



Documento di ePolicy I.C. GIACOMO MATTEOTTI

VIA OTTORINO RESPIGHI 6 - 04011 - APRILIA

Latina (LT) - Lazio

Data di approvazione: 14/05/2025 - 14:53

Cap 1 - Lo scopo della ePolicy

1.1 Scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

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

Capitolo 2 - Sensibilizzazione e prevenzione

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

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

Capitolo 4 - Segnalazione e gestione dei casi

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

1.1 Scopo dell'ePolicy

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

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

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

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

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

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

- garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali
- sensibilizzare su un uso consapevole delle stesse
- prevenire situazioni problematiche, riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

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 pedagogo, 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 l'Animatore Digitale e il Team per l'Innovazione Digitale si prevedono i seguenti compiti:

- stimolare la formazione interna alla Istituzione e fornire consulenza e informazioni al personale in relazione ai rischi on line e alle misure di prevenzione e gestione degli stessi;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite apposite password per scopi istituzionali e consentiti (istruzione e formazione);
- monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle TIC a scuola;
- curare la manutenzione del sito web della scuola per scopi istituzionali e consentiti;
- coinvolgere la comunità scolastica (alunni, genitori...) nella partecipazione alle attività e progetti attinenti la sicurezza in rete.

Per il Referente per il Bullismo e il Cyberbullismo si prevedono i seguenti compiti:

- coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo, avvalendosi anche della collaborazione delle Forze di Polizia, delle associazioni e dei centri di aggregazione giovanile del territorio.
- promuovere attività o progetti da svolgere nelle classi;
- applicare e controllare i protocolli di rilevazione, monitoraggio e gestione delle potenziali azioni di cyber/ bullismo;
- coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori, dato il suo importante ruolo non solo in ambito scolastico ma anche extra scolastico;
- svolgere un importante compito di supporto al Dirigente Scolastico per la revisione/stesura di regolamenti (regolamento d'istituto), atti e documenti (PTOF, PDM, RAV).

Per i/le Docenti si prevede che garantiscano che le modalità di utilizzo corretto e sicuro delle TIC e di Internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi. In accordo con il Dirigente Scolastico, comunicano ai genitori difficoltà, bisogni o disagi rilevati dagli alunni a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo; si informano/aggiornano sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di Internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento.

Il Personale Amministrativo, Tecnico e Ausiliare (ATA) si occupa di:

- assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni
- garantire il funzionamento dei diversi canali di comunicazione della scuola (circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente Scolastico e dell'Animatore Digitale nell'ambito dell'utilizzo delle tecnologie digitali e di Internet
- assumere la responsabilità per i problemi di sicurezza on line
- promuovere la consapevolezza e l'impegno per la salvaguardia on line dell'intera comunità scolastica

- assicurare che l'educazione alla sicurezza on line sia incorporata all'interno del PTOF
- assicurare che tutto il personale sia a conoscenza delle procedure da seguire in caso di incidente per la sicurezza on line
- mantenere agli atti un registro di incidenti di sicurezza on line
- favorire la formazione e la consulenza a tutto il personale
- coordinare le attività della scuola con le autorità locali e le agenzie competenti
- controllare l'accesso a materiali illegali/inappropriati
- controllare eventuali azioni di cyberbullismo.

Gli studenti e le studentesse devono:

- utilizzare, in relazione al proprio grado di maturità e di consapevolezza raggiunta, i sistemi delle tecnologie digitali in coerenza con quanto richiesto dai docenti
- comprendere le potenzialità offerte dalle tecnologie digitali per la ricerca di contenuti e materiali ma anche saper evitare il plagio e rispettare i diritti d'autore;
- comprendere l'importanza di adottare buone pratiche di sicurezza online quando si utilizzano le tecnologie digitali per non correre rischi;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- chiedere chiarimenti nell'utilizzo delle tecnologie didattiche e/o di Internet a docenti e genitori;
- capire l'importanza di segnalare abusi, l'uso improprio dei dispositivi tecnologici o l'accesso a materiali inappropriati.

- 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.

Genitori/adulti di riferimento sono tenuti inoltre a:

- prendere visione dell'ePolicy dell'Istituto (pubblicata sul sito della scuola) volta a regolamentare l'uso della tecnologia a scuola.
- seguire i propri figli a casa, fissare delle regole per l'utilizzo del computer, tenere sotto controllo e monitorare l'uso che i figli fanno di Internet e dei dispositivi elettronici in generale;
- tener conto che la colpa in educando fa capo ai genitori, i quali hanno instaurato una relazione educativa con il/la figlio/a, ritenuta come non adeguata, insufficiente o comunque carente tale da metterlo/a nella situazione di poter recare danno a terzi.

Gli Enti Esterni Pubblici e Privati e le Associazioni

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

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.

All'interno del PTOF 2025-2028 del nostro Istituto sono stabilite le priorità strategiche e le priorità finalizzate al miglioramento degli esiti, che, partendo da un'attenta analisi dei documenti fondanti e di particolare rilevanza, (Indicazioni Nazionali del 2012, Nuovi Scenari del 2018, Raccomandazioni del Consiglio d'Europa del 2018, Nuove Indicazioni Nazionali 2025) evidenziano l'esigenza di sempre maggiori competenze imprenditoriali, sociali e civiche e la necessità di un sostegno sistematico al personale didattico, per introdurre "forme nuove e innovative di insegnamento e apprendimento" in riferimento sia a quanto previsto nei framework europei linguistici (QCER) e digitali (Digcomp 2.2 e DigcompEdu), sia in riferimento alla vision e alla mission dell'Istituto e al patrimonio di esperienza e professionalità che negli anni hanno contribuito a costruire l'identità attuale.

In coerenza con quanto premesso, nella progettazione curricolare ed extracurricolare si è posta particolare attenzione alle azioni previste dalle linee di intervento dei progetti finanziati dai fondi PNRR. Nello specifico:

- al DM 65/2023 "Nuove competenze e nuovi linguaggi" per promuovere l'integrazione, all'interno del curricolo del nostro istituto, di attività, metodologie e contenuti volti a sviluppare le competenze STEM, digitali e di innovazione e a potenziare le competenze multilinguistiche di studenti e insegnanti;
- al DM 66/2023 "Didattica digitale integrata e formazione alla transizione digitale per il personale scolastico" per la "creazione di un sistema multidimensionale per la formazione continua dei docenti e del personale scolastico per la transizione digitale.

Si promuoverà, inoltre, la consultazione del database nazionale per la condivisione di esempi di "Buone Pratiche per la Prevenzione e il Contrasto al Bullismo e Cyberbullismo" disponibile sulla piattaforma Elisa, in un'ottica di scambio e di conoscenza di programmi, percorsi, progetti e strumenti attivi a livello regionale e territoriale.

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

- la pubblicazione del documento sul sito istituzionale della scuola;
- il Patto di Corresponsabilità: le famiglie ricevono il Patto di Corresponsabilità all'inizio dell'anno scolastico e sono tenute a firmarlo, sottolineando il loro impegno nel rispettare le disposizioni della ePolicy e nel collaborare attivamente con la scuola per promuovere un ambiente educativo sicuro e positivo
- presentazione agli studenti: una volta approvato, i docenti presentano il contenuto della ePolicy agli studenti che vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

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 del 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

IL NOSTRO PIANO D'AZIONI

Oltre ai piani di azione standard, il nostro Istituto prevede di:

- organizzare un evento di presentazione dell'e-Policy e del progetto Generazioni Connesse rivolto agli studenti;
- diffondere l'e-Policy negli ambienti scolastici, a studenti, docenti e famiglie attraverso le versioni friendly dell'e-Policy;
- organizzare incontri per la consultazione degli studenti sui temi dell'e-Policy per cui si evidenzia la necessità di regolamentare azioni e comportamenti;
- pubblicare il documento di e-Policy sul sito istituzionale;
- organizzare un evento di presentazione e conoscenza dell'e-Policy rivolto a studenti, genitori e docenti;
- effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica;
- organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica;
- organizzare e promuovere webinar e momenti formativi rivolti a docenti e genitori che riguardano le competenze digitali, l'educazione alla cittadinanza digitale e l'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali;
- organizzare e promuovere momenti di approfondimento rivolti a docenti, genitori e studenti che permettono di informare e formare sui temi della protezione dei dati personali e cybersecurity;
- promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale;
- pianificare e realizzare progetti di peer-education sui temi della sicurezza online nella scuola;
- organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti;
- far conoscere a tutta la comunità educante i diversi canali di segnalazione;
- rilevare bisogni, interessi e comportamento delle famiglie attraverso questionari di autovalutazione per permettere di valutare il proprio livello di competenza digitale rispetto a quanto previsto dal framework europeo DigComp 2.2.

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

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

Cap 2 - Sensibilizzazione e prevenzione

2.1 - Sensibilizzazione e prevenzione

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

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

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

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

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

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

Il nostro Istituto ha scelto una politica interna pro-attiva, tesa a creare un ambiente di apprendimento sereno e sicuro, che insegna a interagire in maniera responsabile.

Rispetto alle tematiche di questo percorso, vengono messe in campo attività mirate ad aiutare i nostri studenti ad aumentare la propria consapevolezza rispetto ai rischi online e a cogliere solo gli aspetti positivi che le tecnologie offrono. Ci occupiamo, dunque, delle tematiche che hanno a che fare con la cittadinanza digitale definite dalla legge 92 del 2019, cioè: relazioni online, cyberbullismo, hate speech, sexting, adescamento, disinformazione, Intelligenza Artificiale e algoritmi, Metaverso, diritti online (CRC).

Lavorare su queste tematiche significa occuparsi delle relazioni online, cioè del modo in cui interagiamo con gli altri in rete: infatti, oggi molte interazioni che abbiamo con gli altri avvengono attraverso chat, social network e anche attraverso i videogiochi. A scuola diventa importante riflettere sulle caratteristiche della comunicazione online, anche per prevenire il cyberbullismo e l'hate speech. Online si manifestano anche fenomeni come il sexting e l'adescamento, strettamente collegati all'educazione all'affettività e alla sessualità. Altra questione centrale è la disinformazione che riguarda le fake

news, un'area che è strettamente collegata anche alle nuove questioni sull'intelligenza artificiale e gli algoritmi: questi due fattori entrano in gioco quando scelgono i contenuti che ognuno di noi visualizza in base alla nostra cronologia, ai nostri like, alle nostre condivisioni. Lavorare su questo tema diventa centrale anche per il futuro della democrazia, proprio per la capacità che possono avere questi sistemi di indirizzarci verso determinati contenuti piuttosto che altri. Anche se ancora oggi non è così sviluppato come si pensava, il Metaverso è una delle frontiere nuove a cui bisogna prestare attenzione. Infine, parlando di cittadinanza, per gli studenti è fondamentale conoscere i loro diritti e imparare a declinarli nel mondo online: la Convenzioni sui Diritti dell'Infanzia dell'Adolescenza può essere la guida per orientare i percorsi di prevenzione.

Per attuare questo percorso di prevenzione, l'Istituto seguirà la strutturazione del concetto di prevenzione nei tre livelli stabiliti dall'Institute of Medicine, di seguito riportati:

1.Prevenzione Universale: considerando tutti gli studenti potenzialmente a rischio, questo tipo di prevenzione prevede una serie di interventi diretti all'intera popolazione studentesca. Pertanto, si tratta di interventi ad ampio raggio. Tale prevenzione è estesa anche alla classe genitoriale.

2.Prevenzione Selettiva: si tratta di azioni dirette a un gruppo di studenti in cui il rischio on line è stato individuato tramite precedenti indagini, segnalazioni fatte dalla scuola oppure dalla conoscenza della presenza di fattori di rischio presenti in quello specifico contesto e/o territorio. Gli interventi sono mirati e prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem solving.

3.Prevenzione Indicata: si tratta di interventi su un caso specifico, studiati per adattarsi agli studenti con l'obiettivo di ridurre i comportamenti problematici oppure dare supporto alle vittime. Questo tipo di intervento si avvale della professionalità di diverse figure perché spesso affronta problemi legati alla salute mentale del minore e, per questo, è opportuno coinvolgere anche la famiglia del/la ragazzo/a.

In relazione alla Prevenzione Universale, la comunità scolastica sarà coinvolta in percorsi di prevenzione dei comportamenti a rischio e alle conseguenze relative all'assunzione di un comportamento a rischio, con specifico riferimento alle attività online. Tali percorsi avranno lo scopo di stabilire e condividere le regole scolastiche contro il cyberbullismo. L'Istituto organizzerà eventi informativi e formativi diretti agli studenti in base alle diverse fasce d'età, come per esempio il progetto "Generazioni Connesse", indirizzato alle classi quinte della Scuola Primaria, progetti in collaborazione con la Polizia di Stato e la Polizia Postale e delle Comunicazioni indirizzati alle classi quinte della Scuola Primaria e alle classi della Scuola Secondaria di Primo Grado e/o progetti organizzati da associazioni ed enti territoriali.

Nelle azioni preventive ed educative, infatti, saranno chiamate in campo diverse agenzie educative oltre alla scuola, come la famiglia, ma anche istituzioni e associazioni, ciascuna con un proprio compito nei confronti degli studenti.

In relazione alla Prevenzione Selettiva, che si terrà nelle classi, si potenzieranno le competenze emotive, sociali e relazionali degli studenti attraverso percorsi curriculari e di educazione socio affettiva. Attraverso l'osservazione sistemica dei comportamenti a rischio si aiuteranno gli alunni coinvolti (vittime e/o carnefici) creando situazioni di dialogo che consentano di far emergere gli aspetti di criticità per i quali, attraverso un confronto, si potrà intervenire, seguendo un percorso di rieducazione alla socialità. Inoltre, il coinvolgimento dei coetanei sarà indispensabile per creare un clima di solidarietà, combattere l'omertà e l'indifferenza, incoraggiare le vittime a chiedere aiuto e sottrarre al "bullo" i potenziali gregari.

Relativamente alla Prevenzione Indicata, destinata ai singoli alunni che manifestano comportamenti a rischio di cyberbullismo (e/o bullismo), si attiverà un percorso di mentoring con i fondi stanziati per la riduzione dei divari territoriali e il contrasto alla dispersione scolastica, in attuazione del PNRR - Investimento M4C1I1.4, finanziato dall'Unione europea - Next generation EU (DM 19/2024) e con il supporto di personale specializzato.

Nel corso del triennio, l'Istituto attiverà una politica di sensibilizzazione sul tema, per accrescere la consapevolezza tra i giovani studenti dei problemi che potrebbero presentarsi all'interno di un gruppo relazionale. Le azioni che verranno intraprese saranno volte a incoraggiare gli studenti a modificare i propri comportamenti rendendoli più funzionali e a facilitare il coinvolgimento di soggetti esterni in modo da mettere insieme diverse idee per lavorare su un obiettivo comune.

Infine, l'Istituto favorirà la diffusione di informazioni e servizi rendendoli disponibili all'intera comunità scolastica.

In questa ottica, l'Istituto si occuperà di:

1. intraprendere un'attività di peer education sui temi della sicurezza online della scuola;
2. proporre a tutte le classi V della Scuola Primaria attività inerenti al progetto "Generazioni connesse";
3. proporre a tutte le classi della Scuola Secondaria di Primo Grado progetti per la diffusione di un uso consapevole delle TIC e della Rete;
4. istituire delle campagne di sensibilizzazione per mettere in luce i rischi di un utilizzo poco corretto delle TIC, anche con il coinvolgimento di esperti esterni;
5. promuovere la diffusione della conoscenza delle Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo del MIM;
6. elaborare una proposta di approccio curricolare inserendo attività di sensibilizzazione nell'azione didattica da svolgere in classe a cura dei docenti utilizzando filmati, episodi di cronaca recenti o testi come stimolo per la discussione in classe, l'acquisizione di consapevolezza del problema, delle motivazioni sottostanti e delle conseguenze e lo sviluppo di un sistema di regole e di una cultura anti prepotenze nella classe;
7. implementare l'e-Safety Policy con il contributo di tutte le componenti (docenti, studenti, famiglie, personale ATA);
8. favorire la diffusione di informazioni e servizi disponibili all'utilità collettiva presentando questa e-Safety Policy agli Organi Collegiali e quindi inserirla nel sistema di regolamenti della Scuola e renderla pubblica sul sito della Scuola;
9. organizzare incontri informativi rivolti a genitori con il coinvolgimento di esperti per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali in quanto il loro coinvolgimento rende la prevenzione più efficace;
10. promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.

2.2 - Il Curricolo Digitale

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

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

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

Nel curriculum 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.

L'Istituto ha redatto un Curricolo Digitale prevedendo un percorso didattico interdisciplinare e trasversale in continuità con i tre ordini di scuola (infanzia, primaria e secondaria di primo grado) in modo da creare le condizioni per cui gli studenti possano sviluppare competenze digitali di facile replicabilità, utilizzo e applicazione.

La competenza digitale, una delle otto competenze chiave europee contenuta nel documento della Raccomandazione relativa alle competenze chiave per l'apprendimento permanente, approvata dal Parlamento Europeo il 22 maggio del 2018, è ormai un traguardo formativo per ogni ordine scolastico, secondo la logica di un curriculum verticale di Istituto, che si pone l'obiettivo di:

- rispondere ai bisogni di conoscenza, di espressione e di comunicazione degli alunni
- aiutare gli alunni a organizzare, riflettere e attribuire un senso alla loro esperienza tecnologica
- orientare all'uso non passivo della tecnologia.

La competenza digitale è propria di chi sa utilizzare con dimestichezza le nuove tecnologie, con finalità di istruzione, formazione e lavoro. Infatti, tale competenza favorisce lo sviluppo di abilità trasversali e attitudini essenziali (come la curiosità, lo spirito di iniziativa, la perseveranza, l'adattabilità, la leadership e la consapevolezza socio-culturale). Fanno parte di questa competenza: l'alfabetizzazione informatica, la comunicazione e collaborazione, la sicurezza online, la creazione di contenuti digitali, la risoluzione di problemi.

Per la costruzione del curriculum si è fatto riferimento al DigComp 2.2 ("Digital Competence Framework for Citizens), il quadro di riferimento europeo per lo sviluppo e la misurazione delle competenze digitali e alle indicazioni Nazionali: per ciascuna dimensione sono stati individuati aree tematiche, tipologia di contenuti, discipline e metodologie.

Il curriculum si basa su una o più discipline curriculari, per affrontare tematiche:

- fondamentali (vd PNSD azione #15, p. 77), a partire da quelli di base: diritti in internet, educazione ai media e ai social, educazione all'informazione;
- caratterizzanti (vd PNSD azione #15, p. 78): STEM, robotica educativa, making e stampa 3D, economia digitale, lettura e scrittura in ambienti digitali, uso dei dati aperti e grandi, arte e digital cultural heritage, imprenditorialità digitale.

Oltre alla attività curriculari previste dal documento, grazie ai fondi PNRR del DM 65/2023 - Nuove competenze e nuovi linguaggi, l'Istituto ha proposto e realizzato diversi corsi extracurriculari rivolti agli alunni dei tre ordini (infanzia, primaria, secondaria di primo grado) con diversi livelli di complessità (corso coding per l'infanzia; corsi coding base e avanzato, STEM e DIGCOMP 2.2 per la primaria; corsi STEM, robotica e DIGCOMP 2.2 per la secondaria di primo grado).

[Curriculum-verticale-delle-competenze-digitali-IC-Matteotti-Copia.pdf](#)

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.

Il kit didattico messo a disposizione dalla piattaforma Generazioni Connesse costituisce la base di partenza delle attività che l'Istituto ha stabilito all'interno del proprio curriculum verticale digitale. Le attività, infatti, seguiranno il percorso delle aree tematiche del framework DigComp 2.2 secondo le competenze e i livelli di padronanza previsti.

A integrazione di ciò, l'IC propone anche l'inserimento e l'utilizzo di alcune applicazioni come Padlet, Canva, Genially, Panquiz, Scrath, Book Creator utili al consolidamento e al potenziamento delle cinque aree di competenza previste.

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.

L'Istituto Comprensivo "Giacomo Matteotti" è dotato dell'informativa per il trattamento dei dati personali ai sensi del Regolamento UE n. 2016/679 ("GDPR") e del D. Lgs. 30.6.2003 n. 196 ("Codice Privacy") modificato dal D. Lgs. 10.08.2018 n.101.

In tale regolamento sono indicate le categorie degli interessati e dei destinatari, che sono definiti in fase di raccolta dei dati per inserirli nelle informative specifiche agli interessati. Sono riportate le finalità istituzionali, il riferimento relativo al titolare del trattamento e al responsabile del trattamento. Viene, altresì, regolata la modalità di trattamento dei dati, che potrà essere effettuato sia con mezzi cartacei sia con mezzi elettronici. Vengono esplicitate, infine, le modalità di esercizio dei diritti da parte dell'interessato.

Si allegano alcuni modelli di liberatoria adottati e conformi alla normativa vigente in materia di protezione dei dati.

[LIBERATORIA PER L'UTILIZZO DELLE IMMAGINI DI MINORENNI](#)

[CIRC 234 PSICOLOGO A SCUOLA modulo autorizzazione genitori \(002\) \(1\)](#)

È inoltre fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori previsti nel PTOF.

Si specifica che i dati sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e

trasparenza"); raccolti per finalità determinate, esplicite e legittime, e trattati in modo che non siano incompatibili con tali finalità; adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di "minimizzazione dei dati"); esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati base del principio di "esattezza"; conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali in base ai principi di "integrità e riservatezza"; configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo in caso di necessità ("principio di necessità").

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.

L'Istituto ha regolamentato anche le modalità di utilizzo della comunicazione online, a partire dal sito istituzionale in relazione alla comunicazione esterna: tutti i servizi offerti tramite il sito web della scuola, nel rispetto delle norme vigenti, non potranno ricondursi, anche indirettamente, al trattamento dei dati personali sensibili oppure a dati giudiziari (vedi Regolamento Trattamento Dati).

All'interno del regolamento interno di Istituto è, invece, regolato l'uso dei dispositivi mobili da parte degli alunni. In particolare, è fatto espresso divieto di utilizzare il cellulare durante le lezioni, essendo questo un elemento di distrazione propria e altrui e rappresentando una mancanza di rispetto verso i docenti, come già stabilito dallo Statuto delle studentesse e degli studenti del 1998 e dalla Circolare Ministeriale n. 30 del 2007. Gli alunni non possono tenere acceso il telefono cellulare, non possono effettuare telefonate con il medesimo, inviare messaggi, acquisire e/o divulgare immagini, filmati o registrazioni vocali.

Essendo lo sviluppo delle competenze digitali tra gli obiettivi del Curricolo Digitale è importante dedicare particolare attenzione all'utilizzo critico e consapevole dei social network e dei media. È necessario che gli allievi della scuola primaria e secondaria raggiungano, tra i vari obiettivi previsti, quelli relativi ai rischi nell'uso del WEB, utilizzando adeguate strategie di protezione dei propri dati, quelli relativi alle regole per la Comunicazione Digitale, tutelando se stessi e gli altri dall'uso errato dei social network e dei social media. È previsto, inoltre, il raggiungimento dei seguenti obiettivi: potenziare le competenze informatiche e digitali; potenziare il cooperative learning in modalità da remoto; conoscere e usare i diversi strumenti digitali di collaborazione (Drive, Teams, posta elettronica...); usare applicazioni e programmi, anche online, per

produrre e presentare contenuti di vario tipo (PPT, Padlet, Thinglink, Prezi...).

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.

Consapevoli che la transizione digitale della scuola prevede un investimento per la creazione di ambienti digitali negli spazi delle scuole, grazie anche ai fondi PNRR in questi ultimi anni stanziati, l'Istituto deve potenziare la disponibilità dei dispositivi digitali individuali, utili sia per l'attività svolta in classe sia per l'attività svolta a casa, con la relativa connettività, in modo da attuare le politiche BYOD, per cui l'utilizzo di dispositivi elettronici personali sia possibile ed efficientemente integrato nella didattica quotidiana. Attualmente i dispositivi digitali sono forniti in comodato d'uso per casi singoli ed eccezionali.

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/le 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.

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 minorenni.

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

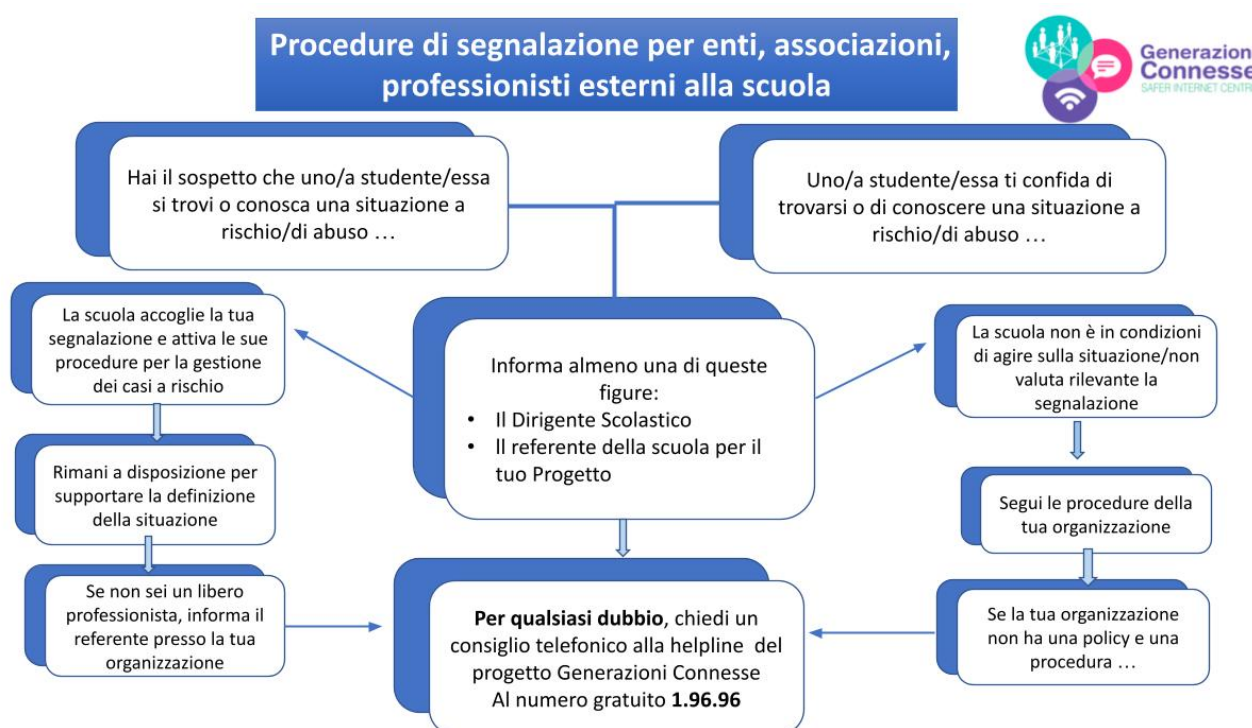
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

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.

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).

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

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

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.

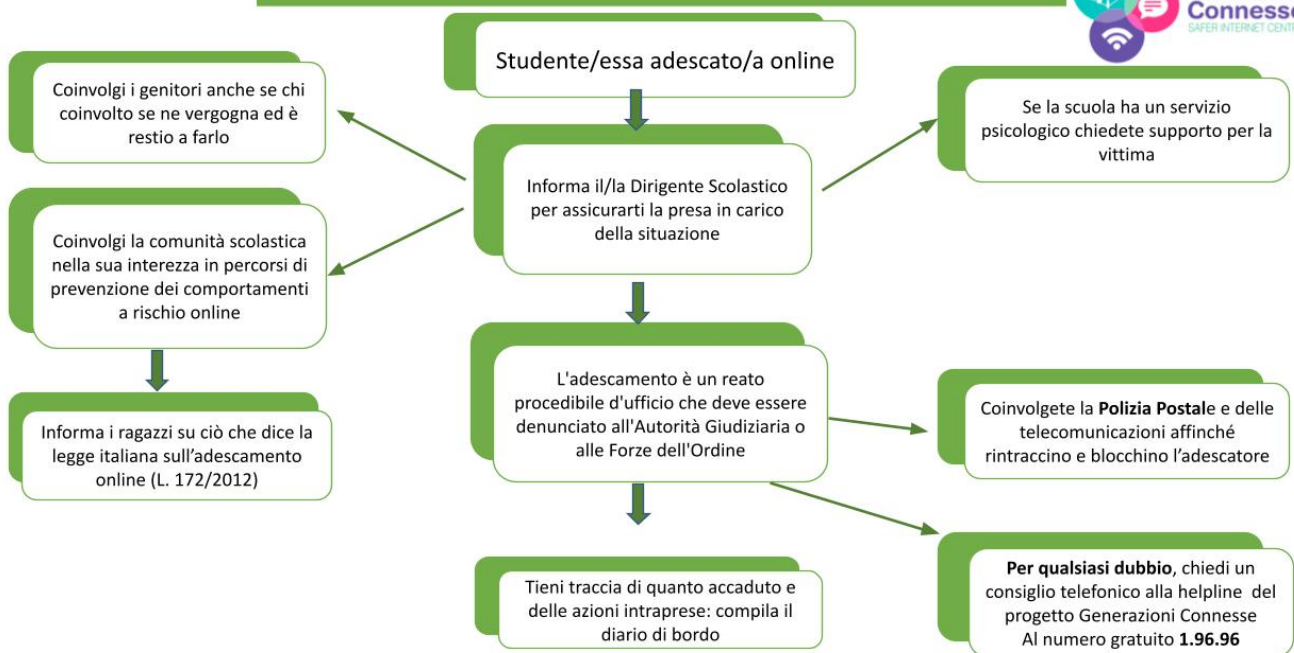
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

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

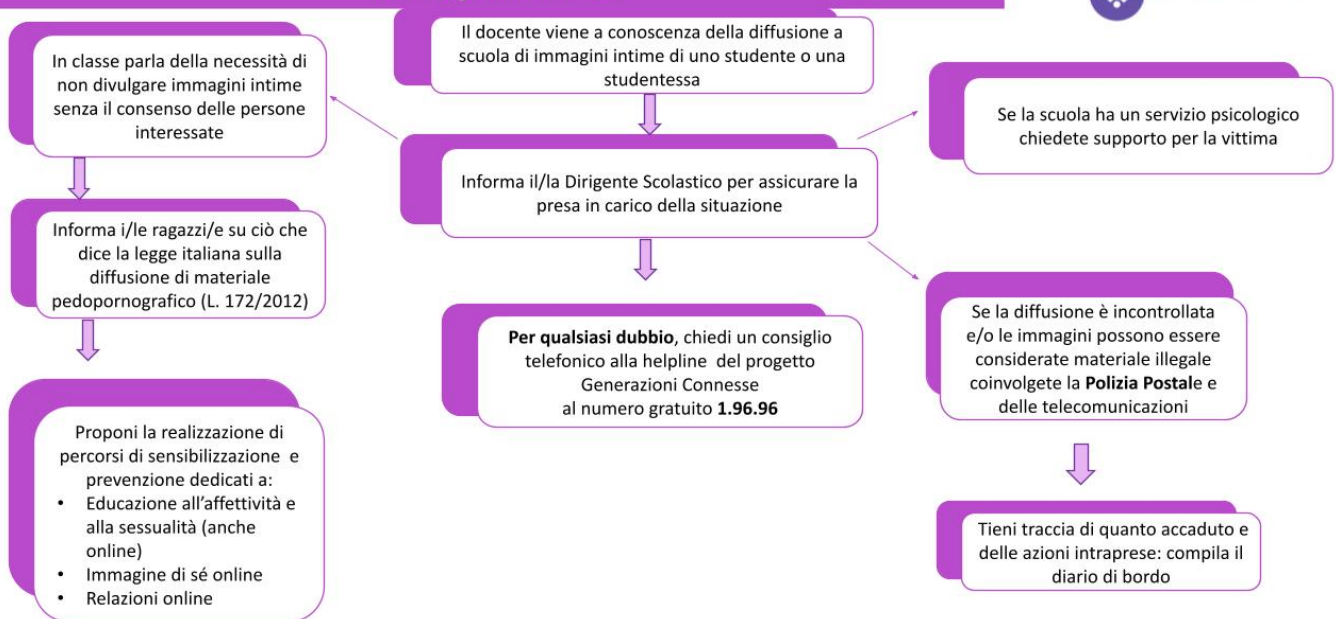
Se emergono evidenze passa allo schema successivo

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?



Procedure interne: cosa fare in caso di diffusione non consensuale di immagini intime?



Strumenti di segnalazione messi a disposizione di studenti/esse dall'Istituto:

- un indirizzo e-mail specifico per le segnalazioni (sosmatteotti@gmail.com);

- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola (ubicata nell'atrio principale di ciascun plesso);
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni (plesso Matteotti: doc. Mandolini L.; plesso Deledda: doc. Iacobellis B./doc. Esposito F.; plesso Campoverde: doc. Barlone F.).

Studenti e studentesse possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96. Inoltre, possono inviare segnalazioni, anche in forma anonima, tramite "Youpol", l'applicazione della Polizia di Stato.

Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi ad altre figure, enti, istituzioni e servizi presenti sul territorio qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani", senza dimenticare che la Helpline di Telefono Azzurro (1.96.96) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

Comitato Regionale Unicef: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.

Co.Re.Com: (Comitato Regionale per le Comunicazioni): svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.

Ufficio Scolastico Regionale: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.

Polizia Postale e delle Comunicazioni: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.

Aziende Sanitarie Locali: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.

Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico: segnalano all'Autorità Giudiziaria e ai Servizi

Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.

Tribunale per i Minorenni: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.