Documento di ePolicy
I.C.S. N. 7 "ENZO DRAGO" ME

VIA CATANIA 103 IS. 26/C - 98124 - MESSINA
Messina (ME) - Sicilia
Data di approvazione: 07/06/2026 - 12:30

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'ePolicy dell'Istituto Comprensivo n. 7 "Enzo Drago" di Messina definisce principi e azioni finalizzati a garantire un approccio alle tecnologie fondato su sicurezza, consapevolezza e responsabilità, condiviso dall'intera comunità scolastica.

L'Istituto, da anni impegnato nella prevenzione del bullismo e del cyberbullismo, ha aderito dall'anno scolastico 2023/2024 alla piattaforma "Generazioni Connesse", promossa dal MIM, per la redazione del presente documento.

In un contesto orientato all'innovazione didattica e dotato di adeguate risorse tecnologiche, la nostra scuola intende promuovere l'acquisizione di abilità digitali trsasversali, in coerenza con il quadro DigComp e con i principi delle Nazioni Unite.

L'ePolicy costituisce uno strumento operativo di riferimento, volto a fornire indicazioni per l'impiego delle tecnologie, accrescere la consapevolezza rispetto alle dinamiche della rete e sostenere interventi formativi e di sensibilizzazione.

L'obiettivo è prevenire e affrontare situazioni problematiche legate all'ambiente digitale, attraverso l'informazione degli studenti, il controllo dei contenuti accessibili e il ruolo attivo dei docenti nel guidare comportamenti adeguati nell'utilizzo delle risorse online. Il documento ha validità triennale ed è oggetto di monitoraggio annuale, cooordinato dal Dirigente Scolastico con il supporto di commissioni dedicate e il coinvolgimento attivo delle famiglie e del personale ATA. Tale processo è finalizzato a valutare l'efficacia delle azioni intraprese, rilevare eventuali nuovi bisogni formativi e individuare criticità per definire interventi di miglioramento.

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.

Per garantire un'efficace attuazione dell'ePolicy, è fondamentale che ciascun membro della comunità scolastica contribuisca, secondo le proprie competenze e funzioni, alla sua promozione, applicazione e revisione. La corresponsabilità tra scuola, famiglie, studenti e soggetti esterni costituisce un pilastro fondamentale per la costruzione di un ambiente digitale sicuro, inclusivo e orientato alla formazione. La nostra scuola, per rispondere efficacemente a tale esigenza, individua le seguenti figure, declinando per ciascuna gli specifici ambiti di intervento:

Il Dirigente Scolastico, adeguatamente aggiornato in materia di sicurezza e prevenzione delle problematiche offline e online, in coerenza con il quadro normativo e le indicazioni del MIM, promuove la cultura della sicurezza digitale all'interno dell'Istituto, anche attraverso l'ePolicy, integrandola nelle più ampie misure di sicurezza. Garantisce l'adozione di sistemi idonei per un uso sicuro delle TIC e della rete, la protezione dei dati personali e il rispetto della normativa sulla privacy.

In collaborazione con l'Animatore Digitale e il referente per il bullismo e il cyberbullismo, favorisce attività di formazione per un utilizzo consapevole e responsabile delle tecnologie. Assicura inoltre la conoscenza delle procedure di intervento in caso di incidenti online, la valutazione dei rischi connessi all'uso delle TIC e un adeguato sistema di monitoraggio e controllo interno della sicurezza digitale.

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.

Nel contesto della nostra scuola, l'ePolicy si configura come uno strumento trasversale, la cui efficacia è strettamente legata alla sua integrazione nei principali documenti istituzionali della scuola. Tale integrazione consente di rendere coerenti le azioni educative, organizzative e regolative dell'Istituto in relazione all'uso delle tecnologie digitali. Essa rappresenta, pertanto, una condizione essenziale per garantire coerenza, continuità ed efficacia agli interventi in ambito digitale, contribuendo alla costruzione di un ambiente scolastico sicuro, inclusivo e orientato alla cittadinanza digitale.

Il nostro Istituto si impegna ad aggiornare il Regolamento d'Istituto inserendo riferimenti espliciti ai principi dell'ePolicy, in particolare per quanto riguarda le norme di comportamento relative all'utilizzo delle tecnologie digitali e della rete negli ambienti scolastici. In tale ambito saranno definite anche le procedure di intervento in caso di uso scorretto degli strumenti digitali, mantenendo una finalità prevalentemente educativa.

Analogamente, il Patto Educativo di Corresponsabilità sarà integrato con specifici richiami all'ePolicy, al fine di rafforzare la collaborazione tra scuola e famiglia nella promozione di comportamenti consapevoli e responsabili. L'Istituto si impegna a favorire momenti di informazione e confronto con i genitori sui temi della sicurezza in rete e della cittadinanza digitale, valorizzando il ruolo attivo delle famiglie nel percorso educativo.

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.

L'ePolicy viene comunicata attraverso canali istituzionali, incontri informativi e momenti formativi dedicati, al fine di garantire una comprensione condivisa delle regole di utilizzo delle tecnologie digitali e delle piattaforme che integrano sistemi di IA.

L'Istituto promuove inoltre una cultura critica e responsabile nell'uso dell'intelligenza artificiale, incoraggiando comportamenti trasparenti e corretti nello svolgimento delle attività didattiche e nella produzione dei lavori scolastici, prevenendo usi impropri e favorendo lo sviluppo del pensiero autonomo e delle competenze digitali.

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

Piano d'azione triennale

1) rilevazione dei bisogni e grado di conoscenza del fenomeno da parte di famiglie, studenti e docenti per comprendere quali sono le necessità della comunità scolastica

2) rilevazione di interessi, bisogni e comportamenti delle famiglie sull' uso positivo del digitale.

Utilizzare il questionario di autovalutazione MYDIGISKILLS, gratuito e disponibile in diverse lingue, per permettere alle famiglie di valutare il proprio livello di competenze digitali rispetto al framework europeo DIGCOMP 3. Lo strumento permette di avere risultati chiari ed analitici sulle diverse competenze

3) Ricorso a SELFIE FOR TEACHERS, strumento di autoriflessione sulle competenze digitali degli insegnanti di ogni ordine e grado, proposto gratuitamente dalla Commissione Europea sulle indicazioni del DigCompEdu, il framework delle competenze europee del docente/formatore.

4) integrazione dal punto di vista amministrativo il documento dell'ePolicy all'interno degli altri documenti della scuola.

5) realizzazione di un evento informativo per la presentazione dell'ePolicy al corpo docenti in seno al Collegio dei docenti di inizio anno

6) realizzazione di un evento informativo on line con le famiglie

7) Sportello di ascolto psicologico per studenti e docenti.

8) Progetto accoglienza nella prima settimana di scuola per promuovere la socializzazione e condividere le regole della comunità scolastica.

9) Progetti di educazione all'affettività -emozioni.

10) diffusione dell'ePolicy all'interno degli ambienti scolastici tramite:

● apposita sezione del sito istituzionale

● apposite circolari sul registro elettronico

● pannelli all'interno dell'edificio scolastico (corridoi, aule...)

● pagine social della scuola

11) formazione di docenti, studenti e famiglie a partire dalle classi prime anche grazie alla collaborazione di apposite associazioni (es. Associazioni di promozione sociale, Generazioniconnesse, #cuoriconnessi, polizia postale, etc)

12) promuovere contest/ concorsi, assemblee di istituto tematiche rivolti a studenti e studentesse per aumentare il grado di sensibilizzazione ed engagement

13) creazione di un curriculum integrato e condiviso sui temi dell'educazione civica, educazione civica digitale, bullismo e cyberbullismo

14) calendarizzazione di incontri periodici del team per monitoraggio e valutazione

15) messa a disposizione della comunità educante di un modulo di prima segnalazione (sul proprio sito web o in cartaceo presso la segreteria della scuola) per chiunque abbia necessità di segnalare situazioni a rischio di presunto o reale bullismo/cyberbullismo.

16) predisposizione di un contenitore nelle sedi scolastiche come ulteriore strumento riservato per la segnalazione.

17) aggiornamento continuo tramite i canali istituzionali e social dell'Istituto.

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 utilizza in modo sistematico le risorse offerte dal progetto Generazioni Connesse al fine di promuovere lo sviluppo delle competenze digitali e dell'educazione civica digitale in tutti gli ordini di scuola. In particolare, il Kit Didattico rappresenta un riferimento metodologico per la progettazione di attività didattiche adeguate ai diversi livelli scolastici, mentre la piattaforma formativa viene utilizzata da docenti, studenti e famiglie come strumento di aggiornamento e approfondimento sui temi della cittadinanza digitale.

I canali ufficiali del progetto, tra cui Facebook, vengono inoltre valorizzati come strumenti di informazione e sensibilizzazione, contribuendo a diffondere una cultura digitale consapevole all'interno della comunità scolastica.

Attraverso l'utilizzo integrato di tali risorse, l'Istituto consolida il proprio impegno nel promuovere un uso responsabile delle tecnologie, ponendo particolare attenzione al benessere digitale degli studenti e alla crescita educativa complessiva.

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.

In coerenza con la normativa sull'Educazione Civica e il Quadro Europeo delle Competenze Digitali, il nostro Istituto implementa l'ePolicy per strutturare interventi di prevenzione e promuovere una partecipazione consapevole alla vita democratica online, mediando tra la tutela dai rischi e la valorizzazione delle opportunità offerte dalla Rete.

Le azioni previste sono calibrate sui bisogni formativi degli studenti e delle studentesse dei diversi ordini di scuola e si sviluppano attraverso un approccio integrato che coinvolge studenti, famiglie e personale scolastico.

Per quanto riguarda i nostri discenti, si promuovono percorsi educativi progressivi e differenziati in base all'età, finalizzati allo sviluppo di una solida consapevolezza digitale. Queste proposte formative mirano a sviluppare la conoscenza dei diritti e dei doveri nel mondo dell'online, la capacità di riconoscere e affrontare i principali rischi della Rete, quali il cyberbullismo, il sexting, le dipendenze e la disinformazione, nonchè l'adozione di comportamenti responsabili e rispettosi nelle interazioni digitali.

L'azione educativa è integrata nell'ambito dell'Educazione Civica e realizzate attraverso metodologie pedagogiche attive, quali laboratori, cooperative learning, discussioni guidate e simulazioni, anche con il supporto di esperti esterni, tra cui rappresentanti della Polizia Postale, psicologi ed esperti di diritto digitale. È inoltre prevista l'attivazione di percorsi di peer education, finalizzati ad incrementare il supporto tra pari e la condivisione di buone pratiche.

L'approccio integrato e multidisciplinare adottato dalla nostra Scuola incoraggia, inoltre, lo sviluppo della riflessione autonoma e del pensiero critico.

In riferimento alle famiglie, si propongo iniziative volte a rafforzare l'alleanza educativa scuola-famiglia, attraverso incontri formativi e informativi dedicati alla prevenzione e alla sensibilizzazione sui temi dell'uso consapevole delle TIC. Tali momenti, organizzati nel corso dell'anno scolastico, sono orientati a fornire strumenti concreti per accompagnare i figli nell'esperienza online, sostenendo il dialogo e la costruzione di una cultura condivisa della responsabilità digitale, anche mediante l'utilizzo delle risorse messe a disposizione dalla piattaforma "Generazioni Connesse".

Un elemento centrale dell'azione preventiva è la formazione del personale docente e e del personale scolastico. Attraverso percorsi di aggiornamento specifici, attuati sia in presenza sia in modalità online, anche in collaborazione con esperti esterni, la scuola si propone di incrementare le competenze educative e professionali relative alla gestione delle dinamiche digitali,

alla mediazione dei conflitti online e all'utilizzo didattico consapevole e sicuro delle tecnologie. Particolare attenzione è dedicata alla conoscenza delle procedure per la gestione, la segnalazione e presa in carico delle situazioni problematiche, al fine di garantire interventi tempestivi ed efficaci.

Tutte le azioni previste sono accompagnate da attività di monitoraggio e valutazione, finalizzate a verificarne l'efficacia, ad individuare eventuali criticità e ad orientare in modo flessibile e mirato le successive scelte educative e formative, in coerenza con quanto previsto dall'ePolicy e dal PTOF.

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.

Nel quadro delle azioni di sensibilizzazione e prevenzione, l'Istituto Comprensivo n. 7 "Enzo Drago" promuove lo sviluppo del curricolo di Educazione alla Cittadinanza Digitale in coerenza con il framework europeo DigComp 2.2, con la normativa vigente in materia di Educazione Civica e con quanto previsto nel PTOF d'Istituto.

Il Curricolo Digitale si configura come uno strumento fondamentale per accompagnare progressivamente gli studenti e le studentesse nell'acquisizione di conoscenze e abilità necessarie per un uso critico e responsabile delle TIC e del Web. Esso si sviluppa in modo trasversale alle discipline e si integra nella progettazione didattica d'Istituto.

In tale prospettiva, il nostro Istituto valorizza le risorse messe a disposizione a livello nazionale e internazionale, tra cui quelle del progetto "Generazioni Connesse", utilizzate come supporto metodologico per la progettazione di percorsi educativi orientati allo sviluppo di una cittadinanza digitale attiva e responsabile.

Il curricolo si arricchisce, inoltre, attraverso l'integrazione del Piano d'Istituto per l'Utilizzo dell'Intelligenza Artificiale (PUIA), approvato a gennaio 2026, che rappresenta un ulteriore strumento strategico per l'innovazione didattica e organizzativa. In coerenza con il PUIA, l'intelligenza artificiale viene progressivamente introdotta sia come oggetto di apprendimento sia come supporto ai processi didattici, promuovendo nei fruitori lo sviluppo di competenze legate alla comprensione dei sistemi di IA, all'analisi critica dei contenuti generati e all'uso etico e responsabile.

L'utilizzo degli strumenti di intelligenza artificiale nella didattica avviene secondo un approccio graduale e guidato, nel quale

il ruolo del docente ha un ruolo centrale nella progettazione delle proposte pedagogiche, nella validazione dei contenuti e nella valutazione dei processi di apprendimento. In questo contesto, l'IA è impiegata per supportare la personalizzazione dei percorsi, fornire feedback formativi, stimolare la partecipazione attiva degli studenti e supportare i processi di apprendimento.

Particolare attenzione è, inoltre, rivolta agli aspetti etici, alla tutela dei dati personali e alla sicurezza, in coerenza con le normative vigenti e con le linee guida ministeriali.

In conformità con il Piano dell'Offerta Formativa, la nostra scuola garantisce per ogni classe moduli operativi dedicati alla Cittadinanza Digitale, integrati nella programmazione di Educazione Civica.

L'approccio didattico è finalizzato a promuovere il passaggio dalla conoscenza teorica alla consapevolezza operativa e si sviluppa attraverso metodologie inclusive, volte a rendere gli studenti protagonisti del proprio percorso di crescita e a ridurre i rischi legati a un uso passivo o inconsapevole delle TIC.

Le competenze vengono sviluppate in modo progressivo e rilevate attraverso osservazioni sistematiche, attività strutturate e compiti autentici, quali:

● Laboratori esperienziali e attività interdisciplinari, finalizzati a integrare le competenze digitali nelle diverse aree del sapere;

● Discussioni guidate e analisi critica, volte a sviluppare la capacità di interpretare i contenuti della rete e maturare un pensiero autonomo;

● Attività di produzione responsabile, orientate a promuovere l'assunzione di comportamenti consapevoli attraverso la creazione di contenuti.

L'adozione del presente documento rappresenta il consolidamento del Curricolo Digitale all'interno del quadro etico e normativo dell'Istituto. L'ePolicy diventa, da questo momento, il riferimento operativo che sistematizza i regolamenti e le attività di prevenzione, per assicurare che la programmazione didattica sia pienamente allineata alle finalità educative e alle azioni di tutela della comunità scolastica.

L'obiettivo è quello di rafforzare una maggiore coerenza tra le attività didattiche, relazioni con le famiglie e le relazioni con il territorio, mediante l'adozione di procedure condivise e trasparenti. Attraverso questa integrazione, l'Istituto intende definire il proprio impegno nel formare una comunità scolastica matura, capace di affrontare le sfide del digitale con spirito critico, collaborazione e responsabilità civica.

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 Comprensivo n. 7 “Enzo Drago” di Messina intende impiegare il Kit Didattico di “Generazioni Connesse” come risorsa metodologica a supporto delle azioni educative connesse all’e-Policy.

Il Kit, articolato per i diversi ordini di scuola, sarà utilizzato come supporto operativo alla progettazione didattica, offrendo materiali e strumenti utili per affrontare tematiche trasversali quali l’etica delle tecnologie digitali, il funzionamento dei sistemi di intelligenza artificiale, i processi di raccolta e utilizzo dei dati, la sicurezza in rete e la costruzione dell’identità digitale.

L’utilizzo del Kit sarà condiviso nei Consigli di classe e nei gruppi di lavoro, con l’obiettivo di rafforzare la coerenza tra la progettazione didattica e i principi dell’ePolicy. Le attività previste favoriranno il coinvolgimento attivo degli studenti e, ove possibile, anche delle famiglie, attraverso momenti di restituzione e incontri formativi dedicati.

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.

La protezione dei dati personali è un elemento fondamentale per la tutela dei minori e dell'intera comunità scolastica e, coerentemente con il Regolamento (UE) 2016/679 (GDPR) e con il D.lgs. 196/2003, pertanto, la scuola si impegna a garantire che ogni trattamento avvenga nel rispetto dei principi di liceità, correttezza, minimizzazione e sicurezza.

In tale prospettiva, la presenza del Responsabile della Protezione dei Dati (RPD o DPO) rappresenta un riferimento essenziale per il supporto normativo, la consulenza e il monitoraggio delle pratiche adottate. L'Istituto si impegna a mantenere aggiornato l'organigramma privacy, al fine di definire in modo chiaro ruoli, responsabilità e competenze dei soggetti coinvolti nei trattamenti.

Particolare attenzione è rivolta alla predisposizione e alla diffusione di informative trasparenti, accessibili agli interessati fin dal momento della raccolta dei dati, nonché alla corretta tenuta e aggiornamento del Registro dei Trattamenti, in collaborazione con il DPO, secondo quanto previsto dall'art. 30 del GDPR.

L'Istituto promuove, inoltre, l'adozione di procedure condivise per la gestione di eventuali violazioni dei dati personali (data breach), nonché il monitoraggio continuo dei requisiti di sicurezza e privacy nell'utilizzo degli strumenti digitali scolastici, quali il registro elettronico, le piattaforme didattiche e i servizi cloud. In questo modo, l'innovazione tecnologica viene accompagnata da una costante attenzione alla tutela dei dati personali e dell'identità digitale degli utenti della comunità scolastica.

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.

Il nostro Istituto Comprensivo riconosce nella Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) uno strumento fondamentale per regolamentare l'impiego delle tecnologie digitali e degli ambienti online in ambito scolastico. In coerenza con il percorso di elaborazione dell'ePolicy, tale documento definisce in modo chiaro diritti, doveri e responsabilità di tutti gli utenti della rete scolastica.

La P.U.A. disciplina l'accesso e l'utilizzo delle risorse digitali messe a disposizione dalla scuola, tra cui la connettività di rete, il registro elettronico, le piattaforme didattiche e i dispositivi tecnologici presenti nei diversi ambienti di apprendimento. Particolare attenzione è rivolta alla prevenzione di comportamenti non coerenti con il contesto educativo, quali la consultazione di contenuti non appropriati, l'uso improprio delle risorse digitali, la diffusione non autorizzata di dati personali o materiali tutelati dal diritto d'autore, nonché qualsiasi forma di comunicazione lesiva della dignità della persona.

Il documento è condiviso con tutte le componenti della comunità scolastica.

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.

Il Regolamento d'Istituto della nostra scuola, come previsto dalla Normativa vigente (Nota Ministeriale n.107190 del 19 dicembre 2023) vieta l'utilizzo di smartphone personali durante le attività didattiche per garantire un ambiente di apprendimento sereno, ordinato e funzionale al processo educativo. Si riconosce il valore delle tecnologie digitali come strumenti a supporto della didattica e promuove l'utilizzo delle dotazioni tecnologiche presenti a scuola, quali LIM, computer, tablet e laboratori, che vengono impiegati sotto la guida dei docenti in modo sicuro, responsabile e coerente con gli obiettivi formativi.

L'introduzione di un modello BYOD (Bring Your Own Device), chesi concentrano sulla promozione di un'integrazione

responsabile, funzionale e sicura dei dispositivi personali nella didattica, non è attualmente prevista. Eventuali sviluppi in tal senso potranno essere oggetto di riflessione futura, attraverso un percorso condiviso che coinvolga tutte le componenti della comunità scolastica e che tenga conto degli aspetti legati alla sicurezza, alla tutela dei dati personali, all'equità di accesso e alla gestione didattica degli strumenti.

Il nostro piano d'azione:

- Avviare un confronto interno con i docenti per definire o aggiornare i regolamenti sull'uso dei dispositivi digitali personali (BYOD);
- Consolidare il coinvolgimento sistematico di docenti e studenti nei processi di revisione delle regole sull'uso della tecnologia, garantendo un aggiornamento continuo in linea con l'evoluzione digitale;
- Realizzare attività formative per studenti e studentesse sui temi della sicurezza online e della navigazione consapevole (cybersecurity);
- Promuovere incontri periodici dedicati alla protezione dei dati personali, alla tutela dell'identità digitale e alla prevenzione dei rischi della rete;
- Estendere i percorsi formativi su protezione dei dati personali (GDPR) e uso sicuro delle TIC a tutto il personale scolastico, inclusi i collaboratori ATA;
- Inserire stabilmente tutte le attività di sensibilizzazione e formazione nel Piano di Aggiornamento dell'Istituto;
- Garantire coerenza e allineamento tra e-Policy, PTOF e Documento Programmatico sulla Sicurezza.

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.

Il nostro Istituto ha già predisposto un protocollo operativo interno chiaro e condiviso per la segnalazione e la gestione dei comportamenti online a rischio, al fine di garantire la tutela e il supporto agli studenti coinvolti. Le segnalazioni, che possono essere effettuate da qualsiasi componente della comunità scolastica (alunni, genitori, docenti e personale ATA), sono raccolte dal Referente per il bullismo e cyberbullismo, che coordina, in collaborazione con il Dirigente Scolastico e il Team Antibullismo, la valutazione del caso e l'eventuale presa in carico.

A seguito alla segnalazione, si procede a una prima analisi dei fatti e all'ascolto delle parti coinvolte, nel rispetto della riservatezza e della tutela dei minori. In relazione alla gravità e alla tipologia della situazione, vengono attivati interventi educativi personalizzati e azioni di supporto, con il coinvolgimento delle famiglie. Nei casi più complessi, è possibile avvalersi della collaborazione di servizi territoriali e figure specialistiche.

Gli interventi attivati sono oggetto di monitoraggio e verifica della loro efficacia, anche ai fini del miglioramento continuo delle procedure adottate.

Il protocollo definisce specifiche modalità operative per la gestione dei seguenti casi:

• **Cyberbullismo**: si esaminano il contesto, l'intenzionalità, l'eventuale reiterazione del comportamento offensivo e l'impatto emotivo sulla vittima. L'intervento prevede il supporto alla parte lesa, il coinvolgimento delle famiglie e, ove necessario, l'attivazione dei servizi territoriali (ASL, Polizia Postale, Servizi Sociali, centri antiviolenza, ecc.).
• **Adescamento online (grooming)**: si garantisce la tutela dello studente coinvolto mediante la conservazione delle prove digitali, il supporto al minore e l'attivazione immediata delle autorità competenti.
• **Sexting e diffusione non consensuale di materiale**: si procede alla tempestiva segnalazione e rimozione dei contenuti lesivi, al supporto della persona offesa e all'attivazione di misure di prevenzione della ri-condivisione, anche in riferimento alle linee guida del Garante per la protezione dei dati personali.

Tutti gli interventi si svolgono nel rispetto della normativa vigente e dei principi di privacy e riservatezza, coinvolgendo, ove necessario, enti e istituzioni del territorio (Polizia Postale, Servizi Sociali, ASL, associazioni accreditate).

Le procedure di segnalazione, documentate in un protocollo scritto, sono rese accessibili all'intera comunità scolastica mediante:

- incontri di formazione e sensibilizzazione rivolti a studenti, famiglie e personale scolastico;
- attività di formazione del personale docente;
- pubblicazione sul sito istituzionale;
- affissione di materiali informativi nei plessi scolastici;
- inserimento nei regolamenti d'Istituto e nel Patto Educativo di Corresponsabilità.

Attraverso l'adozione di queste procedure condivise, il nostro Istituto Comprensivo si impegna a garantire un ambiente

digitale sicuro, inclusivo e orientato al benessere di tutti gli studenti.

4.2 - Quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale (ex art. 357 c.p.) in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

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

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

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

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

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

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

CASO A (SOSPETTO) – Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente . La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, il Dirigente e i docenti coinvolti procedono alla valutazione del caso (valutare l'invio o meno della relazione agli organi giudiziari preposti) e agiscono tramite percorsi di sensibilizzazione.

CASO B (EVIDENZA) – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

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

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

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

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

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

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

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

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

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

Strumenti a disposizione di studenti/esse

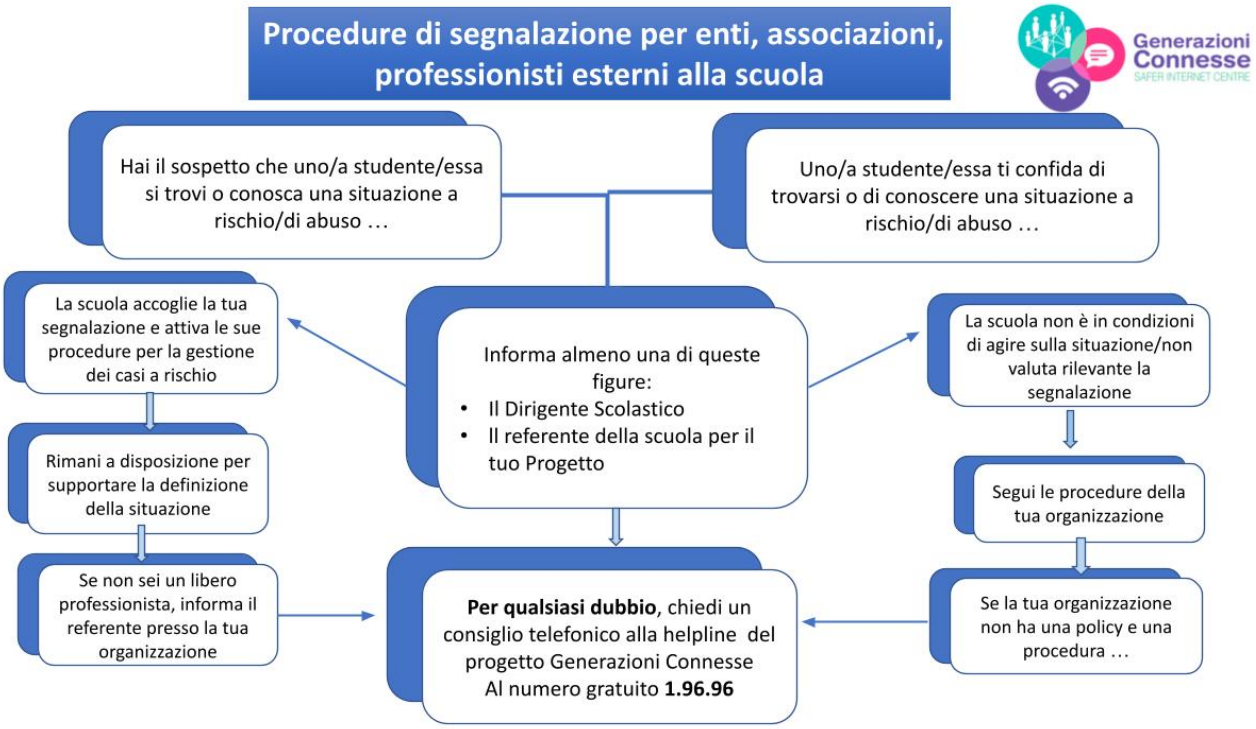
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

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

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

dovranno assumere per l'espletamento efficace della DID e, in ultimo, al Piano scolastico per la Didattica Digitale Integrata, allegato al PTOF.

Procedure



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

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

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

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

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

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

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo

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

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

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

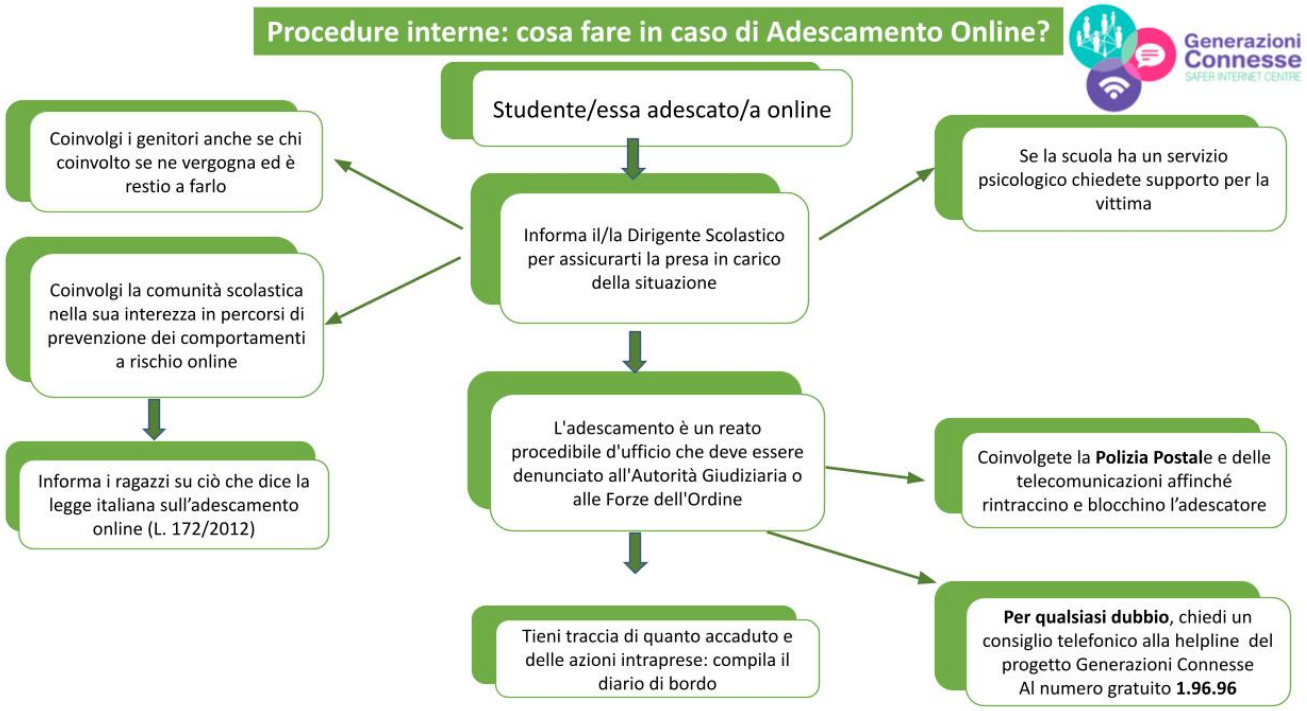
Se emergono evidenze passa allo schema successivo

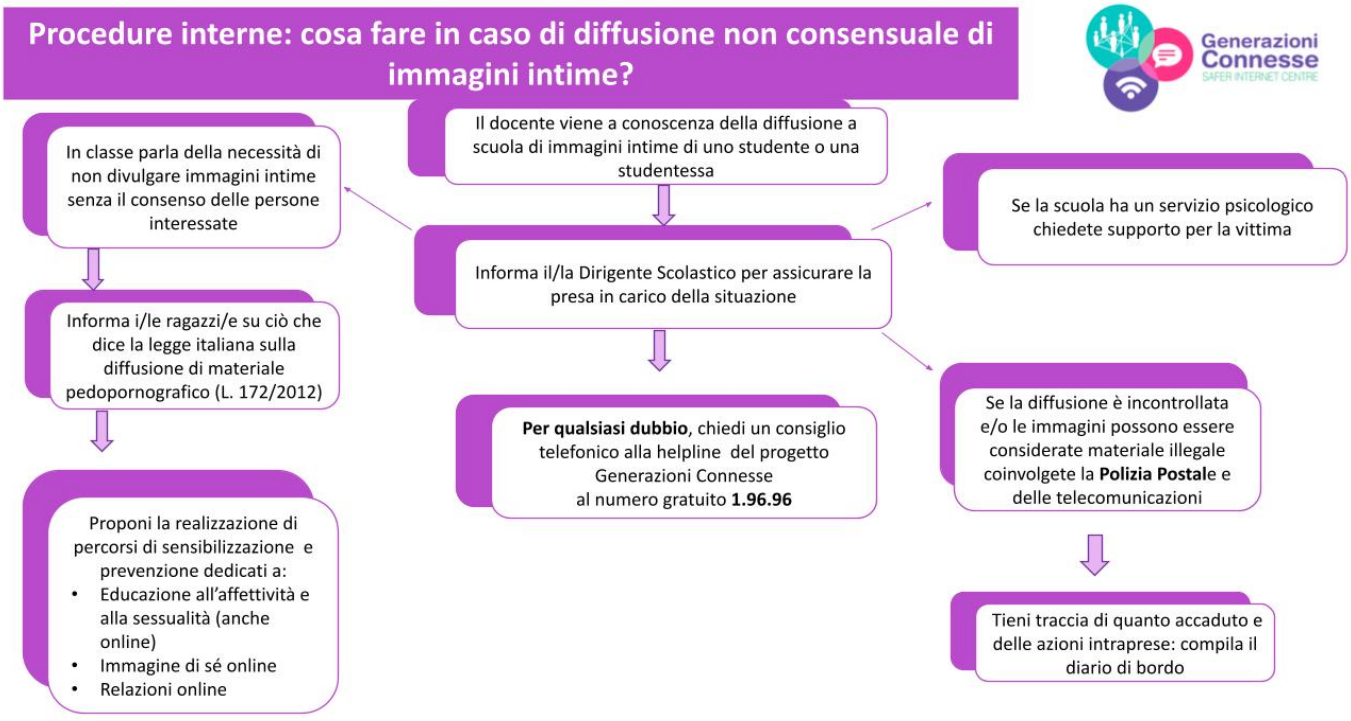
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

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

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

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





Nel nostro Istituto, le segnalazioni relative a situazioni di rischio digitale e non, vengono gestite con tempestività, attenzione e riservatezza, garantendo la tutela dei minori e la trasparenza delle procedure.

La gestione delle segnalazioni è affidata a un team multidisciplinare composto da:

- Dirigente Scolastico;
- Docente referente per il contrasto al bullismo e cyberbullismo;
- Animatore digitale;
- Referente per l'educazione civica;
- Referenti di plesso;
- Docenti impegnati nei progetti di prevenzione;
- Altri referenti individuati in base al caso.

Il docente, in quanto pubblico ufficiale ai sensi dell'art. 357 del Codice Penale Italiano, è chiamato ad esercitare funzioni educative e di vigilanza che vanno oltre la sola attività didattica. In presenza di situazioni problematiche connesse all'uso delle tecnologie digitali, il docente ha, dunque, l'obbligo giuridico e deontologico di attivarsi secondo le procedure previste dall'Istituto e segnalare all'Autorità Giudiziaria o agli Organi competenti ogni fatto che configuri un reato e coinvolga minorenni, anche in ambito digitale. È, pertanto, tenuto a segnalare tempestivamente situazioni riconducibili a cyberbullismo, sexting, adescamento online (grooming) o altri comportamenti gravemente lesivi, secondo quanto previsto dalla L. 71/2017 e dalla normativa vigente.

In casi di particolare complessità, la scuola può avvalersi del supporto di figure esterne quali psicologi dello sportello d'ascolto, esperti territoriali, Forze dell'Ordine, servizi sociali.

In presenza di un sospetto episodio di bullismo o di cyberbullismo, il docente redige una segnalazione scritta, chiara e oggettiva, che viene trasmessa al Referente e al Dirigente Scolastico per una prima valutazione del caso e per l'eventuale attivazione di interventi educativi e di monitoraggio. In presenza di evidenze accertate o di situazioni di particolare gravità, la segnalazione viene gestita con urgenza e, qualora necessario, il Dirigente provvede all'attivazione delle autorità competenti, nel rispetto degli obblighi di legge.

In presenza di fatti certi o lesivi, la segnalazione viene inoltrata con urgenza al Dirigente Scolastico. Qualora i fatti configurino fattispecie di reato o situazioni di grave pregiudizio (ex L. 216/1991), il Dirigente provvede all'inoltro della denuncia alle Autorità competenti (Procura Ordinaria o Minorile).

Quando si verifica una condizione di rischio reale o potenziale per il minore (es. grave difficoltà relazionale, esclusione sociale, sofferenza psicologica), la scuola ha l'obbligo di attivare la segnalazione ai servizi competenti (ex L. 216/1991). La mancata comunicazione configura omissione di atti d'ufficio (art. 328 c.p.).

Per facilitare l'emersione delle situazioni di disagio e garantire l'accessibilità delle segnalazioni, l'Istituto mette a disposizione strumenti dedicati, quali un indirizzo e-mail di posta elettronica istituzionale, Box per segnalazioni anche anonime e momenti di ascolto strutturato. Tutte le segnalazioni sono trattate con la massima riservatezza e documentate secondo le procedure interne, al fine di garantire tracciabilità e correttezza degli interventi intrapresi.

Anche le famiglie svolgono un ruolo fondamentale nel sistema di prevenzione e possono rivolgersi al Dirigente Scolastico, ai docenti o ai referenti d'Istituto per segnalare eventuali situazioni problematiche, contribuendo alla costruzione di un'alleanza educativa efficace.

Per tutti i membri della comunità scolastica è attivo il servizio gratuito Helpline 19696, promosso dal progetto "Generazioni Connesse", accessibile anche tramite chat WhatsApp e sul sito ufficiale. L'Istituto promuove la conoscenza dei principali servizi nazionali di supporto dedicati alla tutela dei minori online, incoraggiando il ricorso a strumenti di aiuto e consulenza in caso di necessità.

Attraverso il monitoraggio delle segnalazioni e la collaborazione con le realtà del territorio, la scuola intende rafforzare un

sistema di prevenzione sempre più efficace, integrando tali azioni nella progettazione educativa e nei documenti istituzionali, al fine di garantire un ambiente scolastico sicuro, responsabile e orientato al benessere di tutta la comunità.

La scuola intende strutturare un sistema di monitoraggio delle segnalazioni utile a:

- Intervenire tempestivamente nei casi a rischio;
- Attivare percorsi di peer education;
- Programmare giornate tematiche e attività didattiche con enti territoriali.

Tali azioni confluiranno nel PTOF, nel Regolamento disciplinare aggiornato con infrazioni relative alla DID, e saranno coerenti con le Linee Guida del MI (2021) per la prevenzione del bullismo e del cyberbullismo.

VIRGINIA RUGGERI
07.06.2026
12:32:52
GMT+02:00