che causano disagio emotivo psichico;
- **cyberstalking**: invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità e non si sente più al sicuro neanche tra le mura domestiche;
- **denigration**: divulgazione all'interno di comunità virtuali - quali newsgroup, blog, forum di discussione, messaggistica immediata, siti internet di pettegolezzi e commenti crudeli, calunniosi e denigratori, allo scopo di danneggiare la reputazione o l'amicizia di colui che viene preso di mira;
- **tricy o outing estorto**: registrazione delle confidenze, raccolte all'interno di un ambiente privato creando un clima di fiducia, poi inserite integralmente in un blog pubblico o in un social;
- **impersonation**: appropriazione dell'identità virtuale della vittima per compiere una serie di azioni che la porranno in difficoltà relazionali e in imbarazzo. Il furto di identità può avvenire a due livelli di complessità informatica: l'aggressore può aprire un nuovo profilo sui social network fingendo di essere la vittima oppure può agire come un vero hacker riuscendo a insinuarsi nell'account della vittima;
- **exclusion**: estromissione intenzionale di un altro utente dal gruppo di amici, dalla chat o da un gioco interattivo;
- **sexting**: invio di messaggi via smartphone e internet, corredati da immagini a sfondo sessuale;
- **happy slapping (schiaffo allegro)**: diffusione di un video dove la vittima è ripresa mentre subisce violenza psichica e fisica.

La normativa in materia

Il Parlamento italiano ha approvato il 18 maggio 2017 la Legge 71/2017, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo", una legge a tutela dei minori per la prevenzione e il contrasto al cyberbullismo che prevede misure prevalentemente a carattere educativo/rieducativo.

Dal 14 giugno 2024 è in vigore la legge 70 del 17 maggio 2024 *"Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e cyberbullismo"*.

La legge 70/2024, che novella la legge 71/2017 *"Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo"*, estendendone l'applicazione anche al fenomeno del bullismo, definisce i **compiti delle singole istituzioni scolastiche** - alcuni dei quali già previsti nelle policy che le scuole hanno adottato e sperimentato dall'entrata in vigore della legge 71/2017 e in attuazione delle vigenti Linee d'orientamento per la prevenzione e il contrasto dei fenomeni di Bullismo e Cyberbullismo del 2021 (D.M. 18/2021), di cui si evidenziano, segnatamente, i seguenti:

- all'art. 4, comma 2, della legge 71/2017, avente ad oggetto *"Linee di orientamento per la prevenzione e il contrasto in ambito scolastico"*, la legge 70/2024 introduce il comma 2 bis che così recita: *"Ogni istituto scolastico, nell'ambito della propria autonomia e in conformità alle linee di orientamento di cui al comma 1, adotta **un codice interno per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo e istituisce un tavolo permanente di monitoraggio del quale fanno parte rappresentanti degli studenti, degli insegnanti, delle famiglie ed esperti di settore».***
- All'art. 4 comma 3 della legge 71/2017 "Ogni istituto scolastico, nell'ambito della propria **autonomia**, individua

fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo, anche avvalendosi della collaborazione delle Forze di polizia nonché delle associazioni e dei centri di aggregazione giovanile presenti sul territorio", dopo il termine "autonomia", con la legge 70/2024, è aggiunto ***«recepisce nel proprio regolamento di istituto le linee di orientamento di cui al comma 1, anche con riferimento alle procedure da adottare per la prevenzione e il contrasto del bullismo e del cyberbullismo".***

- Il comma 1 dell'articolo 5 della legge 71/2017 è così novellato dalla legge 70/2024: *«Salvo che il fatto costituisca reato, il dirigente scolastico che, nell'esercizio delle sue funzioni, venga a conoscenza di atti di cui all'articolo 1, realizzati anche in forma non telematica, che coinvolgano studenti iscritti all'istituto scolastico che dirige, applica le procedure previste dalle linee di orientamento di cui all'articolo 4. Egli informa altresì tempestivamente i genitori dei minori coinvolti o i soggetti esercenti la responsabilità genitoriale su di essi e promuove adeguate iniziative di carattere educativo nei riguardi dei minori medesimi, anche con l'eventuale coinvolgimento del gruppo costituente la classe in percorsi di mediazione scolastica. Nei casi più gravi ovvero se si tratti di condotte reiterate e, comunque, quando le iniziative di carattere educativo adottate dall'istituzione scolastica non abbiano prodotto esito positivo, il dirigente scolastico riferisce alle autorità competenti anche per l'eventuale attivazione delle misure rieducative di cui all'articolo 25 del regio decreto-legge 20 luglio 1934, n. 1404, convertito, con modificazioni, dalla legge 27 maggio 1935, n. 835».*
- L' art. 5 della legge 70/2024 prevede specifici **adeguamenti del regolamento di cui al decreto del Presidente della Repubblica 24 giugno 1998, n. 249** ai seguenti principi: "a) prevedere (...) che la scuola si impegni a porre progressivamente in essere le condizioni per assicurare l'emersione di episodi riconducibili ai fenomeni del ***bullismo e del cyberbullismo, di situazioni di uso o abuso di alcool o di sostanze stupefacenti e di forme di dipendenza;*** *b) integrare la disciplina relativa al* ***Patto educativo di corresponsabilità****, di cui all'articolo 5-bis del citato regolamento di cui al decreto del Presidente della Repubblica n. 249 del 1998, prevedendo che nel Patto siano espressamente indicate tutte le attività di formazione, curriculari ed extracurriculari, che la scuola o i docenti della classe intendono organizzare a favore degli studenti e delle loro famiglie, con particolare riferimento all'uso della rete internet e delle comunità virtuali, e sia altresì previsto l'impegno, da parte delle famiglie e dell'istituto scolastico, a collaborare per consentire l'emersione di episodi riconducibili ai fenomeni del bullismo e del cyberbullismo, di situazioni di uso o abuso di alcool o di sostanze stupefacenti e di forme di dipendenza, dei quali i genitori o gli operatori scolastici dovessero avere notizia".*

La legge 70/2024 attribuisce specifici compiti anche alle Regioni e al Tribunale per i minorenni.

Le Regioni possono adottare, anche in accordo con gli Uffici Scolastici Regionali, iniziative per attivare nelle scuole servizi di sostegno psicologico agli studenti così come previsto dall'art. 4 bis **"Servizio di sostegno psicologico agli studenti"** che la Legge 70/2024 introduce nella Legge 71/2017, che così recita: *"Per l'attuazione delle finalità della presente legge, le regioni possono adottare iniziative affinché sia fornito alle istituzioni scolastiche di ogni ordine e grado, che lo richiedano, anche tramite convenzione con gli uffici scolastici regionali, nei limiti delle risorse disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri per la finanza pubblica, un servizio di sostegno psicologico agli studenti, al fine di favorire lo sviluppo e la formazione della personalità degli studenti medesimi nonché di prevenire fattori di rischio o situazioni di disagio, anche attraverso il coinvolgimento delle famiglie».*

Relativamente ai provvedimenti attribuiti al tribunale per i minorenni, l'art.2 della legge 70/2024 apporta modifiche al regio decreto-legge 20 luglio 1934, n. 1404, convertito, con modificazioni, dalla legge 27 maggio 1935, n. 835: *"Il procuratore della Repubblica presso il tribunale per i minorenni, quando abbia acquisito la notizia che un minore degli anni diciotto dà manifeste prove di irregolarità della condotta o del carattere ovvero tiene condotte aggressive, anche in gruppo, anche per via telematica, nei confronti di persone, animali o cose ovvero lesive della dignità altrui, assunte le necessarie informazioni, verifica le condizioni per l'attivazione di un percorso di mediazione oppure può chiedere al tribunale per i minorenni di disporre, con decreto motivato, previo ascolto del minorenne e dei genitori ovvero degli altri esercenti la responsabilità genitoriale, lo svolgimento di un progetto di intervento educativo con finalità rieducativa e riparativa sotto la direzione e il controllo dei servizi sociali".*

La legge pone al centro il ruolo dell'istituzione scolastica nella prevenzione e nella gestione del fenomeno e ogni Istituto scolastico dovrà provvedere a individuare fra i docenti un Referente con il compito di coordinare le iniziative di prevenzione e di contrasto dei fenomeni di Bullismo e Cyberbullismo. Aspetti chiariti nel dettaglio dalle Linee di orientamento per la prevenzione e il contrasto dei fenomeni di Bullismo e Cyberbullismo del 2021 (D.M. 18/2021).

A tal proposito il Dirigente Scolastico dell'Istituto Comprensivo di Esine ha individuato attraverso il Collegio dei Docenti un Referente del bullismo e cyberbullismo al fine di coinvolgere, prevenire e contrastare il fenomeno del bullismo/cyberbullismo, in tutte le componenti della comunità scolastica, ma in particolare quelle che operano nell'area dell'informatica.

Inoltre l'Istituto e il Referente del bullismo e cyberbullismo possono avvalersi della collaborazione delle Forze di Polizia, delle associazioni e dei centri specializzati del territorio.

La Legge 71/2017 introduce un provvedimento di carattere amministrativo per gli autori di atti di cyberbullismo, la procedura di ammonimento da parte del Questore: il minore autore può essere convocato dal Questore e ammonito se ritenuto responsabile delle azioni telematiche.

Più precisamente, la procedura di ammonimento prevista in materia di stalking (art. 612-bis c.p.), in caso di condotte di ingiuria (art. 594 c.p.), diffamazione (art. 595 c.p.), minaccia (art. 612 c.p.) e trattamento illecito di dati personali (art. 167 del Codice della privacy) commessi mediante internet da minori ultraquattordicenni nei confronti di altro minorenne, se non c'è stata querela o non è stata presentata denuncia, è stata estesa al cyberbullismo e può essere impartita da parte del questore (il questore convoca il minore, insieme ad almeno un genitore o a chi esercita la responsabilità genitoriale). Gli effetti dell'ammonimento cessano al compimento della maggiore età.

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

Responsabilità dei genitori e dei docenti/educatori quando un minore commette un reato o procura un danno: per il nostro ordinamento l'imputabilità penale (ossia la responsabilità personale per i reati commessi) scatta al quattordicesimo anno. La legge sancisce che "nessuno può essere punito per un fatto preveduto dalla legge come reato, se al momento in cui l'ha commesso, non era imputabile", cioè la cosiddetta "capacità d'intendere e volere".

Responsabilità dei genitori

Se il minore non ha compiuto i 14 anni, non risponde penalmente per l'evento, ma i genitori saranno tenuti al risarcimento del danno, per presunta "culpa in educando", così come previsto dal Codice Civile per i fatti commessi dal figlio/a. Non c'è responsabilità penale dei genitori, perché la responsabilità penale è personale. Se i genitori riescono a fornire la prova di aver fatto di tutto per impedire il fatto, possono essere esonerati dall'obbligo di risarcire il danno causato dal figlio/a. Ma questo tipo di prova è molto difficile da produrre, perché significa poter dare evidenza certa:

- *di aver educato e istruito adeguatamente il figlio/a (valutazione che viene dal Giudice commisurata alle circostanze),*
- *di aver vigilato attentamente e costantemente sulla sua condotta,*
- *di non aver in alcun modo potuto impedire il fatto, stante l'imprevedibilità e repentinità, in concreto, dell'azione dannosa.*

Responsabilità degli insegnanti

Nel caso di comportamenti penalmente rilevanti o di danni procurati a scuola: interviene l'art. 2048 del Codice Civile (responsabilità dei precettori) e l'art. 61 della L. 312/1980 n. 312 (responsabilità patrimoniale del personale direttivo, docente educativo e non docente). In base a queste norme gli insegnanti sono responsabili dei danni causati a terzi *"dal fatto illecito dei loro allievi... nel tempo in cui sono sotto la loro vigilanza".*

Per la scuola pubblica, la responsabilità si estende alla Pubblica Amministrazione, che si surroga al suo personale nelle

responsabilità civili derivanti da azioni giudiziarie promosse da terzi.

Come intervenire

Una indicazione operativa da tener presente per intervenire efficacemente è anche capire se si tratta effettivamente di cyberbullismo o di altra tipologia di comportamenti violenti o disfunzionali. Oltre al contesto, altri elementi utili a effettuare questa valutazione sono le modalità in cui avvengono e l'età dei protagonisti.

Un'altra indicazione operativa concerne una valutazione circa l'eventuale stato di disagio vissuto dalla/e persona/e minorenne/i coinvolta/e, per cui potrebbe essere necessario rivolgersi a un servizio deputato a offrire un supporto psicologico e/o di mediazione. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza.

Per quanto riguarda la necessità di segnalazione e rimozione, i genitori o chi esercita la responsabilità del minore di quattordici anni 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. **Il Garante ha pubblicato nel proprio sito il modello per la segnalazione/reclamo in materia di cyberbullismo da inviare a: cyberbullismo@gpdp.it.**

Parallelamente, nel caso in cui si ipotizzi che ci si possa trovare di fronte a una fattispecie di reato (come, ad esempio, il furto di identità o la persistenza di una condotta persecutoria che mette seriamente a rischio il benessere psicofisico del bambino/a o adolescente coinvolto/a in qualità di vittima) si potrà far riferimento agli uffici preposti delle Forze di Polizia per inoltrare la segnalazione o denuncia/querela e permettere alle autorità competenti l'approfondimento della situazione da un punto di vista investigativo. È in tal senso possibile far riferimento a queste tipologie di uffici: **Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato – Commissariato online (attraverso il portale https://www.commissariatodips.it).**

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

Azioni del nostro Istituto

L'I.C. di Esine mira a sensibilizzare gli utenti e a prevenire il fenomeno del cyberbullismo su tre livelli distinti:

- Azioni a livello individuale

- conoscenza del fenomeno;
- miglioramento delle competenze digitali del singolo alunno/a;
- potenziamento dell'autostima di ognuno.

- Azioni a livello di classe

- conoscenza del fenomeno del cyberbullismo;
- promozione di conoscenza reciproca, coesione, rispetto e risoluzione dei conflitti per rafforzare la coesione interna e il rispetto della diversità (circle time, apprendimento cooperativo...).

- Azioni a livello d'Istituto

- nomina del Referente del bullismo e cyberbullismo, che coordina le varie azioni;
- conoscenza del fenomeno (incontri a tema, iniziative rivolte alle famiglie);
- giornata nazionale contro il bullismo e cyberbullismo (7 Febbraio);
- sportello d'ascolto con psicologo;
- diffusione di buone pratiche.

L'I.C. di Esine prevede inoltre di adottare, sempre su tre livelli, le seguenti azioni di contrasto al fenomeno del cyberbullismo:

- Azioni a livello individuale

- rilevazione del fenomeno attraverso questionari o test per conoscere come l'alunno/a s trova in classe e a scuola.

- Azioni a livello di classe

- rilevazione del fenomeno;
- discussione e condivisione dei dati raccolti nei Consigli di Classe e interclasse per individuare strategie educative efficaci.

- Azioni a livello d'Istituto

- Regolamento d'Istituto;
- vigilanza nei luoghi e momenti più a rischio di utilizzo dello smartphone personale (bagni, spogliatoi, intervallo, cambio dell'ora, entrata e uscita...).

Le azioni di prevenzione e contrasto al bullismo e al cyberbullismo si inseriscono nella Scuola in architetture formative più ampie che traguardano, anche nell'ambito della legge 92/2019 *"Introduzione dell'insegnamento scolastico dell'educazione civica",* l'affermazione della cultura del rispetto, in relazione alla quale la legge 70/2024 istituisce la **Giornata del rispetto**, che ricorre il 20 gennaio, *"quale momento specifico di approfondimento delle tematiche del rispetto degli altri, della sensibilizzazione sui temi della non violenza psicologica e fisica e del contrasto di ogni forma di discriminazione e prevaricazione".*

A riguardo, si rammenta che Regione Lombardia, in attuazione di propri dispositivi normativi, a cominciare dalla legge regionale 1/2017 *"Disciplina degli interventi regionali in materia di prevenzione e contrasto al fenomeno del bullismo e del cyberbullismo"***,** ha promosso, in collaborazione con l'USR per la Lombardia, molteplici iniziative in linea con le disposizioni della legge 70/2024, a cui le scuole possono fare riferimento per consolidare, in una prospettiva integrata e sistematica, le strategie preventive e d'intervento in ordine al bullismo e cyberbullismo. In particolare:

- il Protocollo dedicato all'attivazione di un servizio psico-pedagogico a favore degli istituti scolastici di primo e secondo grado e delle istituzioni formative di istruzione e formazione professionale (legge regionale n. 16 del 6 agosto 2021), https://usr.istruzionelombardia.gov.it/wp-content/uploads/2023/10/m_pi.AOODRLO.REGISTRO-UFFICIALEU.0029995.06-10-2023.pdf

- Il Protocollo finalizzato allo sviluppo e al consolidamento in ambito scolastico di buone prassi per la prevenzione e il contrasto dei fenomeni legati alle diverse forme di dipendenza, al bullismo e cyberbullismo, alle altre forme di disagio sociale minorile e per la promozione della Legalità – Regione Lombardia, Prefettura di Milano, USR Lombardia, https://usr.istruzionelombardia.gov.it/intesa-regione-lombardia-prefettura-milano-usr-lombardia/

- La D.G.R. n. 7499/2022 *"Attuazione DGR 6761/2022: definizione delle modalità per la realizzazione di interventi per contrastare il disagio dei minori"* con la quale sono state individuate le ATS che hanno predisposto un Piano di azione territoriale per avviare interventi con la finalità di implementare e rafforzare le politiche di prevenzione e contrasto al bullismo e cyberbullismo e alle forme di disagio giovanile che si manifestano con comportamenti devianti (baby gang, atti di

vandalismo),https://www.regione.lombardia.it/wps/portal/istituzionale/HP/DettaglioRedazionale/servizi-e-informazioni/Enti-e-Operatori/sistema-sociale-regionale/politiche-per-i-minori/piano-interventi-disagio-minori-23-24/piano-interventi-disagio-minori-23-24

Saranno anche organizzati momenti informativi e di confronto a cura del *Gruppo di lavoro integrato per la prevenzione del bullismo e cyberbullismo*, costituito dall'USR Lombardia con proprio provvedimento, prot. n. 91 del 1.02.2024.

Hate speech: che cos'è e come prevenirlo

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

Cos'è l'hate speech

"L'incitamento all'odio deve essere inteso, quindi, come comprensivo di tutte le forme di espressione che diffondono, incitano, promuovono o giustificano l'odio razziale, la xenofobia, l'antisemitismo o altre forme di odio generate dall'intolleranza, ivi comprese: l'intolleranza espressa dal nazionalismo, e dall'etnocentrismo aggressivi, la discriminazione e l'ostilità nei confronti delle minoranze, dei migranti e delle persone con origine straniera" (www.coe.int).

Le azioni che il nostro Istituto intende intraprendere sono:

- informativa ai docenti, agli alunni/e, alle famiglie, al personale ATA
- formazione da parte di esperti
- attività in classe (anche laboratoriali)
- progetti per la promozione del rispetto della diversità:
  - rispetto delle differenze di genere;
  - di orientamento e identità sessuale;
  - di cultura e provenienza.
- azioni di educazione e sensibilizzazione:
  - adesione al Manifesto della comunicazione non ostile;
  - visione dei "Supererrori", filmati resi disponibili sul sito di Generazioni Connesse.
- azioni di visibilità sul territorio:
  - partecipazione a livello di Istituto o di ambito a eventuali eventi dedicati alle Giornate contro il bullismo e il razzismo.

Come riconoscerlo e prevenirlo

Le caratteristiche dell'hate speech, come riconoscerlo e prevenirlo, sono riportate nel documento "No hate Ita":

- **il discorso d'odio procura sofferenza.** La parola ferisce, e a maggior ragione l'odio! Il discorso può violare i diritti umani. Il discorso d'odio online non è meno grave della sua espressione offline, ma è più difficile da individuare e da combattere;
- **gli atteggiamenti alimentano gli atti.** Il discorso dell'odio è pericoloso anche perché può condurre a più gravi violazioni dei diritti umani, e perfino alla violenza fisica. Può contribuire a inasprire le tensioni razziali e altre forme di discriminazione e di violenza;
- **l'odio online non è solo espresso a parole.** Internet ci permette di comunicare rapidamente e in modi svariati, ad esempio, mediante i social media e i giochi online, molto spesso, d'altronde, in maniera anonima. L'odio online può esprimersi sotto forma di video e foto, come pure, più solitamente, di contenuto testuale. Le forme visive o multimediali hanno sovente un impatto più forte sugli atteggiamenti (consci e inconsci);
- **l'odio prende di mira sia gli individui che i gruppi.** L'odio online può prendere di mira dei gruppi che spesso sono già vulnerabili sotto altri aspetti, come i richiedenti asilo, le minoranze religiose o le persone con disabilità. Tuttavia, anche i singoli individui sono sempre maggiormente oggetto di attacchi. Le conseguenze sono talvolta fatali, come dimostrato da numerosi fatti di cronaca riferiti dai media, riguardanti giovani vittime di cyberbullismo che sono state spinte al suicidio;
- **internet è difficilmente controllabile.** La diffusione di messaggi di incitamento all'odio è maggiormente tollerata su internet rispetto al mondo offline ed è sottoposta a minori controlli. È ugualmente più facile (e comporta meno rischi) insultare o molestare online, perché le persone spesso si esprimono sotto la copertura dell'anonimato;
- **ha radici profonde.** Gli atteggiamenti e le tensioni sociali che suscitano sentimenti di odio online affondano le loro radici nella società, e non sono diversi, in genere, da quelli che alimentano il discorso dell'odio offline;
- **impunità e anonimato.** Sono le due presunte caratteristiche delle interazioni sociali in rete: l'impunità e l'anonimato. Queste abbassano le remore etiche. In realtà, però, qualsiasi azione compiuta sul web consente di rintracciare il suo autore.

Come riconoscerlo

Il discorso dell'odio si manifesta con un ampio spettro di azioni: sebbene tutte le espressioni che istigano all'odio meritino di essere classificate come malvagie, ne esistono alcune che possono essere peggiori di altre.

È utile, quindi, prendere in considerazione alcuni aspetti:

- **il contenuto e il tono**

Certe espressioni di odio sono più estreme, utilizzano termini più insultanti e possono perfino istigare altri ad agire. All'altra estremità della scala, troviamo insulti più moderati o generalizzazioni eccessive, che presentano certi gruppi o individui sotto una cattiva (e perfino sotto falsa) luce;

- **l'intenzione degli autori degli insulti**

Può capitare di offendere gli altri senza volerlo, e poi di pentirsene;

- **i bersagli o i bersagli potenziali**

Alcuni gruppi, o individui, possono essere più vulnerabili di altri alle critiche. Può dipendere dal modo in cui sono globalmente considerati nella società, o da come sono rappresentati nei media, oppure dalla loro situazione personale, che non permette loro di difendersi efficacemente;

- **il contesto**

Il contesto di una particolare espressione di odio è legato talvolta a circostanze storiche e culturali specifiche. Può includere altri fattori, come il mezzo utilizzato e il gruppo preso di mira, le tensioni o i pregiudizi esistenti, l'autorità del suo autore, etc.;

- **l'impatto o l'impatto potenziale**

L'impatto reale o potenziale esercitato sugli individui, sui gruppi o sull'insieme della società è una delle principali considerazioni da tenere presenti. Spesso, le ripercussioni negative subite dall'individuo o dal gruppo si rivelano più importanti della valutazione dell'episodio da parte di osservatori esterni.

Come intervenire

Lo sviluppo delle competenze digitali e l'educazione a un uso etico e consapevole delle tecnologie assumono quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete.

Il nostro Istituto intende affrontare il fenomeno, sempre più diffuso a livello educativo e scolastico, prefiggendosi i seguenti obiettivi:

- valorizzare la dimensione relazionale, sensibilizzando alunni/e verso capacità di analisi e discernimento, per fornire strumenti idonei tanto comunicativi quanto educativi sotto l'aspetto civico e morale;
- favorire l'educazione interculturale, fornendo agli alunni/e 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 degli alunni/e per evitare che i discorsi di incitamento all'odio possano tradursi in offese e umiliazioni nei confronti delle vittime.

Al raggiungimento di questi obiettivi concorrono tutte le discipline che, pure nella loro diversità di approccio, si attivano per il raggiungimento delle competenze chiave di cittadinanza.

In relazione alle manifestazioni socio-affettive fra pari, al linguaggio "volgare" o irrispettoso, al fine di evitare prevaricazioni e imbarazzo o disagio, i docenti intervengono per favorire negli alunni/e:

- un buon rapporto con il proprio corpo;
- per far percepire meglio eventuali violazioni dei limiti di prossimità o di "confidenza" e imparare a opporvisi;
- per far acquisire fiducia nelle proprie sensazioni e nel proprio intuito e determinazione nel rifiutare i contatti anche "a distanza" sgradevoli o "strani";
- per renderli consapevoli del diritto al rispetto dei propri limiti e di quelli altrui;
- per far capire loro che l'interazione online deve sottostare a delle regole di buon comportamento, né più né meno della comunicazione a viso aperto, quale quella della vita reale.

Qualora la scuola rilevi una situazione psico-socio-educativa particolarmente problematica, convocherà i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possano rivolgersi, consigliando anche di servirsi dello sportello di ascolto psicologico gratuito attivo presso l'Istituto.

Gli alunni/e vengono resi partecipi di differenti iniziative solidali al fine di sensibilizzarli ai temi del sociale e della legalità.

Dipendenza da Internet e gioco online

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

scolastico e irrefrenabile voglia di utilizzo della Rete.

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

La dipendenza da internet, 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 alunni/e affinché questi siano consapevoli dei rischi che comporta l'iperconnessione.

I segnali patologici di questo che viene descritto come **"un vero e proprio abuso della tecnologia"**, anche denominato **"Internet Addiction Disorder"** (I.A.D. coniato dallo psichiatra Ivan Goldberg 1996), sono specifici così come accade per le altre dipendenze più "tradizionali".

In particolare, si hanno: la tolleranza, ossia quando vi è un crescente bisogno di aumentare il tempo su internet e l'astinenza, quando vi è l'interruzione o la riduzione dell'uso della Rete che comporta ansia, agitazione psicomotoria, fantasie e pensieri ossessivi (malessere psichico e/o fisico che si manifesta quando si interrompe o si riduce il comportamento).

Tutto questo ha ripercussioni sulla sfera delle relazioni interpersonali che diventano via via più povere e alle quali si preferisce il mondo virtuale, con alterazioni dell'umore e della percezione del tempo.

Da sottolineare, la nomofobia (nomo deriva da "no-mobile") termine usato per categorizzare quei soggetti che sperimentano emozioni negative, quali ansia, tristezza e rabbia quando non sono connessi con il proprio smartphone.

Spesso il trascorrere del tempo online, in termini disfunzionali, è scandito dal gioco virtuale che può anche assumere forme di Dipendenza dal gioco online (Net Gaming Addiction o Internet Gaming Addiction) inserito all'interno del Manuale Diagnostico Statistico dei Disturbi Mentali (DSM 5). Da specificare che la dipendenza qui si realizza quando c'è un abuso, ossia un utilizzo continuativo e sistematico della Rete al fine di giocare impegnando la maggior parte delle giornate, con la conseguente sottrazione del tempo alle altre attività quotidiane del minore.

Di seguito i sintomi che devono essere presenti (per un arco di tempo di almeno un anno):

1. il giocatore è assorbito totalmente dal gioco;
2. il giocatore è preoccupato e ossessionato dal gioco;
3. il gioco consente alla persona di sfuggire alla realtà con la sperimentazione di emozioni più piacevoli;
4. il giocatore manifesta sempre di più l'impulso di giocare e di sperimentare emozioni positive;
5. il giocatore sente di dover dedicare più tempo ai giochi;
6. il giocatore se non può giocare manifesta ansia, depressione e irritabilità;
7. può emergere un ritiro sociale;
8. il giocatore, anche se comprende la gravità della situazione e sospende di giocare comunque non riesce a interrompere del tutto;
9. il giocatore mente agli altri sull'utilizzo che fa dei giochi online;
10. il giocatore ha perso o mette a rischio relazioni o opportunità a causa dei giochi su internet o ha perso interesse verso attività nella vita reale.

La S.I.I.Pa.C., la Società Italiana Intervento Patologie Compulsive, definisce la dipendenza da internet come progressivo e totale assorbimento del soggetto alla Rete; di seguito alcune caratteristiche specifiche:

- **Dominanza.** L'attività domina i pensieri e il comportamento del soggetto, assumendo un valore primario tra tutti gli interessi.
- **Alterazioni del tono dell'umore.** L'inizio dell'attività provoca cambiamenti nel tono dell'umore. Il soggetto

prova un aumento d'eccitazione o maggiore rilassatezza come diretta conseguenza dell'incontro con l'oggetto della dipendenza.

- **Conflitto.** 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.** Tendenza a ricominciare l'attività dopo averla interrotta.

L'Istituto in tal senso propone incontri con esperti per affrontare il variegato mondo delle dipendenze, al fine di sensibilizzare le famiglie a monitorare le ore trascorse online. Docenti ed esperti cercheranno di far comprendere agli alunni/e la differenza tra "momento" di gioco di svago e "necessità" di giocare in rete, promuovendo attività che permettano loro di acquisire competenze nella gestione del sovraccarico informatico e delle relative distrazioni.

Anche per questo motivo nel nostro Istituto è attivo da anni il progetto Life Skills Training, un programma educativo validato scientificamente nella promozione della salute della popolazione scolastica.

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.

"Spesso sono realizzate e vengono diffuse attraverso il cellulare (tramite invio di mms o condivisione tramite bluetooth) o attraverso siti, e-mail, chat. Spesso tali immagini o video, anche se inviate a una stretta cerchia di persone, si diffondono in modo incontrollabile e possono creare seri problemi, sia personali che legali, alla persona ritratta. L'invio di foto che ritraggonno minorenni al di sotto dei 18 anni in pose sessualmente esplicite configura, infatti, il reato di distribuzione di materiale pedopornografico".

I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di "revenge porn" letteralmente "vendetta porno" fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte (la Legge 19 luglio 2019 n. 69, all'articolo 10 ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti. Si veda l'articolo 612 ter del Codice Penale rubricato "Diffusione illecita di immagini o 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 consapevolezza, o comunque la sola idea di diffusione di contenuti personali, si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il/i soggetto/i della foto/del video che colui/coloro che hanno contribuito a diffonderla.

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

depressione.

L'Istituto ritiene che per prevenire il "sexting" sia necessario svolgere un percorso specifico.

Per tale motivo propone percorsi formativi che hanno come finalità la prevenzione della devianza e del disagio giovanile che permetta la costruzione dello “star bene” con sé e con gli altri.

L'Istituto organizza attività, progetti, corsi, eventi con l’obiettivo di coinvolgere, informare genitori, insegnanti e, in generale, gli adulti educatori sulle tematiche inerenti la formazione degli alunni/e sui seguenti temi:

- alfabetizzazione emotiva;
- autostima;
- socializzazione e dinamiche relazionali;
- cooperazione;
- educazione all’affettività e alla sessualità.

Adescamento online

Il ***grooming*** (dall’inglese “groom” - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di ***teen dating*** (siti di incontri per adolescenti). Un’eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

In Italia l’adescamento si configura come reato dal 2012 (art. 609-undecies – l’adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell’adescamento.

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. Anche per questo potrebbero essere aperti e curiosi verso nuove esperienze e, talvolta, attratti da relazioni intime e apparentemente rassicuranti. In questa fase è importante, infatti, il bisogno di avere attenzioni esclusive da un’altra persona, di ottenere rinforzi esterni di approvazione per il proprio corpo e la propria immagine. È proprio in ragione della fiducia costruita nella relazione che le vittime di adescamento online riferiscono di sentirsi umiliate, usate, tradite e tendono a sentirsi in colpa e ad autosvalutarsi per essere cadute nella trappola.

L’adescamento, quindi, non avviene apparentemente con una dinamica violenta, ma il “prendersi cura” del minore rappresenta la conditio per carpirne la fiducia e instaurare una relazione a sfondo erotico. Può capitare che l’adescatore si presenti al minore sotto falsa identità, fingendo quindi di essere un’altra persona così da attirare maggiormente l’attenzione del minore.

Le fasi dell’adescamento

Il processo di adescamento segue generalmente 5 fasi:

1. **Fase dell’amicizia iniziale**: 1. questa è la fase in cui l’adescatore cerca i primi contatti con la vittima individuata,

provando a socializzare con lei. Tenterà, quindi, di conoscerla meglio al fine di scoprirne bisogni, interessi e il contesto in cui vive. Condividendo argomenti di interesse del minore l'adescatore cercherà pian piano di conquistarsi la sua fiducia, ponendogli domande frequenti che attestano interesse e attenzione nei suoi confronti. Gradualmente affronterà con la vittima argomenti sempre più privati e intimi.

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

Fonte: Schema sulle fasi dell'adescamento online dei minori a cura della Polizia Postale e delle Comunicazioni, all'interno del

progetto Una vita da social. Insieme all'Osservatorio Nazionale Adolescenza: https://www.adolescienza.it/

Riferimenti normativi

Nel testo della Convenzione di Lanzarote (legge 172 dell'1 ottobre 2012) il reato viene definito come "qualsiasi atto volto a carpire la fiducia di un minore di anni sedici per scopi sessuali, attraverso artifici, lusinghe o minacce posti in essere anche mediante internet o altre reti o mezzi di comunicazione". Si parla di reato anche se l'incontro reale con il minore non avviene; è sufficiente, infatti, il tentativo. La legge 172 del 2012, (art. 351 c.p.p.) prevede che la vittima o chi è testimone di episodi di grooming, debba essere ascoltato in sede di raccolta di sommarie informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

Come riconoscerlo

Per riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli segnali che possono essere indicatori importanti, come ad esempio un cambiamento improvviso nel comportamento di un minore.

L'importanza di un'adeguata educazione all'affettività e alla sessualità

Al fine di prevenire casi di adescamento online è opportuno, pertanto, accompagnare alunni/e in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a 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 sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato.

Affinché ciò avvenga è necessario tenere sempre un canale di comunicazione con loro.

Lo sportello di ascolto e la possibilità di rivolgersi direttamente ai docenti è una possibilità che sussiste già da diversi anni nel nostro Istituto, al fine di supportare pedagogicamente gli alunni/e in difficoltà.

La sessualità in Rete è spesso rappresentata in modo decontestualizzato e 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", tanto più forte e virile quanto più è in grado di conquistare e dominare quell'"oggetto".

In un contesto simile non c'è da stupirsi se, talvolta, anche i comportamenti degli adolescenti in Rete nella gestione della propria sessualità o semplicemente della propria immagine online riproducano tali modelli. Modelli che la società odierna sembra tuttora confermare in numerosi 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 alunni/e vivono la propria sessualità e la propria immagine online, al loro desiderio di esprimersi e affermare se stessi.

Fondamentale quindi, come sappiamo, è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche 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.

Come intervenire

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

Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima

possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video...).

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

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

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

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

La denuncia all'autorità giudiziaria o agli organi di Polizia costituisce il passo necessario per avviare un intervento di tutela a favore della vittima e attivare un procedimento penale nei confronti del presunto colpevole.

La presa in carico di situazioni di abuso sessuale, così delicate e complesse, richiede un approccio multidisciplinare, da parte di diverse figure professionali. I versanti su cui si articola l'intervento possono essere essenzialmente tre: medico, sociopsicologico e giudiziario.

Il compito della scuola, per tutti i reati descritti, non è comunque solo quello di "segnalare", ma più ampio e importante, soprattutto nella prevenzione dell'abuso, nonché nella ripresa della piccola vittima, in quanto ha al suo interno fattori relazionali ed educativi che possono aiutare il bambino/adolescente a riprendere una crescita serena.

A tal fine la scuola collabora con gli enti del territorio, alle Forze dell'Ordine, insieme alle altre figure professionali e alle famiglie, scambiando informazioni e condividendo progetti e prassi operative, favorendo le occasioni di confronto e di dialogo.

L'Istituto ritiene che per prevenire il "grooming" sia necessario svolgere un percorso specifico.

Per tale motivo propone percorsi formativi che hanno come finalità la prevenzione della devianza e del disagio giovanile che permetta la costruzione dello "star bene" con sé e con gli altri.

L'Istituto organizza attività, progetti, corsi, eventi con l'obiettivo di coinvolgere, informare genitori, insegnanti e, in generale, gli adulti educatori sulle tematiche inerenti la formazione degli alunni/e sui seguenti temi:

- alfabetizzazione emotiva;
- autostima;
- socializzazione e dinamiche relazionali;
- cooperazione;
- educazione all'affettività e alla sessualità.

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.*

La pedopornografia esiste da prima dell'avvento di internet. Tuttavia, la diffusione della Rete, l'evoluzione e la moltiplicazione dei "luoghi" virtuali, il cambiamento costante delle stesse tecnologie digitali, ha radicalmente cambiato il modo in cui il materiale pedopornografico viene prodotto e diffuso, contribuendo a un aumento della sua disponibilità e dei canali di diffusione.

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.

Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia. L'intento è quello di facilitare il processo di rimozione del materiale stesso dalla Rete e allo stesso tempo consentire le opportune attività investigative finalizzate a identificare chi possiede quel materiale, chi lo diffonde e chi lo produce, ma, soprattutto e primariamente, a identificare i minori abusati presenti nelle immagini e video, assicurando la fine di un abuso che potrebbe essere ancora in corso e il supporto necessario.

Parallelamente, se si ravvisa un rischio per il benessere psicofisico dei/lle bambini/e, ragazzi/e coinvolte nella visione di questi contenuti sarà opportuno ricorrere a un supporto psicologico anche passando per una consultazione presso il medico di base o pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi sociosanitari del territorio di appartenenza: Consultori Familiari, Servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, etc.

Se si è a conoscenza di tale tipologia di reato è possibile far riferimento alla: Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Polizia di Stato – Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato – Commissariato online.

L'Istituto ritiene che per prevenire il fenomeno della "pedopornografia" sia necessario svolgere un percorso specifico.

Per tale motivo propone percorsi formativi che hanno come finalità la prevenzione della devianza e del disagio giovanile che permetta la costruzione dello “star bene” con sé e con gli altri.

L'Istituto organizza attività, progetti, corsi, eventi con l’obiettivo di coinvolgere, informare genitori, insegnanti e, in generale, gli adulti educatori sulle tematiche inerenti la formazione degli alunni/e sui seguenti temi:

- alfabetizzazione emotiva;
- autostima;
- socializzazione e dinamiche relazionali;
- cooperazione;
- educazione all’affettività e alla sessualità.

4.2 - Quali strumenti e a chi

L’insegnante riveste la qualifica di pubblico ufficiale (ex art. 357 c.p.) 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.

Il Codice Penale Italiano, all’art. 357, definisce il pubblico ufficiale come colui che esercita una “pubblica funzione legislativa, giudiziaria o amministrativa”. Questa definizione si estende ai docenti nel momento in cui sono impegnati nell’esercizio delle loro funzioni all’interno degli istituti scolastici.

La Corte di Cassazione, con la sentenza n. 15367/2014, ha ribadito la qualifica di pubblico ufficiale per l’insegnante, estendendo tale riconoscimento non solo alla tenuta delle lezioni, ma anche a tutte le attività connesse. Questo include, ad esempio, gli incontri con i genitori degli allievi.

Le situazioni problematiche in relazione all’uso delle tecnologie digitali dovrebbero essere sempre gestite da un team di docenti composto da:

1. Dirigente
2. Docente referente,
3. L’animatore digitale (secondo il Piano Nazionale per la Scuola Digitale, abbreviato in PNSD, introdotto dalla Legge 107/2015)
4. Referente bullismo (ex. Legge Italiana Contro il Cyberbullismo, l. 71/2017
5. Altri docenti già impegnati nelle attività di promozione dell’educazione civica.

Le situazioni di pregiudizio presunto o reale possono richiedere il supporto e l'intervento di esperti esterni alla scuola.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due macro - 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.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo"

con l'obiettivo di allertare il Dirigente . La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, il Dirigente e i docenti coinvolti procedono alla valutazione del caso (valutare l'invio o meno della relazione agli organi giudiziari preposti) e agiscono tramite percorsi di sensibilizzazione.

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.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente. La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, si procede alla valutazione approfondita e alla verifica di quanto segnalato, avviando (se appurato la rilevanza penale) la procedura giudiziaria con denuncia all'autorità giudiziaria per attivare un procedimento penale.

Qualora si rilevasse un fatto riconducibile alla fattispecie di reato, l'insegnante - nel ruolo di pubblico ufficiale – non deve procedere con indagini di accertamento ma ha sempre l'obbligo di segnalare l'evento all'autorità giudiziaria. (ex. l. 71/2017). Con autorità competente si intendono:

- Procure Ordinarie: nel caso in cui il minore/i sia la vittima/e e il presunto autore del reato sia maggiorenne,
- Procura Minorile: in caso il presunto autore del reato sia minorenne.

Vi è anche l'obbligatorietà della segnalazione delle situazioni di pregiudizio a carico dei minori: L. 216/1991: per le situazioni di grave rischio l'istituzione scolastica è tenuta alla segnalazione delle medesime. Per pregiudizio si intende una condizione di rischio o grave difficoltà che provocano un danno reale o potenziale alla salute, alla sopravvivenza, allo sviluppo o alla dignità del bambino, nell'ambito di una relazione di responsabilità, fiducia o potere.

La segnalazione come da procedura interna è il primo passo per aiutare un minore che vive una situazione di rischio o di grave difficoltà e va intesa come un momento di condivisione e solidarietà nei confronti del minore. La mancata segnalazione costituisce, infatti, omissione di atti d'ufficio (art.328 C.P.).

Può essere utile, valutando accuratamente ciascuna situazione, attivare colloqui individuali con tutti i minori coinvolti, siano essi vittime, testimoni e/o autori. È importante considerare il possibile coinvolgimento dei genitori e di coloro incaricati della tutela dei minori coinvolti. L'intervento va indirizzato valutando l'eventuale impatto educativo e/o il contesto emotivo senza discriminare tra vittime, testimoni e/o autori.

Prevedere possibili incontri di mediazione tra i minori coinvolti vanno ponderati con la consapevolezza del loro stato emotivo, anche e in base agli elementi raccolti in merito del fatto/episodio avvenuto (elementi che si dovrebbero valutare di caso in caso). Importante è prevedere il coinvolgimento dei genitori sia della vittima che del bullo (ove possibile).

Anche i genitori devono e possono segnalare casi di sospetto o evidenza dei fenomeni, segnalarlo al Dirigente, o al docente coordinatore di classe o referente di istituto oppure direttamente al team antibullismo attraverso apposita procedura che definisce l'istituto (mail ad hoc, tramite gli uffici e postazioni specifiche, etc...).

Gli insegnanti e i genitori, come studenti e studentesse, si possono rivolgere alla Helpline del progetto Generazioni Connesse, al numero gratuito 19696, attraverso la chat disponibile sul sito o tramite chat WhatsApp per ricevere supporto e consulenza. Per tutti i dettagli, il riferimento è agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

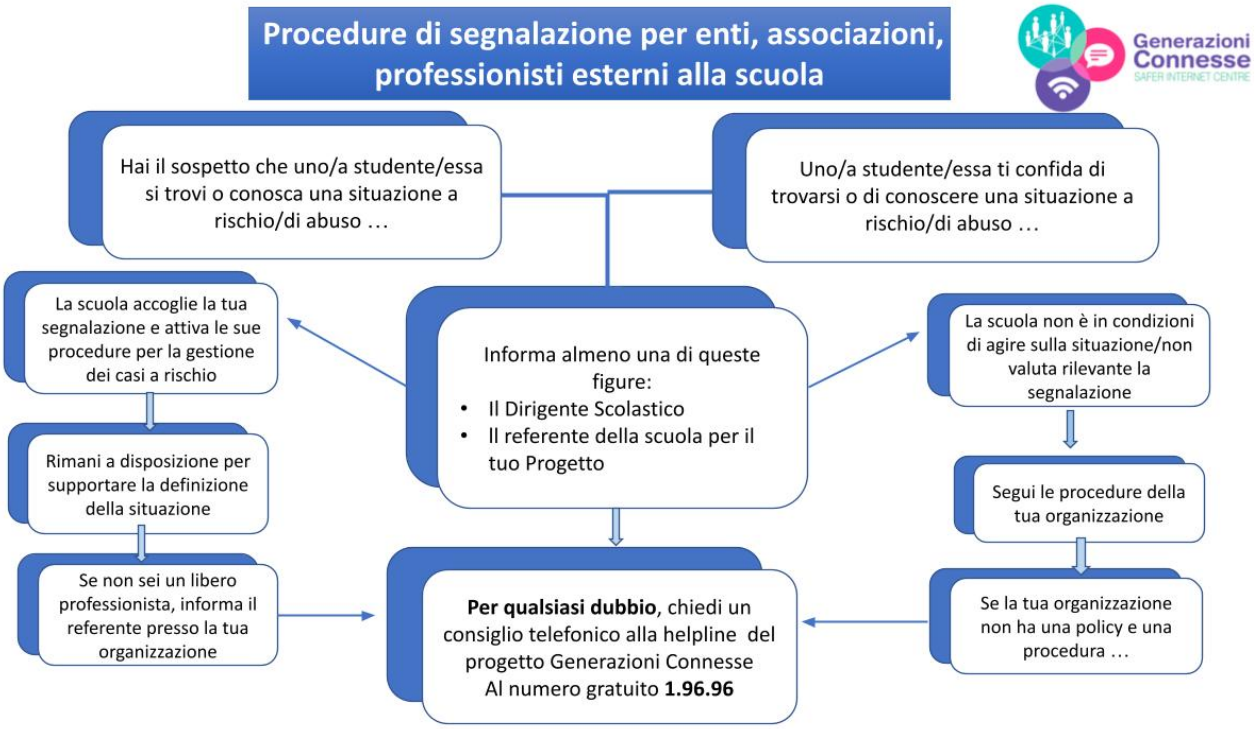
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail

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

In particolare, sarebbe utile che la scuola attivi un sistema di segnalazione utile anche al monitoraggio dei fenomeni dal quale partire per integrare azioni didattiche preventive e giornate di sensibilizzazione, insieme agli Enti/Servizi presenti sul territorio di riferimento. Importante, altresì, immaginare e programmare percorsi di peer education per la prevenzione e il contrasto degli agiti.

Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle Linee di Orientamento per la prevenzione e il contrasto dei fenomeni di Bullismo e Cyberbullismo del MI (Ministero dell'Istruzione) aggiornate al 2021, al Patto educativo di corresponsabilità e annessa appendice relativa agli impegni che le parti in causa dovranno assumere per l'espletamento efficace della DID e, in ultimo, al Piano scolastico per la Didattica Digitale Integrata, allegato al PTOF.

Procedure



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

Il docente ha evidenza che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Se non è già stato fatto, avvisa il referente per il cyberbullismo (e/o il team antibullismo) che attiva le procedure ("Corso 4" della piattaforma ELISA) e il Dirigente Scolastico.
Ricordare sempre che in base alla legge 71-2017:
A) Se c'è fattispecie di reato va fatta la segnalazione alle forze dell'ordine
B) Se non c'è fattispecie di reato.
Il DS (e/o il team antibullismo):
- informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto) su quanto accade e condividete informazioni e strategie.
- Informa i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy)
- Attiva il consiglio di classe.

A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla Polizia Postale:
a) contenuto; b) modalità di diffusione.
Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).

Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

NELLE CLASSI
Il team antibullismo collabora coi docenti della classe per realizzare l'intervento nella classe:
a seconda della situazione valuta se
- affrontare direttamente l'accaduto o
- sensibilizzare la classe (vedi Corso 4 Piattaforma Elisa)
- trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo

Il docente riceve una segnalazione (da un genitore, un altro studente …) o sospetta che stia accadendo qualcosa a uno/a studente/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Condividi con il referente o al team antibullismo: si attiva il processo di attenzione e valutazione a cura del referente.

Insieme si valuta se è il caso
- di avvisare il consiglio di classe;
- di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.

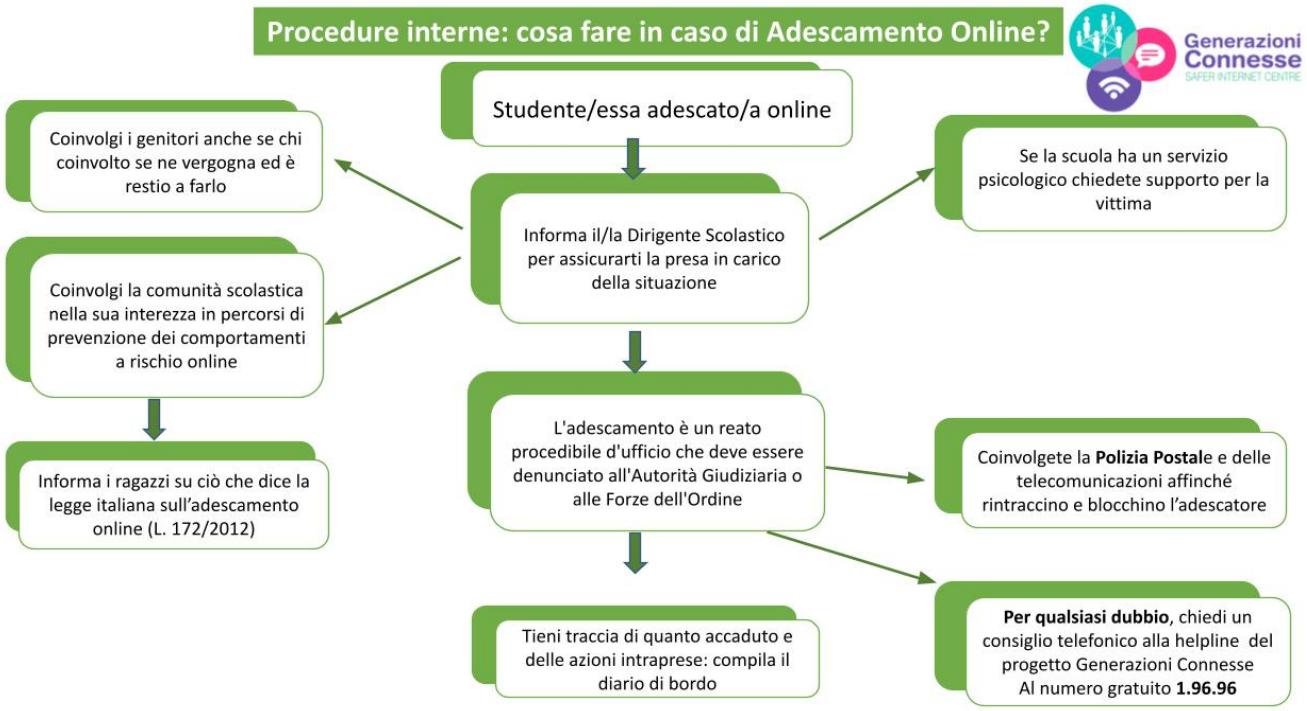
Se emergono evidenze passa allo schema successivo

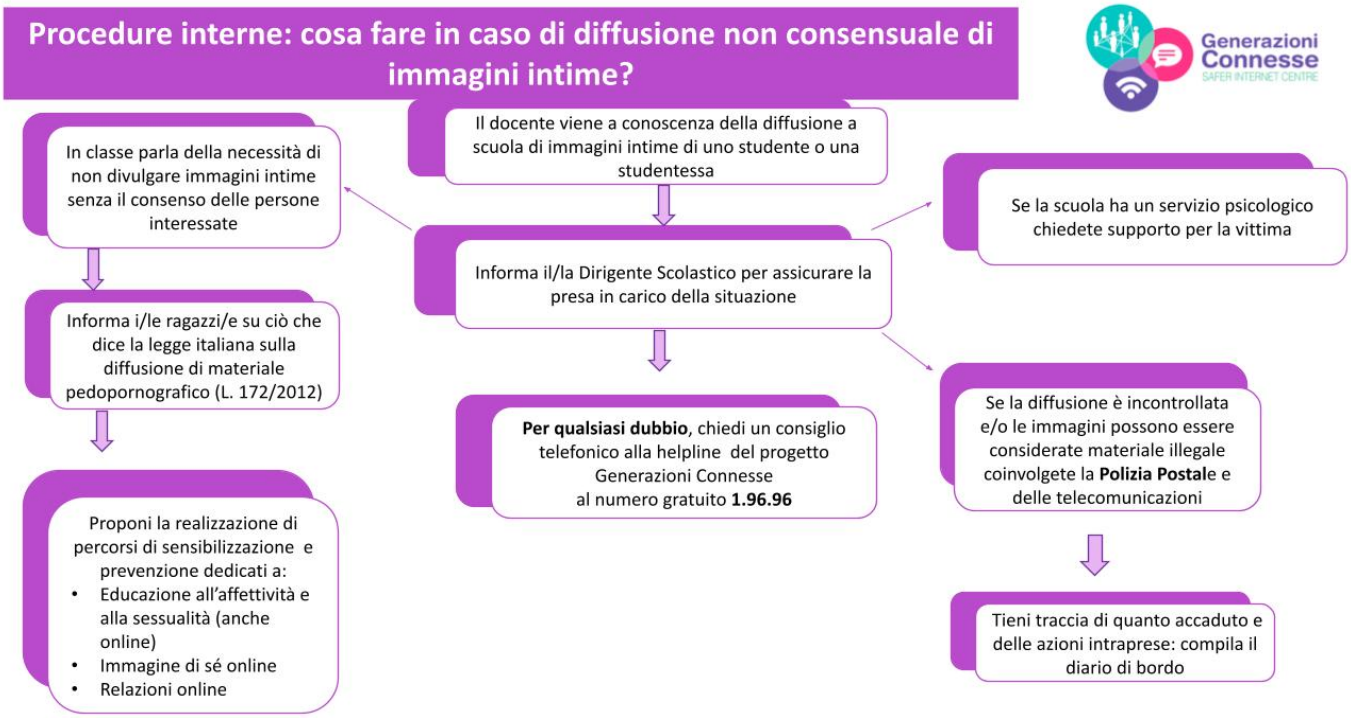
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

Scarica le linee di orientamento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo

Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Ricorda a studenti/esse che possono chiedere in qualsiasi momento una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 o via chat





Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito **1.96.96**.

In relazione al CASO A, è opportuno il coinvolgimento del Referente d'Istituto per il contrasto del bullismo e del

cyberbullismo, al fine di valutare le possibili strategie d'intervento. Se si ravvisano gli estremi, viene informato il Dirigente Scolastico unitamente al Consiglio di classe.

Nel frattempo, il docente (e i docenti informati) ascolta gli alunni/e, osservando e monitorando il clima di classe, ciò che accade, le dinamiche relazionali, senza fare indagini dirette.

Uno strumento utile per raccogliere informazioni può essere il diario di bordo (allegato alla presente ePolicy): il docente deve cercare di capire se gli episodi sono circoscritti al gruppo o se interessano l'intero Istituto. Operativamente è fondamentale coinvolgere tutti gli alunni/e, informandoli sui fenomeni e sulle caratteristiche degli stessi, suggerendo di chiedere aiuto se pensano di vivere situazioni, di subire atti identificabili come bullismo o cyberbullismo.

In relazione al CASO B, il docente deve condividere immediatamente quanto osservato con il Referente per il bullismo e il cyberbullismo, al fine di valutare insieme le possibili strategie di intervento. Si avvisa anche il Dirigente Scolastico che convoca il Consiglio di classe. Se non si ravvisano fattispecie di reato, è opportuno:

- informare i genitori (o chi esercita la responsabilità genitoriale) degli alunni/e direttamente coinvolti/e (qualsiasi ruolo abbiano avuto), se possibile con la presenza di professionisti dell'aiuto, su quanto accade e condividere informazioni, strategie e modalità di supporto;
- richiedere, in concomitanza, la consulenza dello psicologo scolastico (sportello di ascolto) a supporto della gestione della situazione, in base alla gravità dell'accaduto;
- creare momenti di confronto costruttivo in classe, con la presenza di figure specialistiche territoriali;
- informare i genitori degli alunni/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy);
- informare gli alunni/e ultra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy);
- convocare e attivare il Consiglio di classe;
- valutare come coinvolgere gli operatori scolastici su quello che sta accadendo.

A seconda della situazione e delle valutazioni effettuate con Referente, Dirigente e genitori, si potrebbe poi segnalare alla Polizia Postale – ove necessario ai fini di legge:

- contenuto del materiale online offensivo;
- modalità di diffusione;
- fattispecie di reato eventuale.

Se è opportuno, richiedere un sostegno ai servizi e alle associazioni territoriali o ad altre autorità competenti.

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

All'interno della procedura disciplinare, che vale per qualsiasi comportamento contrario al Regolamento di Istituto, si inserisce una parte specifica per gli episodi di bullismo e cyberbullismo in base all'attuale normativa: attraverso la compilazione del modulo in formato cartaceo opportunamente predisposto, viene effettuata una segnalazione al Referente per il bullismo e il cyberbullismo che ne dà immediata comunicazione al Dirigente Scolastico il quale valuta se ricorrono gli estremi per una denuncia; la segnalazione può essere anonima, ma va sempre riportata per iscritto anche se raccolta oralmente.

La segnalazione del caso dovrà quindi essere fatta dal singolo docente o dall'adulto a conoscenza del fatto, tramite modulo per la segnalazione casi, al Referente, il quale, insieme al Team Antibullismo e dell'Emergenza, si occuperà di raccogliere tutte le informazioni possibili, anche attraverso colloqui di approfondimento con gli attori coinvolti e di segnalare l'accaduto al Dirigente Scolastico.

Sarà poi il Dirigente, insieme al Team, a valutare se la segnalazione debba essere rivolta a organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali o se il caso vada gestito all'interno della scuola con il coinvolgimento del Consiglio di classe e delle famiglie degli alunni/e coinvolti. Si sceglierà uno o più interventi da attuare a cui seguirà una fase di monitoraggio. (cfr. schema di procedura di intervento nell'Allegato 3)

L'Istituto Comprensivo di Esine ha elaborato il seguente protocollo "Gestione emergenze".

Quando emerge un fatto di bullismo/cyberbullismo vanno considerati tutti gli attori in gioco: vittima/e, bullo/i, spettatori o maggioranza silenziosa, aiutanti/sostenitori, difensori del bullo o della vittima, gli adulti.

Il docente informato del caso di bullismo o cyberbullismo, dopo aver ricostruito fatti e responsabilità informa:

- il Dirigente Scolastico;
- il Referente del bullismo e cyberbullismo;
- il Coordinatore di classe;
- il Dirigente convoca gli alunni/e coinvolti direttamente (bullo/i, vittima/e) e i genitori degli stessi.

Il Dirigente Scolastico, se lo ritiene opportuno, convoca un Consiglio di classe straordinario, per stabilire le misure degli interventi e le sanzioni disciplinari.

Il Dirigente, in accordo con il Consiglio di Classe, informa le famiglie degli alunni/e coinvolti e attiva:

- gli interventi individuali: misure di supporto per la vittima;
- le sanzioni disciplinari e percorsi rieducativi per il/i bullo/i;
- gli interventi sulla classe.

Colloquio del Dirigente con i genitori

Avviene in tempi separati (genitori della vittima, genitori del bullo con i rispettivi figli/e).

Viene eseguita la comunicazione del fatto e firma da parte dei genitori del modulo di segnalazione, da conservare nel registro dei verbali. I genitori vanno informati delle loro responsabilità civili e legali, in quanto genitori di minori di 14 anni, dell'eventuale reato del figlio/a e dell'obbligo della scuola di fare segnalazione alle autorità competenti se il fatto si configura come reato.

Viene inoltre fatta richiesta ai genitori di collaborazione e vigilanza nei mesi successivi, secondo le indicazioni del "Patto Educativo di Corresponsabilità".

La sanzione disciplinare stabilita, di tipo anche riparativo, oltre eventuale sospensione, può essere comunicata anche nei giorni successivi.

Se lo si ritiene necessario, il Dirigente organizza un incontro tra i genitori degli alunni/e coinvolti/e, in modo da favorire il dialogo e rasserenare il clima.

Interventi sulla classe

Parallelamente agli interventi individuali è importante che si avvii nella classe un momento di riflessione e discussione, allo scopo di modificare le relazioni tra gli alunni/e. Il coordinatore di classe si informa prima con i singoli alunni/e coinvolti

direttamente, poi con la classe intera, esplicitando il problema e discutendo con gli alunni/e su quello che è accaduto.

Nel periodo successivo in classe si manterrà alta la vigilanza sulle relazioni tra gli alunni/e, favorendo un clima collaborativo tramite didattiche di Cooperative Learning, il reinserimento dei compagni/e ex vittime, svolgendo giochi di ruolo per rendere consapevoli gli alunni/e delle conseguenze delle loro azioni. Verranno inoltre condivise con gli alunni/e le regole ristabilite.

Sanzioni disciplinari

I comportamenti accertati che si configurano come forme di bullismo e cyberbullismo sono considerati come infrazioni gravi e vengono sanzionati sulla base del Regolamento Disciplinare degli alunni/e. La sanzione disciplinare, commisurata all'intensità dell'episodio, deve prevedere anche una attività riparatoria ed educativa che sia visibile e vada a beneficio della vittima e/o della classe.

La classe a sua volta dovrà fare una sua azione riparatoria nei confronti della vittima. Le sanzioni saranno particolarmente incisive per fatti di estrema gravità, preferibilmente con l'attivazione di percorsi educativi di recupero mediante lo svolgimento di attività di natura sociale, culturale e in generale a vantaggio della comunità scolastica. Vengono considerati deplorevoli e sanzionabili anche le condotte dei compagni/e sostenitori del bullo.

In caso di episodi gravi di cyberbullismo, il Dirigente informa i docenti e attiva le procedure previste dal protocollo e dal Regolamento di Disciplina.

Attenuanti e aggravanti:

1. il riconoscimento dell'errore, il risarcimento del danno e le scuse personali costituiscono attenuanti per le quali si applica la riduzione della pena (sono esclusi i reati di violenza fisica, psicologica o l'intimidazione del gruppo, specie se reiterata e il reato di cyberstalking);
2. aver commesso un'infrazione disciplinare, in concorso con una o più persone, costituisce aggravante per la quale si applica l'aumento della sanzione;
3. è possibile convertire parte della sanzione nello svolgimento di attività educative, definite in accordo con le famiglie secondo un piano educativo condiviso.

Nel caso in cui la segnalazione arrivi direttamente al Dirigente Scolastico, questi procederà come da prescrizioni normative:

- il fatto non costituisce reato o ipotizza un reato a querela di parte: il Dirigente Scolastico informa tempestivamente i soggetti esercenti la responsabilità genitoriale, ovvero i tutori dei minori coinvolti e attiva adeguate azioni di carattere educativo;
- il Dirigente Scolastico ha notizia di reato: sporge subito denuncia per iscritto all'autorità giudiziaria (Questura, Carabinieri, ecc.), anche quando non sia individuata la persona alla quale il reato è attribuito (art. 331 cpp);
- si evidenzia che sia la detenzione che la divulgazione di qualsiasi immagine di tipo sessuale o di esposizione di nudità (prodotto anche attraverso la pratica del "sexting") è considerato dalla legislazione vigente materiale pedopornografico; è, pertanto, necessario comunicarlo immediatamente al Dirigente Scolastico perché trasmetta la notizia tempestivamente, con relazione circostanziata, alla Polizia Postale o altra Forza di Polizia;
- quando un docente o un componente del personale A.T.A. viene a conoscenza di un comportamento ipotizzabile verosimilmente e ragionevolmente come reato ha l'obbligo di comunicarlo con la massima urgenza al Dirigente Scolastico perché adotti le misure necessarie.

Obbligo di denuncia

Devono essere denunciati dal Dirigente Scolastico alle autorità competenti (Carabinieri, Polizia, Polizia Postale) i seguenti reati perseguibili d'ufficio:

- rapina ed estorsione (art 628 c.p. e art 629 c.p.) riferibili a episodi di minacce e violenze per ottenere (o sottrarre)

oggetti o somme di denaro;

- lesioni gravissime (art 582 c.p. – 585 c.p.) e lesioni guaribili in più di 40 giorni o che comportano una diminuzione permanente della funzionalità di un organo;
- violenza sessuale (art 609 s.p.) commessa singolarmente o in gruppo; in questo caso viene considerata più grave e punita più severamente (per chiarire cosa si intende per violenza sessuale, bisogna considerare che ogni atto sessuale rientra in questa definizione, ad esempio: se un gruppo di minori blocca fisicamente una compagna palpeggiandola, rispondono tutti penalmente e non solo la persona che materialmente esegue l'atto);
- violenza o minaccia a pubblico ufficiale per alunni/e che hanno compiuto il quattordicesimo anno di età (art. 336 c.p. e art. 337 c. p.).

Gli episodi di bullismo perseguibili in caso di querela sono:

- lesioni, percosse, minacce, ingiurie, diffamazione, molestia, atti persecutori/Stalking (art. 582,581, 612, 591, 595 ,660,612 del Codice Penale): in questi casi è necessario informare la famiglia (e/o i Servizi Sociali) che può procedere alla querela, a sua discrezione. Il mancato avviso alla famiglia, da parte della Istituzione scolastica, è passibile di denuncia.

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.

Il nostro Istituto, nell'ottica di una fattiva e proficua collaborazione scuola-famiglia, in linea con il Patto di Corresponsabilità, invita a effettuare la segnalazione al Referente del bullismo e cyberbullismo, al Team Antibullismo e dell'Emergenza e al Dirigente dei casi avvenuti nell'ambito scolastico.

Qualora i casi si verificassero al di fuori di esso è possibile consultare gli indirizzi degli enti presenti sul territorio nazionale riportati nel Vademecum di Generazioni Connesse, suddiviso per Regioni.

Sul territorio svolgono attività a sostegno della sicurezza in rete:

- linea di ascolto 1.96.96 e chat di Telefono Azzurro: accolgono qualsiasi richiesta di ascolto e di aiuto da parte di bambini/e e ragazzi/e fino ai 18 anni o di adulti che intendono confrontarsi su situazioni di disagio/pericolo in cui si trova un minorenne. Il servizio di helpline è riservato, gratuito e sicuro, dedicato ai giovani o adulti che possono chattare, inviare e-mail o parlare al telefono con professionisti qualificati relativamente a dubbi, domande o problemi legati all'uso delle nuove tecnologie digitali e alla sicurezza online.
  - HELPLINE la linea d'ascolto di Generazioni Connesse
  - operativa 24 ore su 24
  - tel. 1.96.96 oppure www.commissariatodips.it
- Stop-it, il progetto di Save the Children Italia di lotta allo sfruttamento e all'abuso sessuale a danno dei minori su e tramite internet; utile per segnalare immagini e video pedopornografici.
- Servizi messi a disposizione dal "Safer Internet Center" per segnalazione di contenuti illegali e dannosi:
  - Telefono Azzurro: http://www.azzurro.it/emergenza-0;
  - "Clicca e Segnala" di Telefono Azzurro per segnalare contenuti illeciti (materiale pedopornografico) o potenzialmente dannosi per bambini e adolescenti - www.azzurro.it/it/clicca-e-segnala Stop-it di Save the Children www.stop-it.it;
- CO.RE.COM (Comitato Regionale per le Comunicazioni) Lombardia - Via Fabio Filzi, 22201124 - Milano – 02/67482300 - corecom@consiglio.regione.lombardia.it - www.corecomlombardia.it
- USR (Ufficio Scolastico Regionale) Lombardia - Via Pola, 11 20124 – Milano – 02/5746271
- Polizia postale "Ufficio Denunce" - Via Lattanzio Gambara, 12, 25124 – Brescia - 030/2913028
- Stazione Carabinieri competente per la scuola:
  - Comando Stazione Carabinieri Esine 0364/466649
  - Comando Stazione Carabinieri Piancogno 0364/466466

Queste strutture supportano la scuola in situazioni di emergenza, ma potrebbero anche essere coinvolte per poter svolgere momenti di formazione sul tema del cyberbullismo.

Altri allegati

- **Scheda di segnalazione**
- **Diario di bordo**
- **iGloss@ 1.0 l'ABC dei comportamenti devianti online**
- **Elenco reati procedibili d'ufficio**
- **Vademecum Generazioni Connesse**

ALLEGATO 1

Procedure operative per la gestione delle infrazioni alla e-Safety Policy

Ogni volta che un membro del personale o alunno/a viola la e-Safety Policy, la decisione finale sul livello di sanzioni sarà a discrezione del Dirigente Scolastico e rifletterà le procedure comportamentali e disciplinari della scuola.

Di seguito sono fornite alcune procedure operative come esemplificazione.

ALUNNI/E - INFRAZIONI POSSIBILI

- uso di siti non-educativi durante le lezioni;
- utilizzo non autorizzato di e-mail;
- uso non autorizzato del cellulare (o di altre nuove tecnologie) durante le lezioni;
- uso di instant messaging/siti di social networking;
- uso continuato messaggistica/chat room istantanea, siti di social networking, newsgroup;
- uso di materiale offensivo;
- rovinare o distruggere deliberatamente i dati di qualcuno, violare la privacy altrui o messaggi inappropriati, video o immagini su un sito di social networking;
- invio di un messaggio e-mail o MSN che è considerato molestia o azione di bullismo;
- cercare di accedere a materiale offensivo o pornografico;
- accedere deliberatamente allo scaricamento o alla diffusione di qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofobico o violento;
- trasmissione di materiale che viola i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati.

SANZIONI

Fare riferimento all'insegnante della classe/Referente/Dirigente Scolastico:

1. rimozione dei diritti di accesso a internet per un periodo;
2. ritiro dello smartphone;
3. contattare i genitori;
4. contattare le autorità competenti;
5. conservare le prove;
6. informare i provider di servizi di posta elettronica del mittente;
7. fare rapporto alle autorità competenti dove si sospetti la pedofilia o altre attività illegali.

PERSONALE SCOLASTICO - INFRAZIONI POSSIBILI

- uso di internet per attività personali non legate allo sviluppo professionale (shopping online, email personali, instant messaging ecc);
- utilizzo di supporti di memorizzazione dei dati personali (ad esempio, chiavette USB) senza considerare l'accesso e l'adeguatezza di qualsiasi file memorizzato;
- non implementare adeguate procedure di salvaguardia;
- qualsiasi comportamento sul World Wide Web che compromette la professionalità del personale nella scuola e nella comunità;

- uso improprio di primo livello di sicurezza dei dati, ad esempio uso illecito di password;
- violazione del copyright o della licenza per l'installazione di software;
- gravi danni intenzionali all'hardware o software del computer;
- qualsiasi tentativo deliberato di violare la protezione dei dati o di sicurezza informatica;
- creare, accedere, scaricare e diffondere deliberatamente qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofobico o violento;
- ricevere o trasmettere materiale che viola i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati;
- portare il nome della scuola in discredito.

SANZIONI

Fare riferimento al Referente/DSGA/Dirigente Scolastico:

1. avvertimento;
2. rimozione del pc in un luogo sicuro per garantire che non vi sia alcun ulteriore accesso;
3. far verificare tutte le attrezzature per garantire che non vi sia alcun rischio di alunni/e che accedono a materiali inappropriati.

ALLEGATO 2

PROCEDURA PER CASO DI PRESUNTO BULLISMO E VITTIMIZZAZIONE A SCUOLA

1. Prima segnalazione
2. Valutazione approfondita
3. Gestione del caso attraverso uno o più interventi:
    - approccio educativo con la classe;
    - intervento individuale;
    - gestione della relazione;
    - coinvolgimento la famiglia;
    - supporto intensivo a lungo termine e di rete.
4. Monitoraggio