



E-Safety Policy - in collaborazione con

1. Introduzione

1.1. Scopo dell'ePolicy

Attraverso l'ePolicy 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'ePolicy 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 ed educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

1.2. Ruoli e responsabilità

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 definire con chiarezza ruoli, compiti e responsabilità di ciascuna delle figure professionali che, a vario titolo, si occupano di gestione e programmazione delle attività formative, didattiche ed educative dell'Istituto e di **tutte le figure appartenenti alla comunità educante**. A tal proposito si rimanda: al documento integrale di ePolicy; 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.

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.

1.3. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

Il documento di ePolicy, approvato dal Collegio dei Docenti e dal Consiglio di Istituto, viene condiviso con tutta la comunità educante, ciascun attore scolastico è a sua volta promotore del documento. L'ePolicy viene condivisa e comunicata al personale, agli alunni/e, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;

- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;
- il Piano Triennale dell'Offerta Formativa (PTOF).

1.4. Gestione delle infrazioni alla ePolicy

La scuola gestirà le infrazioni all'ePolicy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

Per le discipline/condotte sanzionabili e relative sanzioni, in relazione all'uso improprio delle TIC, dei dispositivi e della Rete a scuola da parte degli alunni/e, alla gestione da parte del personale scolastico della strumentazione e/o la mancata sorveglianza e pronto intervento nel caso di infrazione da parte degli alunni/e, alle condotte educative dei genitori e/o in risposta a eventuali atteggiamenti comportamenti che possano risultare pericolosi per sé e/o dannosi per altri (culpa in educando e in vigilando), si rimanda al documento di ePolicy integrale e 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.

1.5. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

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;
- Regolamenti dei laboratori presenti nell'Istituto.

1.6. Integrazione dell'ePolicy con Regolamenti esistenti

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 verificano 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.

2. Formazione e Curricolo

2.1. Curricolo sulle competenze digitali per gli alunni/e

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 Primaria e Secondaria di primo grado.

2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica

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) sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo e inclusivo.

2.3. Formazione dei docenti sull'utilizzo consapevole e sicuro di internet e/o tecnologie digitali

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.

2.4. Sensibilizzazione delle famiglie e Patto di Corresponsabilità

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.

3. Gestione dell'infrastruttura e della strumentazione ICT della e nella scuola

3.1. Protezione dei dati personali

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.

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

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

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.

3.2. Accesso a internet

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

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.

3.3. Strumenti di comunicazione online

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.

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 a 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 “Sogi” 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.

3.4. Strumentazione personale

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.

4. Rischi online: conoscere, prevenire e rilevare

4.1. Sensibilizzazione e prevenzione

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

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

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.

4.2. Cyberbullismo: che cos'è e come prevenirlo

Il cyberbullismo è una forma di prepotenza virtuale messa in atto attraverso l'uso di internet e delle tecnologie digitali.

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 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.

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

- **flaming**: 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.

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

Nel caso in cui si ipotizzi che ci si possa trovare di fronte a una fattispecie di reato si potrà far riferimento agli uffici preposti: 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 (19696): operatori esperti e preparati sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che dei/le 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.

4.3. Hate speech: che cos'è e come prevenirlo

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.

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.

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.

4.4. Dipendenza da internet e gioco online

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

L'Istituto 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.

4.5. Sexting

Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti medialmente sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

4.6. Adescamento online

Il **grooming** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenzialmente abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata.

4.7. Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, **concrete o simulate** o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

L'Istituto ritiene che per prevenire il "sexting", il "grooming/adescamento online" e la "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.

5. Segnalazione e gestione dei casi

5.1. Cosa segnalare

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.

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che un alunno/a possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e standardizzate riportare nell'ePolicy.

5.2. Come segnalare: quali strumenti e a chi

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.

5.3. Gli attori sul territorio per intervenire

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".

Sul territorio svolgono attività a sostegno della sicurezza in rete:

- linea di ascolto 1.96.96 (www.commissariatodips.it) e chat di Telefono Azzurro
HELPLINE la linea d'ascolto di Generazioni Connesse
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, 22 20124 - 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](tel:0302913028)
- Stazione Carabinieri competente per la scuola:
Comando Stazione Carabinieri Esine [0364/466649](tel:0364466649)
Comando Stazione Carabinieri Piancogno [0364/466466](tel:0364466466)

Il nostro piano di azioni

Sulla base delle "Linee guida per l'uso positivo delle tecnologie digitali e della prevenzione dei rischi nelle scuole", vengono assunti i seguenti punti per una collaborazione sinergica tra scuola-famiglia-servizi territoriali, al fine di creare un modello composito e lineare di azioni condivise:

- coinvolgimento di tutti gli attori della scuola: alunni/e, docenti, genitori e personale ATA, per l'affermazione di un modello di scuola come comunità;
- alleanza educativa tra scuola e famiglia;
- interventi educativi e azioni di supporto, quale prevenzione per eventuali comportamenti a rischio;
- misure preventive specifiche di tutela anche con l'ausilio di attori territoriali, come Polizia postale e ATS per servizi specialistici;
- promozione dell'educazione al rispetto;
- sviluppo del pensiero critico;
- promozione dell'Educazione Civica Digitale.

Allegati

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



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

Avvisa il referente per il cyberbullismo (e/o il referente indicato nell'ePolicy) e il Dirigente Scolastico che convoca il CDC.

A) Se c'è fattispecie di reato - seguite le procedure della scuola

B) Se non c'è fattispecie di reato

- Richiedi la consulenza dello psicologo/a scolastico

- Informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto), se possibile con la presenza dello psicologo/a, 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.

- Valuta come coinvolgere gli operatori scolastici su quanto sta accadendo.

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

- Cerca di capire il livello di diffusione dell'episodio nell'Istituto e parla della necessità di non diffondere ulteriormente online i materiali.

- Parla del cyberbullismo e delle sue conseguenze (non nominare gli alunni coinvolti). Suggestisci di chiedere aiuto per situazioni di questo tipo. Prevedi un momento laboratoriale in modo da facilitare l'elaborazione della situazione.

- a seconda della situazione trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.

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).



© All rights reserved Generazioni Connesse 2019



Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



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

Sonda il clima di classe, ascoltando i ragazzi e monitorando ciò che accade (ma senza fare indagini o interrogatori).
Cerca di capire il livello di diffusione dell'episodio a livello di Istituto.

Parla in classe del cyberbullismo e delle sue conseguenze (non nominare gli alunni che sospetti coinvolti). Suggestisci di **chiedere aiuto** per situazioni di questo tipo.
Proponi attività in classe sull'empatia e sul riconoscimento delle emozioni (proprie e altrui)

Se emergono evidenze passa allo schema successivo

Condividi con il referente per il cyberbullismo (e/o il referente indicato nell'e-policy): valuta con lui/loro le possibili strategie di intervento.

Valuta se è il caso di avvisare il consiglio di classe.
Valuta se è il caso di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.

Informa i/le ragazzi/e su ciò che dice la legge italiana su cyberbullismo L. 71/2017)
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

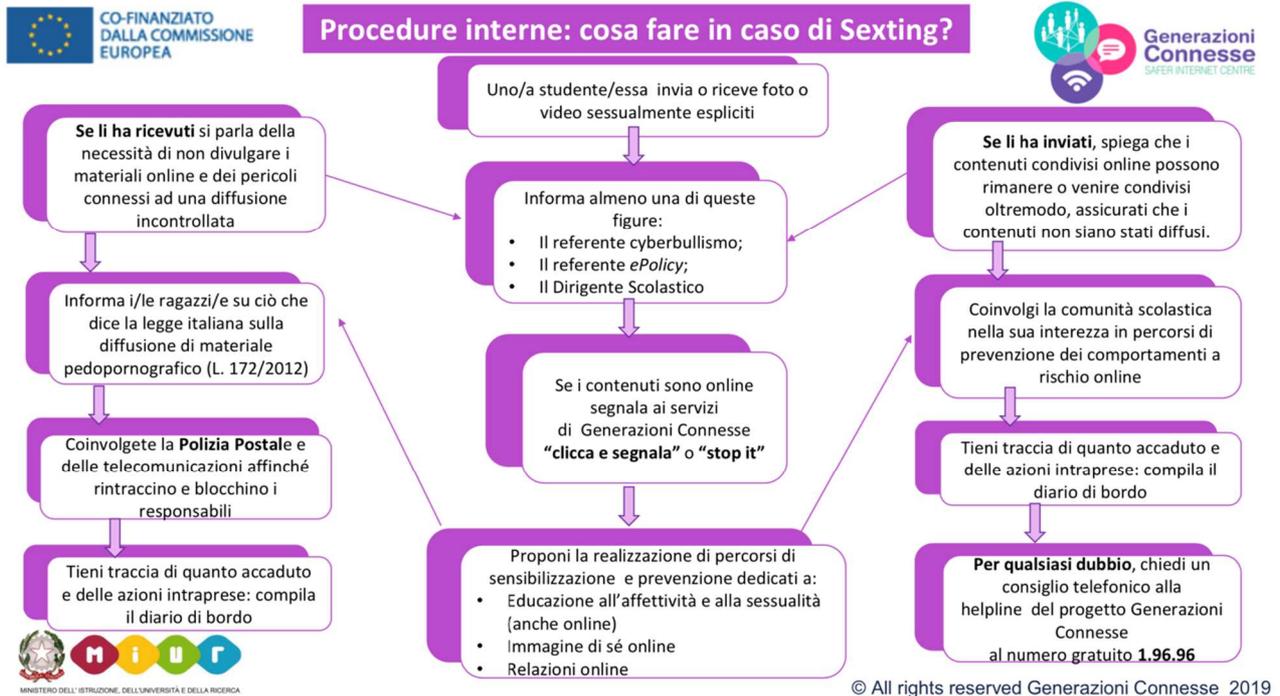
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

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

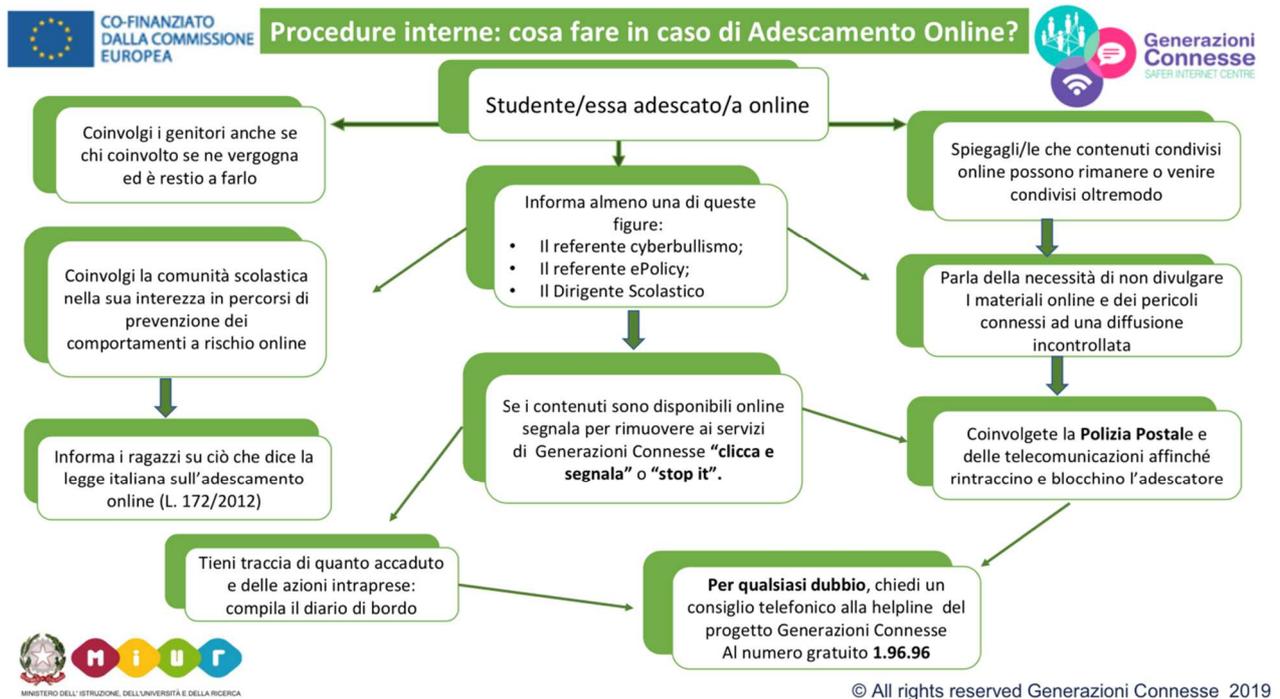


© All rights reserved Generazioni Connesse 2019

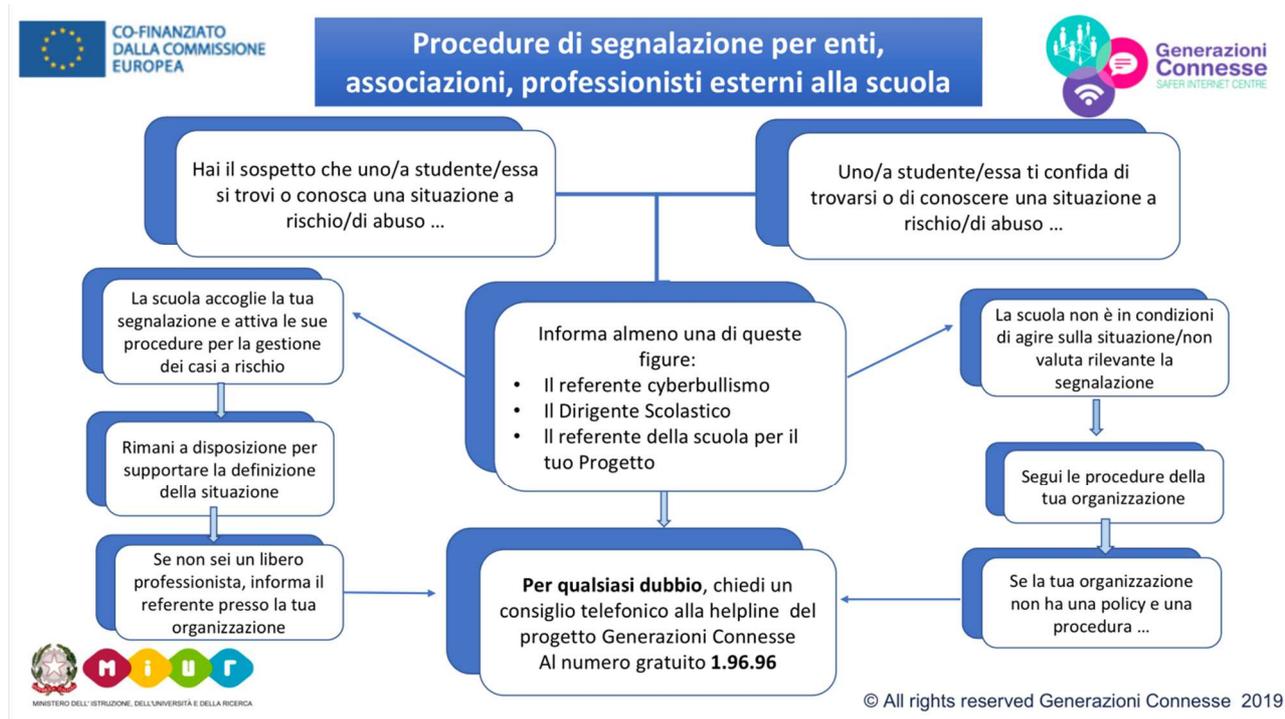
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola

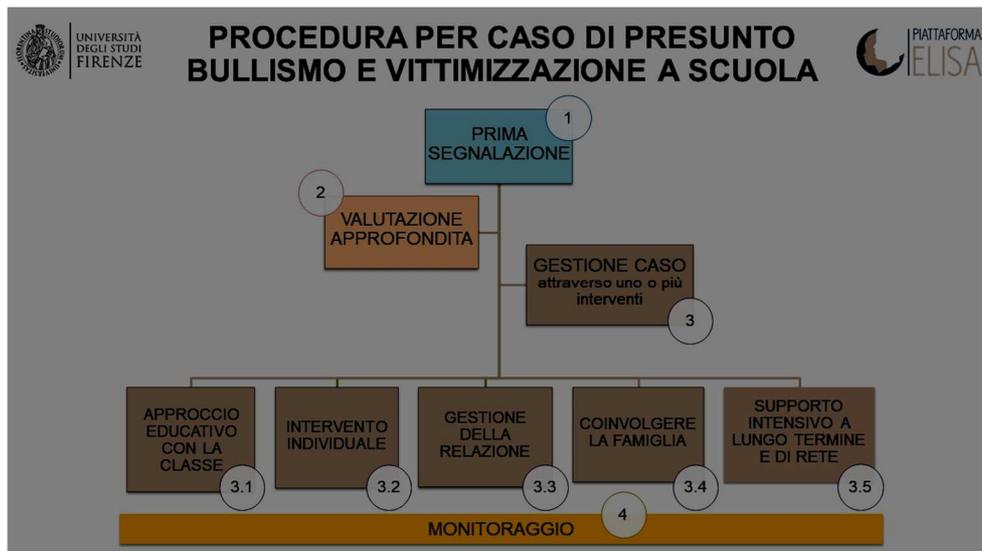


Altri allegati

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

Per le procedure operative per la gestione delle infrazioni alla e-Safety Policy e relative possibili infrazioni si rimanda al documento integrale di ePolicy (v. allegato 1).

Procedura per caso di presunto bullismo e vittimizzazione a scuola (v. allegato 2)



1. **Prima segnalazione** - Scheda di prima segnalazione in allegato all'ePolicy (v. allegato D)

2. **Valutazione approfondita**

In base alle informazioni acquisite dalle diverse sezioni (gravità della sintomatologia della vittima, gravità della sintomatologia del bullo, caratteristiche del quadro contestuale del gruppo classe e della famiglia), si delinea il **livello di priorità dell'intervento**.

LIVELLO DI RISCHIO DI BULLISMO E DI VITTIMIZZAZIONE	LIVELLO SISTEMATICO DI BULLISMO E VITTIMIZZAZIONE	LIVELLO DI URGENZA DI BULLISMO E VITTIMIZZAZIONE
Codice verde	Codice giallo	Codice rosso
Situazione da monitorare con interventi preventivi nella classe	Interventi indicati e strutturati a scuola e in sequenza coinvolgimento della rete se non ci sono risultati	Interventi di emergenza con supporto della rete

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** - permette al Team Antibullismo e dell'Emergenza di verificare la presenza di cambiamenti a seguito dell'intervento/degli interventi messi in atto e di valutarne l'efficacia, annotando ogni osservazione.

Se il monitoraggio evidenzia che la situazione non è risolta, allora il processo deve iniziare di nuovo