

Documento di ePolicy
IC N. 4 - FORLI'

VIA FELICE ORSINI 48 - 47121 - FORLI'
Forlì-Cesena (FC) - Emilia-Romagna
Data di approvazione: 03/06/2026 - 14:33

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

1. Sensibilizzazione e prevenzione
2. Il Curricolo Digitale
3. IL KIT DIDATTICO

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.

L'E-policy rappresenta l'impegno ufficiale del nostro Istituto Comprensivo nel guidare ogni membro della comunità educante verso un uso della rete che sia:

- *Consapevole*: Capire che ogni azione online lascia una "traccia";
- *Critico*: Saper distinguere tra informazioni attendibili e manipolazioni, proteggendosi dai rischi;
- *Efficace:* Sfruttare le potenzialità della tecnologia per migliorare l'apprendimento e la creatività.

Le Tecnologie dell'Informazione e della Comunicazione (TIC) sono, oggigiorno, un pilastro imprescindibile del percorso educativo e dell'apprendimento. In linea con la Raccomandazione del Consiglio Europeo del 2018 che include le competenze digitali tra le abilità chiave per l'apprendimento permanente, la scuola ha il compito primario di dotare studenti e studentesse di tali competenze sin dall'infanzia. Data la crescente complessità del mondo digitale, una **E-policy di istituto risulta necessaria al fine di prevenire situazioni problematiche e di riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti digitali**.

La E-policy esprime la nostra visione educativa in relazione all'educazione al digitale, focalizzandosi sui seguenti ambiti:

1. Approccio Formativo: La strategia educativa adottata per lo sviluppo delle competenze digitali, trattando temi essenziali come la privacy, la sicurezza online e l'integrazione delle tecnologie digitali nei percorsi didattici.
2. Norme Operative: La definizione delle regole di condotta e delle procedure specifiche per l'utilizzo delle TIC all'interno dell'ambiente scolastico.
3. Misure Preventiva: Le iniziative di sensibilizzazione e prevenzione per contrastare i comportamenti on-line a rischio.
4. Gestione del Rischio: I protocolli stabiliti per la rilevazione, segnalazione e gestione tempestiva di tutte le situazioni critiche correlate a un impiego inappropriato delle tecnologie.

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.

Informativa generale di comportamento:

1. **Per i docenti del nostro istituto:**

In presenza di segnali o sospetti relativi a comportamenti impropri (come il cyberbullismo), il docente è tenuto ad agire con massima tempestività.

Procedura di allerta: non limitarsi a una segnalazione verbale, ma redigere un resoconto scritto dettagliato. Questo va inoltrato al referente per il bullismo/cyberbullismo o al gruppo di lavoro dedicato.

Valutazione collegiale: Il team specializzato analizza l'accaduto in stretta collaborazione con la Dirigenza. Se necessario si riunisce il cdc.

Risoluzione: In base alla gravità, l'Istituto deciderà se attivare percorsi educativi di sensibilizzazione o se procedere interpellando le autorità.

In questi casi verranno presi in considerazione il regolamento d'istituto per la prevenzione ed il contrasto del bullismo e cyberbullismo, presente sul sito del nostro istituto.

2. **Per esperti ed enti esterni al nostro istituto:**

Chiunque collabori con l'Istituto deve farsi garante di un ambiente protetto, basato sul rispetto reciproco e sulla cura educativa. Ogni interazione deve essere seria e professionale, evitando qualsiasi atteggiamento che possa risultare inadeguato. Ogni decisione deve mettere al primo posto il benessere dello studente. È essenziale saper ascoltare con attenzione i ragazzi, dando valore ai loro racconti o alle loro preoccupazioni. È categoricamente proibito invadere la sfera privata e l'intimità degli alunni. Non è ammessa alcuna forma di tolleranza verso azioni illegali, violente o che possano compromettere l'integrità fisica e psicologica dei minori.

3. **Per gli STUDENTI che hanno accesso alle tecnologie informatiche della scuola e alla piattaforma:**

Si fa riferimento al regolamento interno di disciplina e all'informativa sulla privacy consegnata alle famiglie ad ogni inizio anno scolastico.

Sarà cura dei docenti istruire i ragazzi ad una educazione consapevole della gestione dei loro account istituzionali e dei device di proprietà della scuola.

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.

Il documento di E-policy viene condiviso con tutta la comunità educante, sottolineando compiti, funzioni e attività reciproche. La condivisione del documento avviene attraverso:

- La pubblicazione del documento sul sito istituzionale della scuola;
- L'integrazione all'interno del Patto di Corresponsabilità educativa scuola-famiglia;
- L'integrazione nell'aggiornamento del PTOF;
- L'intergrazione nel Regolamento di disciplina;
- L'ntegrazione nel prossimo aggiornamento del regolamento d'istituto per la prevenzione ed il contrasto del bullismo e cyberbullismo;
- Copia consultabile in segreteria (pdf) e resa disponibile sul sito.

Il documento è approvato da:

- Collegio dei Docenti con delibera n°60 dell'8 aprile 2026;
- Consiglio di Istituto con delibera n°34 del 14 maggio 2026.

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.

1. **Il curricolo sulle competenze digitali per la comunità educante (il DigComp 3.0)**

Dal curricolo d'istituto: 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. Tali competenze digitali si integrano trasversalmente e verticalmente con i curricoli delle singole discipline in tutti gli ordini scolastici dell'Istituto, secondo le Linee Guida Nazionali ed entrano a far parte del curricolo verticale dell'educazione civica.

2. 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'e-Policy non risiede solo nel suo contenuto normativo, ma nella sua capacità di diventare un patrimonio condiviso da tutta la comunità scolastica. Per garantire che le linee guida sull'uso consapevole delle tecnologie siano realmente messe in atto, la scuola adotta diverse strategia di diffusione, differenziate per destinatari e contesti.

Per le famiglie sarà resa disponibile l'e-policy sul sito, data comunicazione sui canali istituzionali quali affissioni all'albo e circolari in bacheca. E' importante informare i genitori sulle condotte che si dovranno adottare a scuola e, in generale, offrire loro consigli da mettere in pratica con i propri figli, in riferimento ai rischi connessi a un uso distorto della rete da parte degli studenti.

A tal proposito appare buona prassi:
- elaborare regole condivise sull'uso delle tecnologie digitali da parte dei genitori nelle comunicazioni con la scuola e con i docenti (es. mail, gruppo whatsapp, sito della scuola, ecc.) e informarli adeguatamente anche riguardo alle regole per gli studenti;
- fornire ai genitori consigli o linee guida sull'uso delle tecnologie digitali nella comunicazione con i figli e in generale in famiglia (ad es. a tal fine si potrà fare riferimento alla sezione dedicata ai genitori del sito www.generazioniconnesse.it).

Formazione personale scolastico

Il nostro istituto riconosce e favorisce la partecipazione del personale ad iniziative promosse direttamente dalla scuola con l'aiuto dell'animatore digitale; erogate e suggerite dalle reti di scuole e dall'Amministrazione.

- **Come comunicare e condividere l'E-Policy 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 scuola promuove attivamente sinergie con attori pubblici e privati (Enti Locali, Forze dell'Ordine, Associazioni, Aziende tecnologiche) per arricchire l'offerta formativa sull'Educazione Civica Digitale. Tuttavia, affinché tali interventi siano efficaci e sicuri, la condivisione dell'E-Policy diventa il prerequisito fondamentale per ogni collaborazione ed ogni progettualità terrà conto dei contenuti di questo documento. Qualora richiesto, la scuola si impegna a:

- Trasmettere su richiesta formale l'E-Policy d'Istituto ai referenti dei progetti esterni. Ogni esperto o formatore è tenuto a prenderne visione e ad uniformare il proprio intervento ai principi di sicurezza e protezione dei minori adottati dalla scuola. L'E-Policy sarà comunque mantenuta permanente sul sito web.

- Richiedere il rispetto del Regolamento sull'uso dei dispositivi e la policy sulla gestione dei dati personali (GDPR).

Trasparenza verso la Comunità Educante
La scuola comunica alle famiglie l'elenco dei partner esterni coinvolti (attraverso circolari o durante gli incontri con i genitori), esplicitando:

1. Chi realizza l'intervento.

2. Quali strumenti digitali verranno utilizzati.

3. In che modo l'intervento si ricollega ai valori espressi nell'E-Policy d'Istituto

La scuola si riserva il diritto di sospendere collaborazioni con soggetti esterni che, nello svolgimento delle attività, non rispettino le norme di sicurezza digitale o adottino linguaggi non conformi alla sensibilità dei minori e alle linee guida dell'E-Policy.

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

I Piani di Azione dell'E-Policy fanno parte della programmazione scolastica, definendo gli obiettivi concreti per diffondere la cultura della sicurezza digitale e rendere operativi i suoi protocolli. Rappresentano il mezzo attraverso cui l'istituto traduce i principi teorici in impegni misurabili e responsabilità condivise. Attraverso questi piani, la scuola si impegna attivamente su quattro fronti essenziali:

- **Analisi dei Bisogni**: Rilevazione costante delle necessità e dei rischi emergenti all'interno della comunità scolastica.
- **Crescita Formativa:** Realizzazione di percorsi di formazione e/o aggiornamento mirati
- **Diffusione della Consapevolezza:** Campagne informative sull'uso critico della rete e delle tecnologie.
- **Controllo e Qualità:** Monitoraggio periodico e valutazione dei risultati raggiunti

1° ANNO DI ATTIVITA' CON L'E-Policy

Azioni da svolgere *entro una annualità scolastica*:

MODULO I

1. Presentazione dell'E-Policy durante un'attività collegiale;
2. Diffusione durante alcuni eventi organizzati dalla scuola (es. Open Day);
3. Diffusione alle famiglie attraverso versioni semplificate dell'e-Policy e informativa su sito web e canali social;
4. Organizzazione evento informativo.

MODULO II

1. Effettuare una rilevazione del fabbisogno formativo dei docenti sui temi dell'educazione civica digitale

2° ANNO DI ATTIVITA' CON L'E-Policy

Azioni da svolgere *entro due annualità scolastiche:*

1. Incontro informativo rivolto agli studenti dell'Istituto e alle famiglie, anche attraverso il supporto di esperti/associazioni esterne.

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

Il nostro istituto si avvarrà delle risorse messe a disposizione da Generazioni Connesse quali

- Kit Didattico
- Area formazione di GC (per docenti, famiglie, studenti/sse con E-Policy)
- Canale Youtube GC (webinar, video-stimolo, serie per target differenti)
- Canale Instagram GC
- Canale Facebook GC
- Canale Tik-Tok GC

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.

La nostra scuola promuove attivamente l'aggiornamento professionale del corpo docente in ambito delle TIC.

A tal fine, l'Istituto non solo valorizza le proposte formative ministeriali, di rete o interne (coordinate dall'animatore digitale), ma incentiva anche l'autoformazione individuale. Viene inoltre garantita la proposta istituzionale di percorsi specifici dedicati all'innovazione delle metodologie e degli strumenti didattici digitali, sia con organizzazione scolastica che eventualmente consigliata con percorsi esterni.

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.

CURRICOLO D'ISTITUTO:

EDUCAZIONE CIVICA NELLA SCUOLA PRIMARIA

NUCLEO TEMATICO	TRAGUARDO PER LO SVILUPPO DELLE COMPETENZE	OBIETTIVI DI APPRENDIMENTO

CITTADINANZA DIGITALE	Traguardo per lo sviluppo delle competenze n. 10 Sviluppare la capacità di accedere alle informazioni, alle fonti, ai contenuti digitali, in modo critico, responsabile e consapevole.	- Ricercare in rete semplici informazioni, distinguendo dati veri e falsi. - Utilizzare le tecnologie per elaborare semplici prodotti digitali. - Riconoscere semplici fonti di informazioni digitali.
	Traguardo per lo sviluppo delle competenze n. 11 Interagire con gli altri attraverso le tecnologie digitali consentite, individuando forme di comunicazione adeguate ai diversi contesti di relazione, adottando e rispettando le regole comportamentali proprie di ciascun contesto comunicativo.	- Interagire con strumenti di comunicazione digitale, quali tablet e computer. - Conoscere e applicare semplici regole per l'utilizzo corretto di strumenti di comunicazione digitale, quali tablet e computer. - Conoscere e applicare le principali regole di partecipazione alle classi virtuali e alle piattaforme didattiche.
	Traguardo per lo sviluppo delle competenze n. 12 Gestire l'identità digitale e i dati della rete, salvaguardando la propria e altrui sicurezza negli ambienti digitali, evitando minacce per la salute e il benessere fisico e psicologico di sé e degli altri.	- Conoscere il significato di identità e di informazioni personali in semplici contesti digitali di uso quotidiano. - Conoscere i rischi connessi con l'utilizzo degli strumenti digitali in termini di sicurezza personale. - Conoscere semplici modalità per evitare rischi per la salute e minacce al benessere psico-fisico quando si utilizzano le tecnologie digitali. Educare al contrasto di tutte le forme di bullismo e cyberbullismo.
	Traguardo per lo sviluppo delle competenze n. 3 Rispettare le regole e le norme che governano la democrazia, la convivenza sociale e la vita quotidiana in famiglia, a scuola, nella comunità, al fine di comunicare e rapportarsi correttamente con gli altri, esercitare consapevolmente i propri diritti e doveri per contribuire al bene comune e al rispetto dei diritti delle persone	- Conoscere ed applicare le regole vigenti in classe e nei vari ambienti della scuola (mensa, palestra, laboratori, cortili) e partecipare alla loro eventuale definizione o revisione. Conoscere il principio di uguaglianza nella consapevolezza che le differenze possono rappresentare un valore quando non si trasformano in discriminazioni. - Conoscere i principali fattori di rischio dell'ambiente scolastico, adottare comportamenti idonei a salvaguardare la salute e la sicurezza proprie e altrui e contribuire a definire comportamenti di prevenzione dei rischi. - Conoscere e applicare le principali norme di circolazione stradale.
	Traguardo per lo sviluppo delle competenze n. 4 Tutela della salute e del benessere psicofisico	- Conoscere e attuare le principali regole per la cura della salute, della sicurezza e del benessere proprio e altrui, a casa, a scuola, nella comunità, dal punto di vista igienico-sanitario, alimentare, motorio, comportamentale. Conoscere i rischi e gli effetti dannosi di ogni tipologia di droga.
	Traguardo per lo sviluppo delle competenze n. 10 Sviluppare la capacità di accedere alle informazioni, alle fonti, ai contenuti digitali, in modo critico, responsabile e consapevole.	- Ricercare in rete semplici informazioni, distinguendo dati veri e falsi. - Utilizzare le tecnologie per elaborare semplici prodotti digitali. - Riconoscere semplici fonti di informazioni digitali.
	Traguardo per lo sviluppo delle competenze n. 11 Interagire con gli altri attraverso le tecnologie digitali consentite, individuando forme di comunicazione adeguate ai diversi contesti di relazione, adottando e rispettando le regole comportamentali proprie di ciascun contesto comunicativo.	- Interagire con strumenti di comunicazione digitale, quali tablet e computer. - Conoscere e applicare semplici regole per l'utilizzo corretto di strumenti di comunicazione digitale, quali tablet e computer. - Conoscere e applicare le principali regole di partecipazione alle classi virtuali e alle piattaforme didattiche.
	Traguardo per lo sviluppo delle competenze n. 12 Gestire l'identità digitale e i dati della rete, salvaguardando la propria e altrui sicurezza negli ambienti digitali, evitando minacce per la salute e il benessere fisico e psicologico di sé e degli altri.	- Conoscere il significato di identità e di informazioni personali in semplici contesti digitali di uso quotidiano. - Conoscere i rischi connessi con l'utilizzo degli strumenti digitali in termini di sicurezza personale. - Conoscere semplici modalità per evitare rischi per la salute e minacce al benessere psico-fisico quando si utilizzano le tecnologie digitali. Educare al contrasto di tutte le forme di bullismo e cyberbullismo.

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.

L’Istituto pone al centro della propria offerta formativa la cittadinanza digitale attiva, impegnandosi a fornire ai docenti gli strumenti necessari per guidare gli studenti in un uso sicuro del web tramite:

- **Formazione Continua:** proposta di corsi di aggiornamento dedicati alla prevenzione dei rischi online e alla didattica digitale consapevole. Le attività saranno coordinate da figure chiave interne, come l'Animatore digitale.

- **Sinergia con il Territorio**: Per offrire prospettive multidisciplinari, la scuola collabora con consulenti esterni, amministrazioni locali, servizi socio-educativi e associazioni specializzate.

- Si incoraggia vivamente tutto il corpo docente a usufruire dei **percorsi formativi disponibili sulla piattaforma ministeriale Generazioni Connesse**, punto di riferimento nazionale per la sicurezza in rete.

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.

Al fine di garantire la massima tutela dei dati personali trattati, l'Ente ha provveduto alla nomina di un Responsabile della Protezione dei Dati (RPD), figura nota anche con l'acronimo inglese DPO (Data Protection Officer).

Funzioni e collocazione organizzativa

L'RPD opera in qualità di garante interno indipendente, agendo in conformità a quanto previsto dagli articoli 37, 38 e 39 del Regolamento UE 2016/679 (GDPR). Le sue funzioni principali comprendono:

Attività di sorveglianza: monitorare l'osservanza della normativa vigente e delle policy interne in merito a ogni operazione di trattamento (raccolta, conservazione e utilizzo dei dati).

Consulenza tecnica: fornire pareri e supporto all'Ente affinché la protezione dei dati sia integrata fin dalla progettazione di ogni nuovo servizio o processo (privacy by design).

Cooperazione istituzionale: fungere da unico punto di contatto con l'Autorità Garante per la Protezione dei Dati Personali per ogni questione relativa al trattamento.

Contatto per l'interessato

L'RPD costituisce il punto di riferimento per gli utenti (interessati) che desiderino ricevere chiarimenti in merito alla gestione dei propri dati personali. In particolare, è possibile rivolgersi al Responsabile per:

- Richiedere delucidazioni sulle finalità e sulle modalità di trattamento dei dati.

- Esercitare i diritti previsti dal Regolamento (quali accesso, rettifica, cancellazione o limitazione del trattamento).
- Segnalare eventuali criticità, dubbi o presunte violazioni della riservatezza.

Nello svolgimento dei propri compiti, l'RPD opera in piena autonomia e non riceve istruzioni dall'Ente in merito all'esecuzione delle proprie verifiche o alla gestione delle istanze pervenute, garantendo così l'imparzialità e la tutela degli interessati.

Dati di contatto del Responsabile della Protezione dei Dati RDP

Ai sensi dell'art. 37, par. 7 del GDPR, si riportano di seguito i canali di contatto del RDP d'Istituto:

SOCIETA': VARGIUSCUOLA SRL, Via dei Tulipani, 7 09032 Assemini (CA)

TEL: 333 6477109

PEC: vargiuscuola@pec.it

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.

REGOLAMENTO GOOGLE SUITE FOR EDUCATION

L'Istituto attiva la piattaforma Google Workspace come strumento esclusivo di supporto alla didattica e alla comunicazione istituzionale. Il servizio è rivolto a studenti, docenti e personale ATA. L'account è uno strumento di lavoro: ogni uso personale o ricreativo è vietato.

1. Credenziali e Accesso

Assegnazione: Ogni utente riceve un account personale: *nome.cognome@ic4forli.edu.it*

Al primo accesso è obbligatorio cambiare la password provvisoria. La password è segreta e l'utente è l'unico responsabile delle attività compiute con il proprio profilo. In caso di smarrimento, il reset va richiesto alle figure di riferimento.

2. Regole di Comportamento (Netiquette)

L'utente si impegna a:

- Utilizzare un linguaggio rispettoso e non lesivo della dignità altrui.
- Non condividere materiale protetto da copyright o contenuti inappropriati (offensivi, violenti o pornografici).
- Vietato lo Spam: È proibito l'invio di pubblicità o email massive non autorizzate.
- Niente acquisti: L'account non può essere usato per transazioni economiche o iscrizioni a siti non didattici.

3. Responsabilità

L'utente è l'unico responsabile dei contenuti caricati o inviati. L'Istituto è sollevato da ogni responsabilità per danni causati dall'utente a terzi o per la perdita accidentale di dati.

4. Durata e Cessazione del Servizio

L'account resta attivo per tutta la permanenza presso l'Istituto. Alla cessazione (licenziamento, trasferimento o fine contratto): studenti e personale hanno a disposizione un periodo per il recupero dei dati salvati. Decorso il periodo di sospensione, l'account e tutti i contenuti verranno eliminati definitivamente.

5. Privacy e Sicurezza dei Dati

Il trattamento dei dati è conforme al GDPR (Regolamento UE 679/2016). I dati sono usati solo per fini istituzionali. L'utente, attivando l'account, accetta le norme sulla privacy di Google per il settore Education, che garantiscono l'assenza di pubblicità e profilazione commerciale.

6. Sanzioni

In caso di violazione del presente regolamento, l'Istituto può:

- Sospendere o revocare l'account immediatamente.
- Applicare le sanzioni disciplinari se previste dal Regolamento d'Istituto.
- Segnalare eventuali illeciti alle autorità competenti.

L'attivazione dell'account equivale alla sottoscrizione e accettazione incondizionata delle norme sopra indicate.

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.

Al fine di garantire la sicurezza dei dati, la protezione della riservatezza e il regolare svolgimento delle attività istituzionali, vige all'interno dell'Istituto il divieto di utilizzo di telefoni cellulari, smartphone, tablet o altri dispositivi elettronici di proprietà personale collegati alla rete istituzionale per finalità lavorative o didattiche. Qualora lo svolgimento delle mansioni o delle attività didattiche richieda l'uso di strumenti tecnologici, la scuola provvede alla fornitura di dispositivi di proprietà dell'istituto, debitamente configurati e monitorati secondo i massimi standard di sicurezza previsti dal GDPR, da richiedere presso la segreteria in comodato d'uso. Per l'utilizzo di dispositivi personali da collegare alla rete, è possibile fare formale richiesta per autorizzazione.

Si ricorda che la circolare ministeriale N. 5274 dell'11 luglio 2024 " **Disposizioni in merito all'uso degli smartphone e del registro elettronico nel primo ciclo di istruzione - A.S. 2024 -2025"**, dispone il divieto di utilizzo in classe del telefono smartphone, ...anche a fini educativi e didattici, per gli alunni dalla scuola d'infanzia fino alla secondaria di primo grado, salvo i casi in cui lo stesso sia previsto dal Piano Educativo Individualizzato o dal Piano Didattico Personalizzato, come supporto rispettivamente agli alunni con disabilità o con disturbi specifici di apprendimento ovvero per casi di eccezionale necessità per i quali le istituzioni scolastiche possano autorizzare l'uso (ad esempio per motivi di salute)».

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.

L'assetto organizzativo della scuola per la prevenzione e la gestione di fenomeni di bullismo e cyberbullismo, in linea con le Linee di orientamento MIUR 2015 e la Legge 71/2017 e il regolamento interno per la prevenzione e contrasto dei fenomeni di Bullismo/cyberbullismo.

Riferimenti:

- Referente per Bullismo e Cyberbullismo
- Team Antibullismo e per l'Emergenza
- Docenti o coordinatori di classe.

Come Segnalare un Episodio
Per denunciare o segnalare un episodio di bullismo o cyberbullismo di cui si è stati vittima o di cui si è venuti a conoscenza, è possibile scegliere una delle seguenti modalità:

1. Cassetta "BULLY BOX": Depositare una denuncia riservata nella cassetta presente a scuola.
2. Modulo di Segnalazione: Compilare l'apposito modulo (sul sito) e consegnarlo al Coordinatore di Classe.
3. Email: Inoltrare una comunicazione all'indirizzo email: bullismo@ic4forli.edu.it.

Riferimento al regolamento di istituto sulla gestione dei casi di bullismo e cyberbullismo.

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.

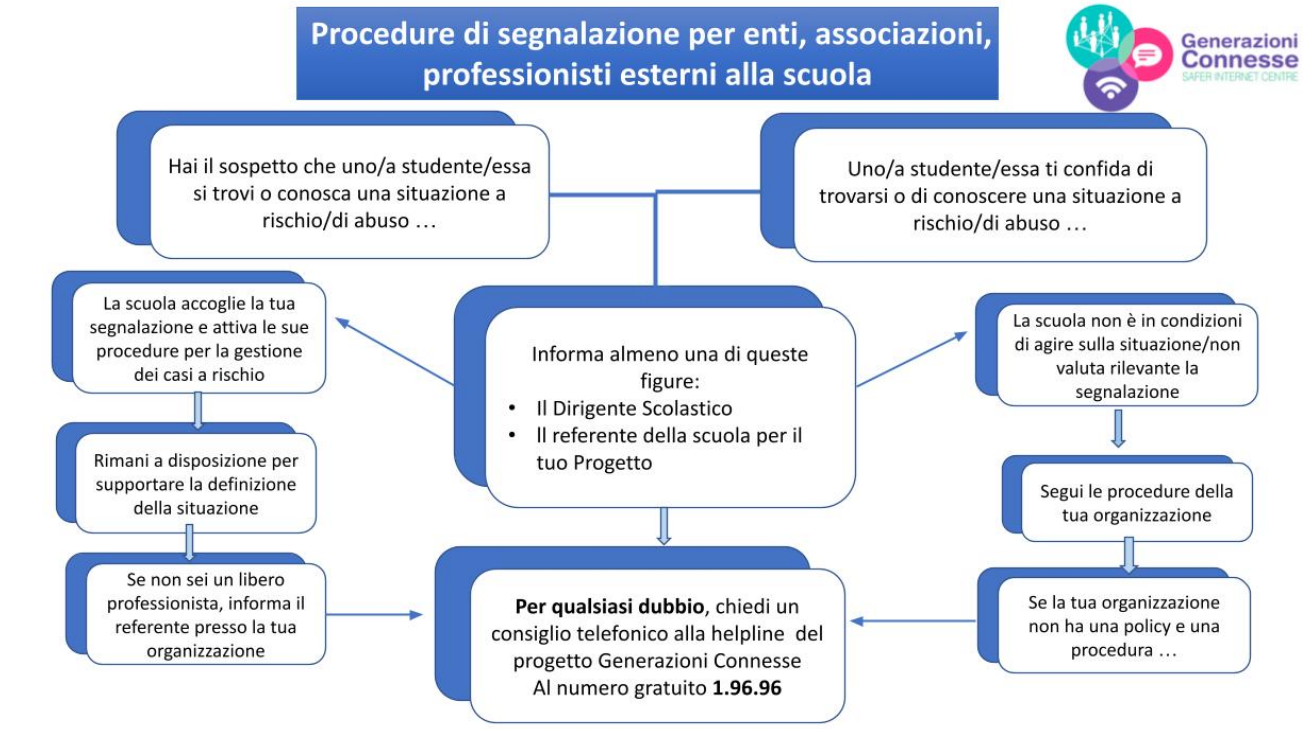
Strumenti a disposizione di studenti/esse

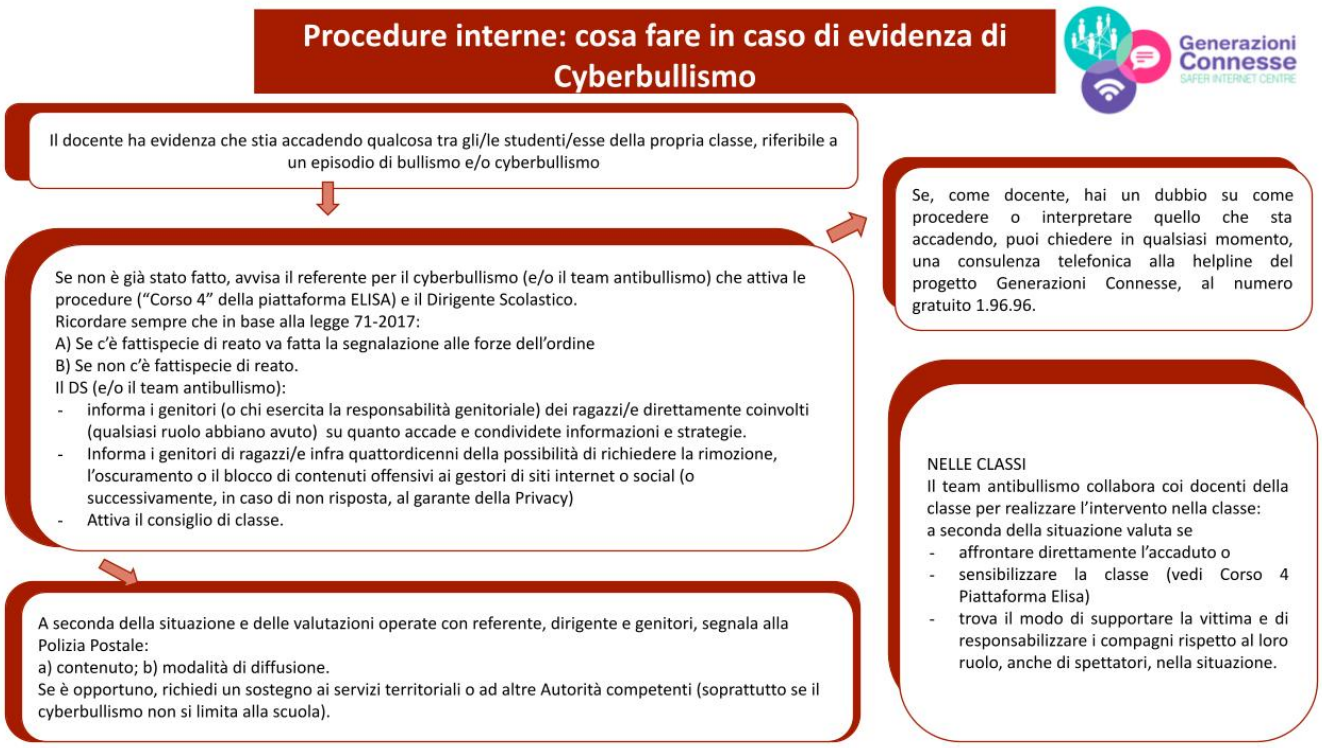
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola; sportello di ascolto con professionisti; docente referente per le segnalazioni.

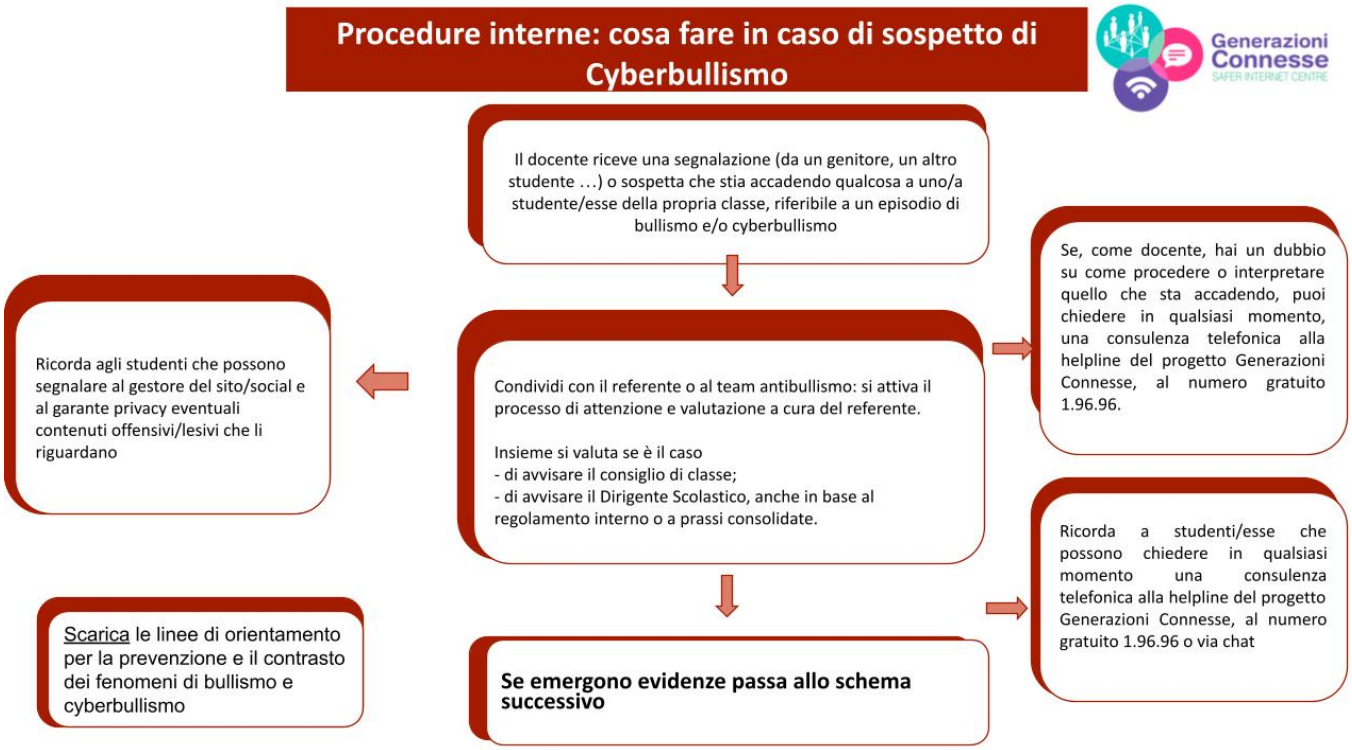
In particolare, sarebbe utile che la scuola attivi un sistema di segnalazione utile anche al monitoraggio dei fenomeni dal quale partire per integrare azioni didattiche preventive e giornate di sensibilizzazione, insieme agli Enti/Servizi presenti sul territorio di riferimento. Importante, altresì, immaginare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

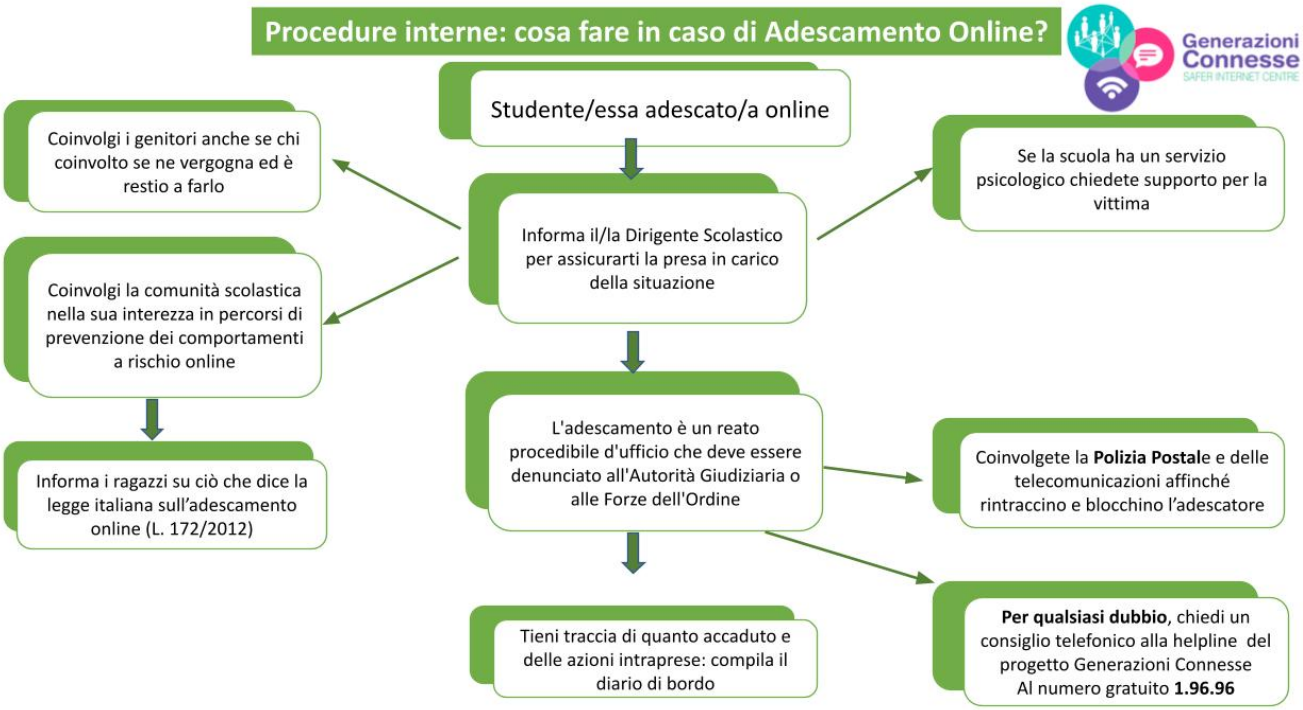
Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle Linee di Orientamento per la prevenzione e il contrasto 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.

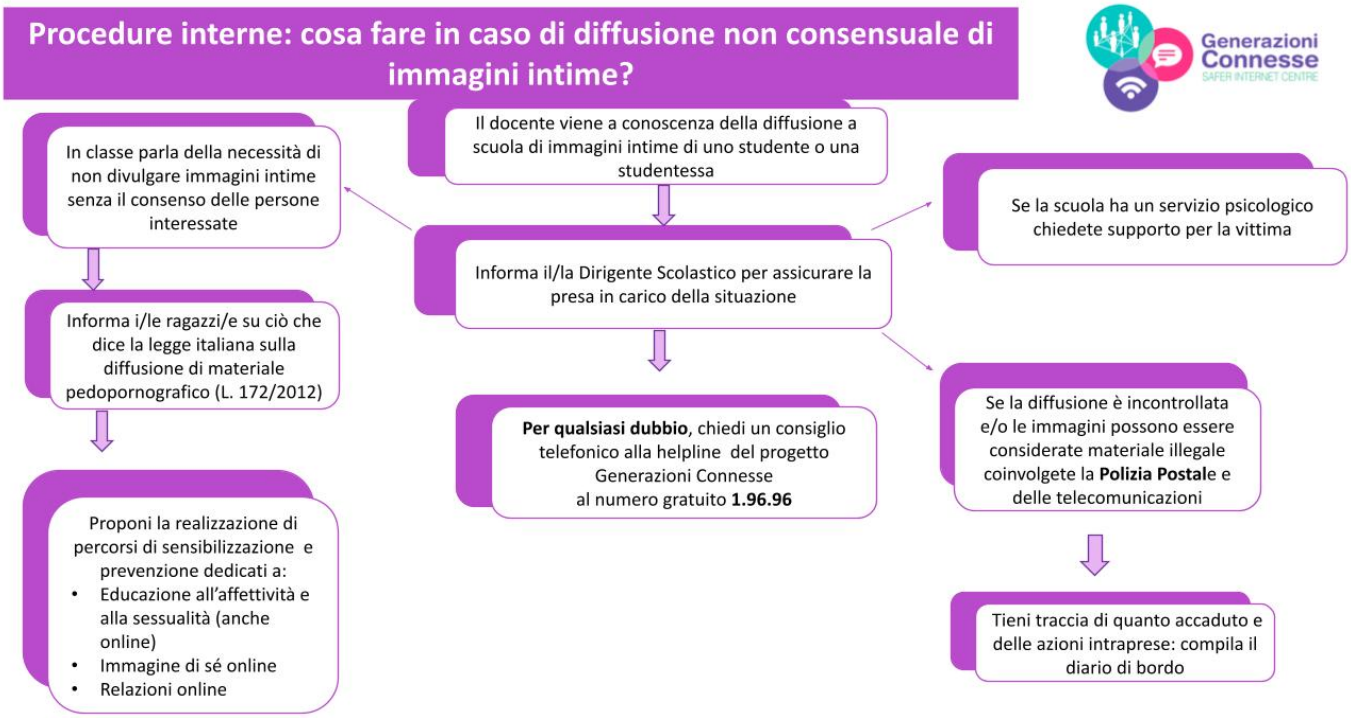
Procedure


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


Procedure interne: cosa fare in caso di evidenza di Cyberbullismo
Generazioni Connesse
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
Generazioni Connesse
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, 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 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 emergono evidenze passa allo schema successivo
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


Procedure interne: cosa fare in caso di Adescamento Online?
Generazioni Connesse
Studente/essa adescato/a online
Informa il/la Dirigente Scolastico per assicurarti la presa in carico della situazione
Coinvolgi i genitori anche se chi coinvolto se ne vergogna ed è restio a farlo
Coinvolgi la comunità scolastica nella sua interezza in percorsi di prevenzione dei comportamenti a rischio online
Informa i ragazzi su ciò che dice la legge italiana sull'adescamento online (L. 172/2012)
Se la scuola ha un servizio psicologico chiedete supporto per la vittima
L'adescamento è un reato procedibile d'ufficio che deve essere denunciato all'Autorità Giudiziaria o alle Forze dell'Ordine
Coinvolgete la Polizia Postale e delle telecomunicazioni affinché rintraccino e blocchino l'adescatore
Tieni traccia di quanto accaduto e delle azioni intraprese: compila il diario di bordo
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse Al numero gratuito 1.96.96



Per l'attivazione delle procedure di segnalazione si rimanda al "Regolamento interno d'istituto per la gestione dei casi di bullismo e cyberbullismo" reperibile sul sito web della scuola.

La verifica e la valutazione dell'accaduto spetta ai referenti del bullismo e cyberbullismo che, dopo una prima analisi della situazione, riferiscono l'accaduto al dirigente e al team antibullismo e per l'emergenza. E' prevista la condivisione a livello di consiglio di classe, sono previsti colloqui con gli alunni coinvolti e la convocazione ufficiale delle famiglie. Dopo la valutazione del caso, si può convocare un consiglio di classe straordinario e si decide per un eventuale procedimento sanzionatorio (sempre con finalità educative e formative), facendo riferimento al regolamento d'Istituto e al regolamento bullismo e cyberbullismo e definiti anche nel regolamento di disciplina.

CONCETTA VANNELLA
03.06.2026 14:36:42 CEST