

ISTITUTO COMPRENSIVO - "DON LORENZO MILANI"-LANCIANO
Prot. 0008135 del 04/07/2025
IV (Uscita)



Documento di ePolicy I.C. LANCIANO "DON L.MILANI"

VIA NAPOLI 83 - 66034 - LANCIANO

Chieti (CH) - Abruzzo

Data di approvazione: 24/06/2025 - 17:20

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.

In ambito scolastico l' ePolicy ha come scopo principale quello di stabilire regole e linee guida per l'uso delle tecnologie digitali all'interno delle istituzioni educative. Con l'aumento dell'uso dei dispositivi elettronici e risorse on line nell'insegnamento e nell'apprendimento , è fondamentale avere una politica chiara che tuteli sia gli studenti che il personale scolastico.

Uno degli obiettivi fondamentali del documento è garantire la sicurezza dei dati personali sia degli studenti che del personale, quindi la protezione dei dati sensibili e la prevenzione di accessi non autorizzati. Il documento di ePolicy promuove l'uso responsabile delle tecnologie invogliando a comportamenti etici nell'interazione on line, in conformità alle LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo e cyberbullismo elaborate dal Ministero dell'Istruzione, dell'Università e della ricerca in collaborazione con il Safer Center per l'Italia, programma comunitario istituito dal Parlamento Europeo e dal Consiglio dell'Unione.

Altro punto importante che l'ePolicy affronta è la sensibilizzazione verso i rischi legati alla cybersicurezza cioè il cyberbullismo e le truffe on line. Quindi l'ePolicy fornisce indicazioni su come riconoscere ed affrontare tali problematiche realizzando un ambiente sicuro ed inclusivo.

L'ePolicy supporta la fusione fra insegnamento e tecnologie, proponendo indicazioni per l'uso efficace delle risorse digitali, rendendo l'apprendimento più coinvolgente.

La diffusione del digitale nella società è inarrestabile ed in rapida crescita, come dimostra l'espansione dell'Intelligenza Artificiale.

L'ePolicy rappresenta uno strumento condiviso per promuovere un uso positivo delle tecnologie, prevenire i rischi e rispettare le norme. L'obiettivo è garantire il benessere digitale di studenti, docenti e famiglie, attraverso la sensibilizzazione, l'educazione e la formazione, favorendo una cittadinanza digitale responsabile e critica. La competenza digitale è fondamentale per esercitare i propri diritti on line.

L'ePolicy si articola di quattro obiettivi:

- promuovere un uso sicuro e responsabile della rete;
- prevenire comportamenti a rischio;
- definire norme di utilizzo;
- gestire situazioni problematiche.

Un approccio preventivo permette di individuare e affrontare i problemi prima che si manifestino, ottimizzando risorse e facilitando interventi efficaci.

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 segua 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.

In ambito scolastico l'implementazione dell'ePolicy necessita della collaborazione dei vari attori (dirigente scolastico, animatore digitale, referente per il bullismo ed altri come riportato), ognuno nel proprio ruolo e nella propria specifica responsabilità.

E' necessario che ci sia quindi una chiara definizione delle responsabilità assunte ed una comunicazione il più efficace possibile per poter creare un ambiente scolastico sicuro e adatto all'apprendimento.

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.

Sebbene, esista un documento di Linee guida che indica le procedure, le regole e le modalità di utilizzo dei dispositivi informatici, si sente la necessità di integrare tali Linee guida con delle norme più definite, che prevedano l'uso di qualunque genere di device di proprietà dell'alunno o della scuola, ciò in quanto perchè le Linee guida in uso prevedono procedure e regole, riguardo i dispositivi informatici, ad uso esclusivo dei docenti. L'istituto non prevede attualmente una *particolare procedura di accesso alle postazioni informatiche* da parte degli allievi e ciò rappresenta un grande rischio sia per la rete d'istituto sia per i dati che gli allievi potrebbero condividere. Gli studenti possono utilizzare i dispositivi informatici secondo le regole d'istituto ed è perciò indispensabile *predisporre un regolamento di utilizzo più incisivo* e responsabilizzante, anche attraverso il documento di ePolicy che venga quindi ad essere integrato nella sua progettualità nel PTOF, citato nel R.A.V., e dichiarato nel Piano di Comunicazione della scuola.

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

1. il curriculum 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.

La **condivisione** e la **comunicazione** dell'ePolicy sono aspetti importanti per garantire che tutta la comunità scolastica comprenda le linee guida stabilite per l'utilizzo della tecnologia digitale. Sono quindi elementi fondamentali alla riuscita del documento per la creazione di un ambiente di apprendimento sicuro e positivo.

Vanno perciò considerati:

1. **l'importanza della condivisione** che è fondamentale per creare un ambiente di apprendimento sicuro e responsabile. Quando la strategia è ben comunicata, tutta la comunità scolastica ha una chiara visione delle aspettative e delle responsabilità. Ciò permette di evitare comportamenti inappropriati a favore della cultura del rispetto e della sicurezza. Lo scopo è quindi quello d'informare tutti i membri della comunità scolastica sulle norme e linee guida relative all'uso delle tecnologie.
2. **modalità di comunicazione.** Ad es. attraverso: - "incontri informativi" nei quali poter presentare il documento di ePolicy e rispondere a eventuali domande; - "documentazione scritta" al fine di rendere il documento di ePolicy accessibile a tutti questo potrebbe essere condiviso sia in formato cartaceo quanto digitale; - "formazione e Workshop" in cui sia al personale che agli allievi possa essere spiegato il documento di ePolicy e possano essere presentati casi pratici e scenari reali; - "Piattaforma on line", ad esempio anche lo stesso utilizzo del sito web scolastico in cui il documento di ePolicy possa essere pubblicato con eventuali aggiornamenti aggiuntivi.
3. **feedback e coinvolgimento**, al fine di rendere più efficace il documento di ePolicy si potrebbero pensare spazi per discussioni, in cui raccogliere suggerimenti da parte degli alunni, dei genitori e del personale, sviluppando così anche il loro senso di responsabilità e appartenenza. Coinvolgendo i genitori affinché possano supportare anche a casa l'ePolicy al fine di un utilizzo sicuro e consapevole della tecnologia.
4. **aggiornamenti e revisione del documento di ePolicy** in considerazione della velocità con la quale si modifica sia la tecnologia quanto la legislazione, assicurerebbe che siano tutti informati sulle ultime linee guida.
5. **cultura della sicurezza**, che si può ottenere dalla condivisione del documento di ePolicy che conduce a promuovere un ambiente in cui tutti gli alunni si sentono protetti e supportati nell'uso delle tecnologie. In cui gli alunni imparano a rispettare le regole e a comportarsi in modo etico on line. Gli alunni si sentono sicuri nel segnalare comportamenti inopportuni o nel segnalare problemi legati alla sicurezza.

In considerazione di questi 5 punti menzionati, la scuola definisce i punti da attuare:

- che gli alunni siano informati che la rete, internet ed ogni dispositivo digitale sono controllati dai docenti ed è possibile utilizzarli solo con la loro autorizzazione e supervisione;
- ai fini dell'acquisizione della consapevolezza dell'uso sicuro e responsabile di internet sono programmati moduli d'insegnamento sulla e-safety nell'ambito delle diverse discipline;
- si provvederà a pubblicare in tutte le aule con accesso ad internet un elenco di regole per la sicurezza on line;
- la linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà discussa durante consigli di classe, collegi dei docenti e consigli d'istituto per poi comunicarla a tutta la comunità scolastica tramite la condivisione del documento di ePolicy;
- il personale docente è informato che il traffico in internet può essere monitorato e si può risalire al singolo utente registrato;
- saranno programmate formazioni per il personale sull'uso sicuro di internet;
- l'animatore digitale supervisiona il sistema di filtraggio adottato e monitora l'uso delle TIC. Segnerà eventuali problemi necessitanti di interventi tecnici alla DSGA;
- l'animatore digitale mette a disposizione dei docenti le sue conoscenze;
- una condotta non in linea con il codice del comportamento dei pubblici dipendenti e dei propri doveri professionali, da parte del personale, è sanzionabile;
- durante gli incontri scuola - famiglia, collegi ed incontri individuali deve essere incoraggiato un approccio di collaborazione nel conseguimento della sicurezza nell'utilizzo nell'uso delle TIC e di internet;
- l'animatore digitale e i docenti forniranno i genitori di indirizzi sul web relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni, sistemi di filtraggio e attività educative per il tempo libero;
- i genitori esperti possono collaborare nelle attività di informazione - formazione del personale e degli alunni.

Inoltre la scuola riguardo la comunicazione e la condivisione con le famiglie elementi fondamentali per assicurare che tutti i membri della comunità scolastica siano coinvolti ed informati potrà utilizzare:

- il "sito web scolastico" all'interno del quale creare una sezione dedicata al documento di ePolicy. All'interno di tale sezione porre una copia del documento stesso, le FAQ comprensive delle domande frequenti per chiarire eventuali dubbi, i link utili alla sicurezza on line.

- Si possono utilizzare delle "newsletter scolastiche", inviate per email o tramite registro elettronico riportanti aggiornamenti dell'ePolicy, eventi di formazione per i genitori per sostenere i propri figli nell'uso sicuro della tecnologia digitale.

- "Incontri con i genitori" per presentare l'ePolicy in cui spiegare le linee guida e le motivazioni alla base dell'ePolicy, rispondere a domande e raccogliere feedback, creare sessioni di formazione per i genitori su temi legati alla sicurezza digitale.

- In alternativa al sito, utilizzare la "piattaforma Microsoft Team" per condividere documenti e aggiornamenti sull'ePolicy.

- "FB o Telegram" possono essere utilizzati per condividere le informazioni sull'ePolicy, postare aggiornamenti e divulgare eventi di sensibilizzazione, coinvolgendo così le famiglie in maniera informale.

- Creare "sondaggi e questionari" per raccogliere feedback riguardo l'ePolicy, capendo le preoccupazioni delle famiglie.

- Creare "gruppi di discussione" in cui i genitori possono condividere esperienze, fare domande e discutere tematiche legate al documento di ePolicy ed alla sicurezza in rete, ciò nell'intento di favorire il senso di comunità e rispetto reciproco.

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

Le azioni che si metteranno in campo nel primo anno di attuazione del piano di azione dell'ePolicy si possono così distinguere:

1. analizzare le competenze digitali degli studenti e delle studentesse;
2. analizzare l'utilizzo dei dispositivi personali a scuola;
3. analizzare il fabbisogno formativo del corpo docente;

4. organizzare incontri formativi per il corpo docente;
5. condividere il documento di ePolicy con il Collegio dei docenti, il consiglio d'istituto e le famiglie;
6. presentare il documento di ePolicy agli alunni;
7. promuovere il progetto Generazioni Connesse;
8. promuovere l'uso positivo delle TIC e della rete;
9. educare all'uso consapevole e responsabile degli strumenti digitali;
10. coinvolgere i genitori nelle attività di promozione ed educazione.

Le azioni da porre in atto

nel secondo anno di attuazione del piano di azione dell'ePolicy saranno le seguenti:

11. definizione di una "Politica di Uso Accettabile" (PUA) delle tecnologie digitali a scuola;
12. analizzare l'utilizzo dei dispositivi personali a scuola da parte degli alunni;
13. definizione delle regole di utilizzo delle TIC a scuola;
14. azioni formative ed educative sulle tecnologie digitali.

Le azioni da porre in atto

nel terzo anno di attuazione del piano di azione dell'ePolicy saranno le seguenti:

15. condividere il documento di ePolicy con il Collegio dei docenti; il Consiglio d'istituto e le famiglie;
16. revisionare e pubblicare il documento di ePolicy sul sito della scuola;
17. promuovere l'utilizzo sicuro della rete internet;
18. monitorare sul buon utilizzo di internet a casa;
19. incoraggiare l'alleanza scuola / famiglia;
20. tenere un alto profilo personale e professionale;
21. prendere in considerazione le opinioni degli alunni;
22. impedire comportamenti irrispettosi, insultanti o lesivi della privacy degli alunni;
23. non tollerare né partecipare a comportamenti illeciti o pericolosi per la sicurezza degli alunni;
24. organizzare eventi per formare gli alunni sull'accesso ad internet e sul buon utilizzo delle tecnologie digitali

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](#)

L'istituto scolastico proporrà le risorse della piattaforma Generazioni Connesse pubblicandole nella apposita sezione dellePolicy presente nel sito web scolastico, coinvolgendo così l'intera comunità scolastica attraverso attività di sensibilizzazione e formazione.

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 on line riguarda la possibilità che i minori possano compiere azioni dannose, essere vittime di queste azioni o semplicemente osservarle. E' fondamentale riconoscere e distinguere questi fenomeni per poter adottare le strategie più efficaci per prevenirli e contenerli. Per farlo, è importante lavorare su aspetti di prevenzione e sensibilizzazione, che permettano di ridurre i fattori di rischio e di aumentare la capacità dei ragazzi di riconoscere situazioni pericolose e segnalarle a un adulto di riferimento.

Le strategie d'intervento si dividono in due grandi categorie:

- 1) sensibilizzazione: azioni volte a promuovere un cambiamento, fornendo informazioni utili a conoscere il fenomeno e illustrando soluzioni o comportamenti corretti da adottare.
- 2) prevenzione: attività e interventi finalizzati a sviluppare competenze digitali, con l'obiettivo di evitare l'insorgenza di rischi legati all'uso del digitale e di garantire la sicurezza di bambini e ragazzi.

Nella scuola, è importante che tutti i membri della comunità docenti, studenti e famiglie siano consapevoli delle caratteristiche degli ambienti on line e delle opportunità e rischi che essi comportano. La promozione di una cittadinanza digitale responsabile si realizza attraverso strumenti come l'ePolicy. Epolicy si propone di definire azioni e interventi per educare e coinvolgere l'intera comunità scolastica, con l'intento di favorire una partecipazione attiva, consapevole e responsabile, basata sulla conoscenza dei diritti, dei rischi e delle opportunità in rete.

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.

Il curriculum Digitale, secondo le linee guida europee e nazionali, è un percorso didattico pensato per tutti gli studenti, che mira a sviluppare competenze digitali non solo dal punto di vista tecnico, ma anche etico, responsabile e critico. L'obiettivo è far sì che gli studenti imparino a usare le tecnologie digitali in modo creativo, consapevole e responsabile, affrontando anche i rischi e le sfide del futuro.

Questo percorso si integra con le varie discipline e coinvolge tutta la comunità scolastica, inclusi docenti, animatori digitali e anche partner esperti come università, imprese e associazioni, per rendere l'apprendimento più ricco e collegato al territorio.

Le attività possono essere svolte durante l'orario scolastico o anche fuori, attraverso laboratori, workshop e progetti che coinvolgono anche le famiglie. Inoltre si cerca di collegare questi percorsi con l'educazione civica digitale, prevista dalla legge, per promuovere una cittadinanza digitale consapevole.

Per quanto riguarda le risorse, si utilizza anche il framework europeo DigComp 2.2, che aiuta a definire le competenze digitali da sviluppare sia per gli studenti che per le famiglie e si inserisce nel più ampio curriculum di educazione alla cittadinanza digitale che si basa anche sull'ePolicy dell'istituto, ed aiuta ad orientare le attività ed i percorsi formativi.

Nel curriculum è previsto per ogni classe uno specifico appuntamento realizzato in base all'età degli alunni anche tramite l'utilizzo del Kit didattico per la conoscenza e consapevolezza del documento stesso. Rappresenta pertanto un elemento fondamentale nell'educazione scolastica moderna, nella scuola primaria ed anche nella secondaria di primo grado. Si tratta di un percorso strutturato che mira a sviluppare le competenze digitali degli studenti.

Per la scuola primaria, il curriculum si concentra sull'introduzione alle tecnologie in modo semplice e ludico, favorendo la curiosità e la creatività dei bambini. Si propongono attività come laboratori, giochi digitali e produzione di contenuti semplici, per sviluppare le prime competenze di informazione, comunicazione e creazione dei contenuti. È importante anche insegnare ai bambini a usare le tecnologie in modo sicuro e rispettoso, promuovendo un uso consapevole fin dai primi anni.

Nella scuola secondaria di primo grado, invece, il curriculum digitale si approfondisce, coinvolgendo gli studenti in attività più complesse come la produzione di video, podcast, presentazioni e l'uso di strumenti digitali per la ricerca e la collaborazione. Si rafforzano anche le competenze di cittadinanza digitale, affrontando temi come la privacy, il rispetto degli altri online e il contrasto alle fake news. In questa fase, si promuove anche l'uso responsabile delle tecnologie per supportare l'apprendimento e la crescita personale.

In entrambi gli ordini di scuola, il curriculum digitale si integra con le discipline e coinvolge tutta la comunità scolastica, inclusi docenti, famiglie e partner esterni.

I regolamenti e le attività legate alla prevenzione, presenti nell'ePolicy, rappresentano una componente costante delle iniziative di sensibilizzazione e diffusione promosse dall'istituto, ma non l'unica modalità d'intervento adottata.

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'ePolicy a livello generale, promuove un lavoro di comprensione e condivisione degli intenti tra tutta la comunità scolastica, creando un terreno comune su cui basare le azioni e le strategie. A livello specifico, invece, si immagina che ogni classe possa approfondire tematiche direttamente collegate alla sicurezza in rete, anche se queste sono spesso complesse e non sempre si integrano immediatamente nelle programmazioni scolastiche tradizionali. Tra gli argomenti più articolati ci sono l'etica digitale, il funzionamento degli algoritmi e il fenomeno della datafication, cioè la trasformazione dei dati in risorsa.

Per supportare questo percorso, si può fare affidamento sui materiali progettati messi a disposizione dal team di Generazioni Connesse. Questi materiali sono pensati sia come strumenti di attivazione, per coinvolgere attivamente docenti e studenti, sia come accompagnamento durante le fasi più delicate e significative del processo di prevenzione, in particolare durante le lezioni in classe. Il kit didattico può essere utilizzato nella sua interezza o selezionato in base alle esigenze e alle scelte del docente offrendo flessibilità nel suo impiego.

Il percorso si articola in cinque aree tematiche fondamentali:

- 1) la comprensione dei cambiamenti generati dalla convergenza tra tecnologie digitali e connettività, non che come questi influenzano il nostro modo di vivere;
- 2) le implicazioni di questi cambiamenti sulla nostra dimensione personale e sociale, analizzando come le tecnologie modificano le relazioni e le dinamiche sociali;
- 3) l'educazione all'informazione (information literacy), che mira a sviluppare competenze per cercare, raccogliere, utilizzare e conservare le informazioni, oltre a comprendere le trasformazioni profonde nell'ecosistema della produzione e distribuzione delle notizie;
- 4) le implicazioni della quantificazione e della computazione, aspetti intrinseci della diffusione delle tecnologie digitali e alla loro influenza sulla nostra vita quotidiana;
- 5) la connessione tra cittadinanza e creatività digitale, sottolineando come le competenze digitali possano favorire una partecipazione attiva e responsabile nella società.

Il Kit didattico prodotto da "Generazioni Connesse" nella scuola primaria può essere uno strumento molto utile, adattandosi

alle esigenze e alla capacità dei bambini più piccoli, infatti può così essere utilizzato per:

- 1) **Attività di sensibilizzazione e introduzione ai temi digitali:** il Kit contiene materiali semplici e coinvolgenti, come giochi, storie illustrate o video, che aiutano i bambini a capire i concetti base sulla sicurezza in rete, l'uso responsabile della tecnologia e l'importanza di rispettare gli altri on line.
- 2) **Laboratori e giochi educativi:** attraverso attività pratiche, i bambini possono imparare a riconoscere comportamenti corretti e scorretti in rete, sviluppando competenze di cittadinanza digitale in modo divertente e interattivo.
- 3) **Supporto ai docenti:** il Kit fornisce anche indicazioni e spunti per gli insegnanti, che possono integrare le attività nelle loro lezioni quotidiane, adattandole alle diverse età e livelli di comprensione dei bambini.
- 4) **Approccio graduale e personalizzato:** la possibilità di selezionare le parti del Kit più adatte permette ai docenti di costruire un percorso personalizzato, introducendo i temi in modo semplice e progressivamente più approfondito, in base alle esigenze della classe.
- 5) **Promozione di valori e comportamenti corretti:** le attività possono aiutare i bambini a sviluppare una coscienza critica rispetto all'uso della tecnologia, favorendo comportamenti responsabili e rispettosi, fondamentali già dalla scuola primaria.

In sintesi, il Kit è uno strumento molto versatile e coinvolgente per introdurre i più piccoli ai temi della sicurezza digitale e della cittadinanza digitale, creando un ambiente di apprendimento che combina divertimento e consapevolezza.

Anche nella scuola secondaria di primo grado il Kit prodotto da "Generazioni Connesse" può essere uno strumento molto utile. Di solito, è pensato per aiutare gli studenti a sviluppare competenze digitali e a comprendere meglio l'uso consapevole della tecnologia e dei social media. Può essere usato in varie modalità, ad esempio tramite attività pratiche, laboratori o lezioni frontali, per sensibilizzare i ragazzi sui rischi e le opportunità del mondo digitale. Può anche favorire il dialogo fra insegnanti e studenti su temi come la sicurezza on line, il rispetto reciproco e l'uso responsabile delle piattaforme digitali. Il Kit integra l'educazione digitale nel curriculum scolastico, rendendo gli studenti più consapevoli e preparati a navigare nel mondo digitale in modo sicuro e responsabile.

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 delle persone è un diritto fondamentale. Ciò significa che ogni individuo ha il diritto di vedere tutelata la propria privacy e di controllare come vengono utilizzati i propri dati. In Europa, tale tutela è sancita dall'art. 8, paragrafo 1 della Carta Dei Diritti Fondamentali dell'Unione Europea nonché dall'art. 16, paragrafo 1 del Trattato sul funzionamento dell'UE (TFUE). Questi stabiliscono chiaramente che ogni persona ha diritto alla protezione dei propri dati personali. Al fine di garantire tutela, ci sono anche alcune normative di riferimento molto importanti, tra queste il "Regolamento Generale sulla Protezione dei Dati", conosciuto come *GDPR* (Regolamento UE 2016/679) ed il "Codice Privacy" italiano (Dlgs 196/2003) che si occupano di regolamentare come devono essere trattati i dati personali in Italia.

Contrariamente a quanto si potrebbe pensare, la normativa sulla privacy non vuole ostacolare lo scambio d'informazioni, anzi, il suo obiettivo principale è proprio quello di favorire la circolazione delle informazioni dei dati all'interno dell'Unione Europea. Tuttavia lo fa introducendo una serie di regole e tutele per proteggere i diritti delle persone.

Gli adempimenti, a cui è tenuto il mondo della scuola, riguardo l'obbligo dell'informativa è sancito dall'art. 14 del GDPR, con questo la scuola fornisce a chi ha fornito i suoi dati personali una serie d'informazioni.

Il settore dell'istruzione, è molto coinvolto da questa tematica in quanto le scuole gestiscono un'enorme quantità di dati personali di studenti, genitori, docenti e personale scolastico. Con l'introduzione del *GDPR*, le scuole hanno obbligatoriamente dovuto nominare un *Responsabile della Protezione dei Dati*, chiamato *RPD* o *DPO*, figura competente delle norme sulla privacy con il compito di garantire che tutto venga eseguito nel rispetto della legge.

Gli obblighi principali che le scuole seguono, sono:

1) **Creare un "organigramma privacy"**: cioè una mappa di come vengono gestiti i dati all'interno della scuola;

2) **Fornire un'informativa sulla privacy:** che deve essere consegnata al momento della raccolta dati, spiegando in modo chiaro cosa si fa con i dati ed il perché;

3) **Tenere un registro dei trattamenti:** cioè un documento che riassume tutte le attività di trattamento dei dati, le categorie dei dati usati e le finalità di ogni operazione;

4) **Gestire il consenso:** in generale, se i dati vengono trattati per finalità istituzionali o didattiche, la scuola non ha bisogno di chiedere il consenso. Tuttavia, se si vogliono usare dati per attività extra - scolastiche, come ad es. corsi di musica, il consenso è necessario;

5) **Prevedere una procedura in caso di violazione dei dati (Data Breach):** questa procedura aiuta la scuola a reagire rapidamente se, ad es., ci fosse un attacco informatico che compromette i dati. La procedura deve indicare chi è il responsabile, quali sono le finalità e modalità di trattamento, quali dati vengono trattati, se ci sono comunicazioni a soggetti terzi o trasferimenti all'estero e anche misure di sicurezza adottate.

La normativa serve a garantire che i dati siano trattati in modo corretto e sicuro, rispettando sempre i diritti di chi li fornisce.

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.

Le tecnologie digitali stanno rivoluzionando gli ambienti di apprendimento, offrendo nuove possibilità per supportare la comunicazione all'interno delle scuole e promuovendo un approccio sempre più collaborativo tra studenti, insegnanti e personale scolastico. L'utilizzo degli strumenti di comunicazione on line, affiancati a quelli tradizionali, ha come obiettivo principale quello di rendere lo scambio d'informazioni più interattivo e orizzontale, favorendo un dialogo più aperto e partecipativo. Questo tipo di utilizzo delle tecnologie segue obiettivi e regole precise, che sono strettamente legate alle caratteristiche, alle funzionalità e potenzialità offerte da questi strumenti digitali. Per quanto riguarda gli strumenti di comunicazione on line utilizzabili a scuola, possiamo distinguere due principali categorie: la *Comunicazione Esterna* e quella *Interna*.

La **Comunicazione Esterna:** questi strumenti sono impiegati dalla scuola per raggiungere target esterni, con l'obiettivo di valorizzare e promuovere le attività dell'istituto nei tre ordini di scuola, oltre a diffondere informazioni di servizio o contenuti importanti tra i vari attori scolastici. tra questi troviamo il sito web della scuola, i profili su social network come *FB* o *Instagram*. Questi canali sono fondamentali per trasmettere all'esterno l'identità, i valori, i progetti e l'idea di educazione che l'istituto vuole comunicare. La comunicazione esterna può essere anche progettata e realizzata coinvolgendo gli studenti che possono produrre contenuti multimediali da diffondere attraverso i vari canali digitali, purché affiancati dai docenti, come ad es. pubblicazione sul sito delle UDA o altri lavori da loro realizzati e pubblicati su diverse tematiche.

La **Comunicazione Interna**: questi strumenti sono pensati per facilitare e rendere più partecipata la didattica e la comunicazione all'interno della scuola. I canali utilizzati nel nostro istituto sono il *Registro Elettronico "ARGO"* e la piattaforma **"TEAMS di microsoft 365"**.

Il *Registro Elettronico "ARGO"*: ogni utente ha un proprio account personale per accedere ai servizi. Attraverso questo strumento vengono inviate circolari, autorizzazioni, comunicazioni relative a provvedimenti disciplinari, programmazioni e altre informazioni di servizio, senza che nulla venga pubblicato sul sito web. Inoltre i docenti possono condividere con i genitori contenuti didattici.

La *piattaforma TEAM*: è una piattaforma utilizzata per comunicare, svolgere incontri in modalità sincrona e condividere contenuti digitali.

E' importante sottolineare che alunni, docenti e genitori, nel momento in cui ricevono le credenziali di accesso e dopo aver accettato l'informativa, devono essere consapevoli che i servizi offerti sono esclusivamente per uso scolastico e didattico.

Per quanto riguarda l'uso di altri strumenti di comunicazione on line tra colleghi come ad es. *WhatsApp* o *Instagram*, è fondamentale rispettare il "diritto alla disconnessione" (art. 22 del CCNL 2016/2018), che tutela il tempo di riposo e di non reperibilità dei lavoratori. Per le chat informali fra colleghi o fra docenti e genitori non esiste ancora una regolamentazione ufficiale, ma si possono stabilire alcune regole condivise per un uso responsabile:

- 1) chiarire fin dall'inizio le finalità del gruppo e rispettarle sempre, pubblicando solo contenuti pertinenti;
- 2) usare un linguaggio adeguato, chiaro e preciso per evitare fraintendimenti;
- 3) non discutere in chat argomenti complessi, bensì parlarne a voce durante consigli eventualmente anche straordinari;
- 4) limitare la condivisione di foto di studenti in chat, al fine di rispettare la legge sulla privacy;
- 5) non coinvolgere in discussioni riguardanti solo pochi, gli altri interlocutori che ne verrebbero disturbati;
- 6) i messaggi devono essere brevi ed esauritivi evitando troppi spezzettamenti.

Per quanto riguarda l'uso della rete a scuola e a casa, esiste un documento chiamato *Politica d'uso Accettabile e Responsabile della Rete (P.U.A.)* che raccoglie una serie di regole da seguire da parte degli utenti coinvolti. Questo documento fa parte del *Documento Programmatico sulla Sicurezza (DPS)*.

La **P.U.A.** evidenzia sia i vantaggi di internet a scuola, sia i rischi legati all'uso on line, come la ricerca di materiali non appropriati, azioni illecite, giochi on line sulla rete scolastica, violazioni della privacy e dei diritti d'autore.

Questa politica definisce le regole di utilizzo della rete per tutti gli attori coinvolti, con particolare attenzione alla tutela dei dati sensibili, soprattutto quelli degli studenti.

Il documento **P.U.A.** definisce le norme per l'utilizzo dei dispositivi informatici forniti dalla scuola. L'impiego di questi strumenti deve avvenire in maniera responsabile sia per quanto riguarda l'integrità fisica degli apparecchi sia per il corretto funzionamento dei software installati.

E' pertanto vietato:

- 1) utilizzare i dispositivi per scopi personali o non legati alle attività di studio;
- 2) collegare periferiche esterne come memorie USB o hard disk;
- 3) installare o disinstallare programmi e /o modificare le impostazioni predefinite;
- 4) copiare, caricare o scaricare musica, film, programmi o altro materiale non pertinente all'attività didattica, protetto da

copyright o in violazione delle norme del codice civile e penale relative al diritto d'autore, alla privacy, alla diffusione di contenuti offensivi, pedopornografici, ecc.

5) accesso alla rete WI- FI;

6) per i dispositivi dell'istituto dotati di accesso WI - FI, si utilizzeranno le credenziali di autenticazione gestite con massima attenzione e riservatezza.

E' fondamentale che tutti gli utenti siano pienamente consapevoli dei rischi connessi all'utilizzo dei dispositivi forniti dall'istituto.

I docenti sono responsabili dell'uso corretto dei dispositivi informatici ed hanno il dovere di sorvegliare e sensibilizzare gli studenti riguardo a un utilizzo consapevole e sicuro.

Gli utenti sono tenuti a rilasciare incustoditi i dispositivi informatici e devono disconnettere il proprio account al termine di ogni sessione di utilizzo.

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.

I dispositivi tecnologici sono parte integrante della vita scolastica (alunni, docenti e personale) e influenzano l'insegnamento e l'apprendimento. Comprendere il loro potenziale è cruciale, anche alla luce delle normative come il *Progetto Generazioni Connesse* e il *PNSD*.

Questa ePolicy mira a definire l'uso dei dispositivi personali in classe, tenendo conto delle indicazioni MIM (**BYOD**). E' fondamentale un dialogo nella comunità scolastica per creare una regolamentazione condivisa che consideri i benefici e le problematiche didattiche.

Quando autorizzato, gli studenti devono usare i dispositivi responsabilmente, rispettando gli altri e le regole scolastiche (DM n. 30/2007). Le famiglie sono responsabili per i danni o le violazioni del regolamento commesse dai figli. Dirigenti, docenti e personale ATA devono vigilare sul comportamento degli studenti in tutti gli spazi scolastici e segnalare infrazioni.

La normativa sulla privacy vieta l'acquisizione, la divulgazione e la pubblicazione di immagini, video o registrazioni senza il consenso scritto degli interessati (o dei tutori per i minori), pena sanzioni civili, penali e disciplinari (DPR n. 259/1998).

L'ePolicy si propone di regolamentare l'uso dei dispositivi personali a scuola, in linea con le indicazioni ministeriali e sottolinea l'importanza di una discussione e di una regolamentazione specifica e condivisa all'interno dell'istituto, valutando pro e contro per la didattica.

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.

Questa sezione del documento di ePolicy, definisce quelle che sono le procedure operative standard da usare per segnalare e gestire i problemi legati a comportamenti on line rischiosi eseguiti dagli alunni. Queste procedure rappresentano una guida costante per il personale scolastico per poter identificare situazioni on line a rischio, stabilendo come la scuola interviene e quali azioni intraprende per supportare gli alunni in difficoltà. Queste procedure forniscono inoltre indicazioni utili a professionisti e organizzazioni esterne che collaborano con l'istituto scolastico.

Le procedure specificano:

- 1) **Le figure responsabili** della ricezione delle segnalazioni, della presa in carico e della gestione dei casi.
- 2) **Le modalità di coinvolgimento** del referente per il contrasto al bullismo e al cyberbullismo e del Dirigente Scolastico. La scuola individua anche un team interno dedicato alla gestione delle segnalazioni (interna o tramite invio agli enti competenti).

Nell'affrontare i casi, prevediamo la collaborazione con figure, enti, istituzioni e servizi territoriali, qualora la gravità o la sistematicità della situazione richiedano interventi esterni alle competenze ed alle risorse della scuola.

Queste procedure sono comunicate e condivise con tutta la comunità scolastica attraverso assemblee con genitori, alunni, personale della scuola, notizie sul web, durante i collegi e tramite ogni canale utile per una comunicazione efficace.

Le **procedure** si riferiscono alle seguenti problematiche:

Cyberbullismo: è cruciale distinguere il cyberbullismo da altre problematiche, analizzando il contesto, le modalità di manifestazione (presenza di pubblico, tra coetanei, ripetitività, intenzionalità, danno percepito) e valutando il disagio degli alunni coinvolti per considerare un supporto psicologico o di mediazione.

Adescamento on line: in caso di sospetto, è prioritario non eliminare prove digitali e non interagire con l'adescatore al posto del minore colpito. E' fondamentale valutare il suo benessere psicofisico ed il rischio. La normativa prevede l'ascolto della vittima o del testimone di reati come grooming con l'assistenza di esperti in psicologia infantile.

Sexting: se immagini o video di minori vengono diffusi senza consenso, è necessario attivare i sistemi di segnalazione per tutelare il minore, rimuovere il materiale on line (dove possibile) e bloccare la diffusione tramite dispositivi mobili.

La legge 29 maggio 2017, n. 71 enfatizza il ruolo cruciale delle scuole nella prevenzione e gestione del fenomeno, introducendo l'obbligo di nominare un referente per il bullismo.

L'istituto scolastico ha il dovere di garantire la vigilanza in tutti gli spazi interni, incluse le aule, corridoi, palestre, spogliatoi e bagni.

In caso di mancata attuazione di misure preventive contro il cyberbullismo, la scuola può incorrere in responsabilità per colpa in organizzando.

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:

- Procura Ordinaria: 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.

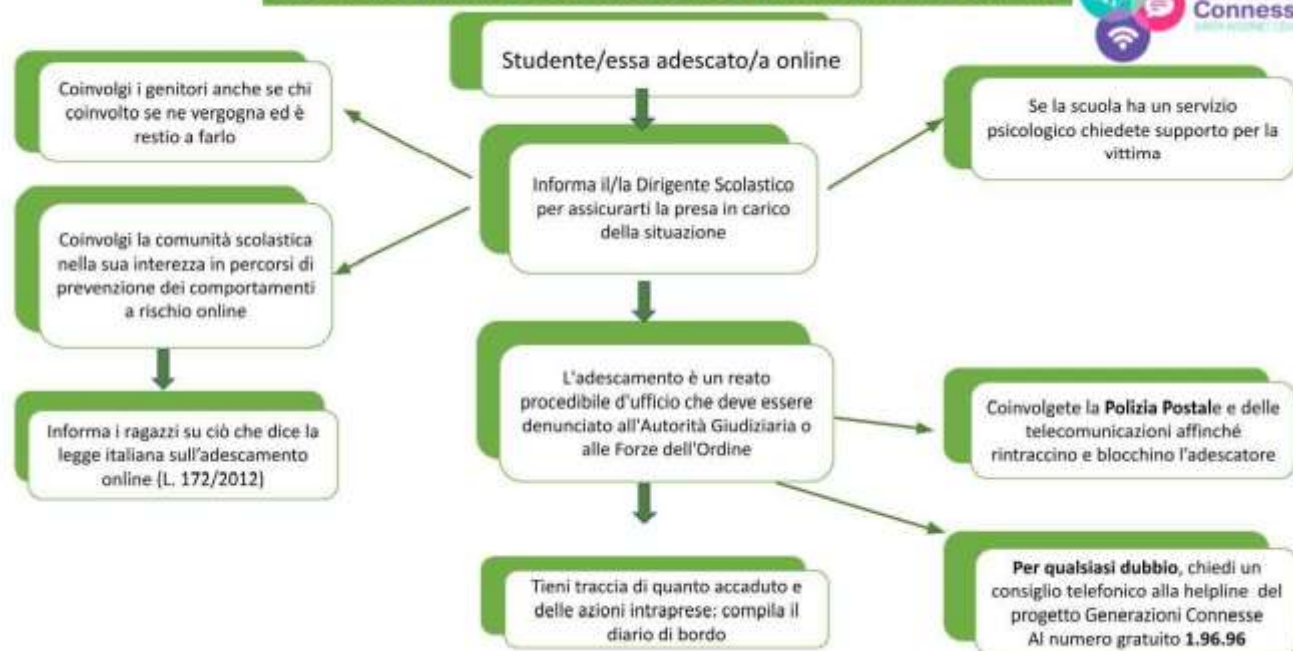
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

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

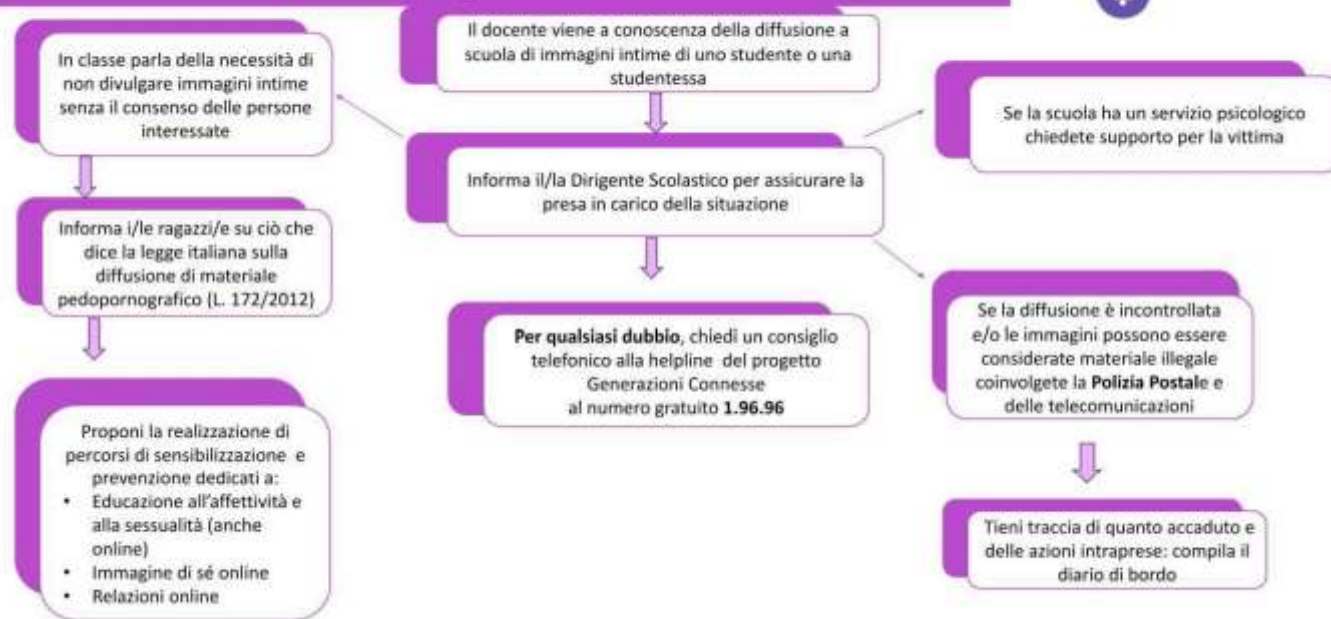
Se emergono evidenze passa allo schema successivo

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?



Gli insegnanti in quanto pubblici ufficiali (art. 357 c.p., confermato dalla Cassazione n. 15367/2014), hanno la responsabilità di segnalare comportamenti on line a rischio degli alunni.

La scuola è dotata di un team specializzato (docente referente, animatore digitale, referente bullismo/cyberbullismo) per

affrontare i rischi digitali. L'animatore digitale promuove un uso consapevole delle tecnologie, mentre il referente bullismo/cyberbullismo interviene tempestivamente, anche con esperti esterni in casi gravi. Un approccio multidisciplinare garantisce un supporto completo.

In **caso di sospetto** (macro Caso A) di cyberbullismo, sexting o adescamento, il docente deve segnalare dettagliatamente al referente ed al team, che valuteranno con la dirigente se coinvolgere autorità giudiziarie o attuare sensibilizzazione. Per casi delicati, si ricorre a consulenza esterna. La scuola può comunque intraprendere percorsi di sensibilizzazione per tutta la comunità scolastica, come già fa da due anni.

In **caso di evidenza** (macro Caso B) di reato, l'insegnante o il team hanno l'obbligo di denuncia all'autorità giudiziaria competente (procure ordinarie minorile). La mancata segnalazione di situazioni di pregiudizio (rischio di danno alla salute, dignità, sopravvivenza del minore) costituisce omissione di atti d'ufficio (art. 328 c.p.).

E' raccomandata l'organizzazione di incontri individuali con tutti i minori coinvolti (vittime, testimoni, responsabili) e la valutazione del coinvolgimento dei genitori. Gli interventi devono considerare l'impatto educativo ed emotivo, trattando tutti equamente.

La scuola può attivare diversi strumenti di segnalazione (email dedicata, box anonimo, sportello d'ascolto già attivo, docente referente).

Studenti, genitori e famiglie possono anche rivolgersi all' Helpine di Telefono Azzurro.

E' anche utile un sistema di monitoraggio dei casi, per sviluppare ulteriori attività di supporto, come eventi informativi, azioni didattiche preventive e collaborazioni con enti territoriali così come già da due anni vengono attivati.

Approvato con delibera n. 78 del Collegio Docenti del 25/06/2025
Approvato con delibera n. 43 del Consiglio d'Istituto del 27/06/2025