Documento di ePolicy
ITCET - LEONARDO SCIASCIA

VIA QUARTARARO PITTORE S.N.C. - 92100 - AGRIGENTO
Agrigento (AG) - Sicilia
Data di approvazione: 12/05/2025 - 22:43

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.

Il nostro istituto è ormai da anni impegnato nel considerare, come obiettivo principale della sua mission, la scuola come luogo di benessere.

La scuola, quale luogo di formazione, inclusione e accoglienza, deve perciò garantire la salute e la serenità psicofisica dello studente poiché essa rappresenta una condizione imprescindibile per il suo sviluppo personale e il raggiungimento del successo formativo. Di qui, la necessità di educare e di vigilare, in piena sinergia con le famiglie, affinché non si verifichino situazioni che possano turbarne il percorso di apprendimento e di crescita.

L'ePolicy si inserisce in un contesto educativo che promuove una **cultura digitale inclusiva, sicura e responsabile**, in linea con gli obiettivi del **Piano Nazionale Scuola Digitale (PNSD)** e del **Framework europeo DigComp**. Il documento rappresenta un impegno concreto per garantire che tutta la comunità educante (studenti, docenti, famiglie e personale scolastico) sviluppi competenze digitali trasversali, necessarie per navigare in modo critico e consapevole nel mondo digitale.

Obiettivi specifici del nostro Istituto

1. **Promuovere un uso positivo delle tecnologie**: attraverso attività formative e progetti didattici che incoraggiano la creatività, la collaborazione e l'apprendimento attivo, utilizzando strumenti digitali in modo etico e responsabile.

2. **Prevenire i rischi online**: sensibilizzando gli studenti sui pericoli del cyberbullismo, del sexting, dell'adescamento online e della dipendenza digitale, attraverso laboratori, incontri con esperti e campagne di informazione.

3. **Integrare le tecnologie nella didattica**: favorendo l'uso delle ICT come strumenti per l'innovazione metodologica, in un'ottica di inclusione e personalizzazione dei percorsi di apprendimento.

4. **Garantire la sicurezza digitale**: adottando misure tecniche e organizzative per proteggere i dati personali degli studenti e del personale scolastico, in conformità al **GDPR** e alle normative vigenti.

Ruolo della comunità educante

- **Docenti**: sono chiamati a essere modelli di riferimento per un uso consapevole delle tecnologie, integrando le competenze digitali nel curricolo scolastico e partecipando a percorsi di formazione continua.

  Essi sono tenuti a veicolare agli studenti atteggiamenti e credenze di non accettabilità di comportamenti irresponsabili, a percepirsi auto-efficaci nel proprio ruolo di docenti e in questo senso è necessaria la formazione e autoformazione attraverso l'implementazione delle conoscenze relative al tema della sicurezza in rete perché la scuola definisca i propri piani di intervento.

- **Studenti**: sono protagonisti attivi del processo di apprendimento, incoraggiati a utilizzare le tecnologie in modo critico, creativo e responsabile, rispettando sé stessi e gli altri. Tutti gli alunni hanno, infatti, il diritto a svolgere il proprio percorso di formazione e crescita all'interno di un ambiente di apprendimento sicuro e sereno. Contemporaneamente tutti gli studenti si impegnano ad avere un atteggiamento inclusivo e rispettoso nei confronti di tutti e di ciascuno.

- **Famiglie**: sebbene non sempre senza difficoltà, le famiglie sono coinvolte in iniziative di informazione e formazione per supportare i figli nell'uso sicuro e positivo della Rete.

- **Personale scolastico**: collabora per garantire un ambiente digitale sicuro e funzionale, rispettando le norme di privacy e sicurezza.

Impegno dell'Istituto

Il nostro Istituto si impegna a:

- Realizzare un **Piano di Azione triennale** con obiettivi chiari e misurabili, monitorando periodicamente i risultati raggiunti.

- Creare una **rete di collaborazione** con enti locali, associazioni e forze dell'ordine per affrontare in modo efficace le situazioni di rischio.

- Promuovere una **cultura della segnalazione**, incoraggiando studenti e famiglie a segnalare tempestivamente episodi di disagio o comportamenti inappropriati online.

1.2 - ePolicy: ruoli e responsabilità nell'implementazione dell'ePolicy

- (In questo paragrafo vengono dettagliati ruoli e responsabilità nell'implementazione del documento all'interno dei contesti scolastici ivi inclusi rappresentanti genitori e studenti per secondaria II grado).

Affinché l'ePolicy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, s'impegni nell'attuazione e promozione di essa.

È opportuno che nel documento vengano definiti con chiarezza ruoli, compiti e responsabilità di ciascuna delle figure all'interno dell'Istituto.

In questo paragrafo dell'ePolicy è importante specificare le figure professionali che, a vario titolo, si occupano di gestione e programmazione delle attività formative, didattiche ed educative dell'Istituto e tutte quelle figure appartenenti alla comunità educante.

IL DIRIGENTE SCOLASTICO

Il ruolo del Dirigente Scolastico nel promuovere l'uso consentito delle tecnologie digitali e di internet include i seguenti compiti:

- promuovere la cultura della sicurezza online e garantirla a tutti i membri della comunità scolastica, in linea con il quadro normativo di riferimento, le indicazioni del MIM, delle sue agenzie e attraverso il documento di ePolicy;
- promuovere la cultura della sicurezza online – anche attraverso il documento di ePolicy - integrandola ed inserendola nelle misure di sicurezza più generali dell'intero Istituto;
- ha la responsabilità di fornire sistemi per un uso sicuro delle TIC, internet, i suoi strumenti ed ambienti e deve garantire alla popolazione scolastica la sicurezza di navigazione tramite internet utilizzando adeguati sistemi informatici e filtri;
- ha la responsabilità della gestione dei dati e della sicurezza delle informazioni e garantisce che l'Istituto segue le pratiche migliori possibili nella gestione dei dati stessi;
- deve tutelare la scuola e garantire agli utenti la sicurezza di navigazione utilizzando adeguati sistemi informatici e servizi di filtri Internet;
- ha il compito di garantire a tutto il personale una formazione adeguata sulla sicurezza online per essere tutelato nell'esercizio del proprio ruolo educativo e non;
- deve essere a conoscenza delle procedure da seguire in caso di un grave incidente di sicurezza online;
- deve garantire adeguate valutazioni di rischio nell'usare strumenti e TIC, effettuate in modo che comunque quanto programmato possa soddisfare le istanze educative e didattiche dichiarate nel PTOF di Istituto;
- deve garantire l'esistenza di un sistema che assicuri il monitoraggio e il controllo interno della sicurezza online in collaborazione con le figure di sistema;
- deve essere a conoscenza ed attuare le procedure necessarie in caso di grave incidente di sicurezza online.

L'ANIMATORE DIGITALE E IL TEAM PER L'INNOVAZIONE DIGITALE

L'animatore digitale e il Team per l'Innovazione digitale sono co-responsabili, con il referente ePolicy, dell'attuazione dei piani di azione in particolare in riferimento alla formazione dei docenti. Sono inoltre responsabili del controllo all'accesso da parte degli studenti delle Tic

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

Il referente cyberbullismo è co-responsabile, con il team ePolicy, dell'attuazione dei piani di azione e coordina le iniziative di prevenzione e contrasto del cyberbullismo.

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

In coerenza con le Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo del Ministero dell'Istruzione (D.M. n. 18 del 13/1/2021, agg. 2021 – nota prot. 482 del 18-02-2021), il Team ha le funzioni di coadiuvare il Dirigente Scolastico, coordinatore del Team nella scuola, nella definizione degli interventi di prevenzione e nella gestione dei casi di bullismo e cyberbullismo che si possono presentare. Promuove inoltre la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale e comunica ad alunni, famiglie e tutto il personale scolastico dell'esistenza del team, a cui poter fare riferimento per segnalazioni o richieste di informazioni sul tema.

Il Team ha il compito di:

- coadiuvare il Dirigente scolastico, coordinatore del Team, nella definizione degli interventi di prevenzione del bullismo (per questa funzione partecipano anche il presidente del Consiglio d'Istituto e i Rappresentanti degli studenti).
- Intervenire (come gruppo ristretto, composto da Dirigente e referente o referenti per il bullismo e il cyberbullismo, psicologo o pedagogista, se presente) nelle situazioni acute di bullismo.
- Promuovere la redazione e l'applicazione della ePolicy e monitorare le segnalazioni.

I/LE DOCENTI

I/le docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Possono, innanzitutto, integrare la propria disciplina con approfondimenti, promuovendo l'uso delle tecnologie digitali nella didattica. I docenti devono accompagnare e supportare gli/le studenti nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete. Inoltre, educano gli studenti alla prudenza, a non fornire dati ed informazioni personali, ad abbandonare un sito dai contenuti che possono turbare o spaventare e a non incontrare persone conosciute in Rete senza averne prima parlato con i genitori. Informano gli alunni sui rischi presenti in Rete, senza demonizzarla, ma sollecitandone un uso consapevole, in modo che Internet possa rimanere per bambini/e e ragazzi/e una fonte di divertimento e uno strumento di apprendimento.

I/le docenti osservano altresì regolarmente i comportamenti a rischio (sia dei potenziali bulli, sia delle potenziali vittime) e hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che veda coinvolti studenti e studentesse dandone tempestiva comunicazione al Dirigente Scolastico, al Referente per il Cyberbullismo e Bullismo e al Consiglio di Classe per definire strategie di intervento condivise.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Responsabile della protezione dei dati (RPD o DPO) conosce l'ePolicy di Istituto, fornisce la propria consulenza in merito agli obblighi derivanti dal GDPR e sorveglia sull'esatta osservanza della normativa in materia di tutela dei dati personali ed è co-responsabile delle azioni di informazione e formazione nell'Istituto sulla protezione dei dati personali

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

Il personale ATA, all'interno dei singoli regolamenti d'Istituto, è coinvolto nelle pratiche di prevenzione – ivi incluso il processo di definizione e implementazione dell'ePolicy di Istituto - ed è tenuto alla segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.

GLI STUDENTI E LE STUDENTESSE

Gli studenti e le studentesse devono, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti. Con il supporto della scuola dovrebbero imparare a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le. Affinché questo accada devono partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

I rappresentanti degli/delle studenti sono informati del documento di ePolicy e invitati a costruire i piani di azione, a partire dal secondo anno della secondaria di II grado,

I GENITORI/ADULTI DI RIFERIMENTO

I Genitori, in continuità con l'Istituto scolastico, sono attori partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile degli strumenti personali (pc, smartphone, etc). Come parte della comunità educante sono tenuti a relazionarsi in modo costruttivo con i/le docenti sulle linee educative che riguardano le TIC e la Rete e – ivi incluso il documento di ePolicy - comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet.

È estremamente importante che accettino e condividano quanto scritto nell'ePolicy d'Istituto e nel patto di corresponsabilità in un'ottica di collaborazione reciproca. Si promuove il coinvolgimento dei rappresentanti di genitori/adulti di riferimento all'interno del percorso di definizione e implementazione dell'ePolicy.

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

Enti esterni pubblici e privati, il mondo dell'associazionismo dovranno conformarsi alla politica della scuola riguardo all'uso consapevole delle TIC e della rete per la realizzazione di iniziative nelle scuole, finalizzate a promuovere un uso positivo e consapevole delle Tecnologie Digitali da parte dei più giovani, e/o finalizzate a prevenire e contrastare situazioni di rischio online e valutare la rispondenza delle proposte di attività di sensibilizzazione/formazione alle esigenze di qualità contenute nel documento di ePolicy. Dovranno inoltre promuovere comportamenti sicuri durante le attività che si svolgono con gli/le studenti e verificare di aver implementato una serie di misure volte a garantire la tutela dei minori nel caso di insorgenza di problematiche e ad assicurarne la tempestiva individuazione e presa in carico.

Ruoli e Responsabilità nel Nostro Istituto

Nel nostro Istituto, l'implementazione dell'ePolicy è un processo **collaborativo e partecipativo**, che coinvolge attivamente tutte le componenti della comunità educante. Di seguito, vengono delineati i ruoli e le responsabilità specifiche per ciascuna figura, in linea con le esigenze e le priorità del nostro contesto scolastico.

Il Dirigente Scolastico

Oltre ai compiti già delineati, il Dirigente Scolastico del nostro Istituto si impegna a:

- Promuovere **iniziative di formazione continua** per il personale docente e ATA, con particolare attenzione alle nuove sfide digitali.
- Garantire l'integrazione dell'ePolicy con il **Piano Triennale dell'Offerta Formativa (PTOF)**, assicurando che le competenze digitali siano parte integrante del curricolo scolastico.
- Favorire la creazione di una **rete di collaborazione** con enti locali, associazioni e forze dell'ordine per affrontare in modo efficace le situazioni di rischio online.

L'Animatore Digitale e il Team per l'Innovazione

Nel nostro Istituto, l'Animatore Digitale e il Team per l'Innovazione:

- Coordinano **laboratori didattici** per studenti e docenti, finalizzati all'uso creativo e responsabile delle tecnologie digitali.
- Supportano i docenti nell'integrazione delle ICT nella didattica quotidiana, promuovendo metodologie innovative come il **flipped classroom** e il **project-based learning**.
- Monitorano l'efficacia dei filtri e delle misure di sicurezza adottate per la navigazione online, segnalando eventuali criticità al Dirigente Scolastico.

Il Referente per il Bullismo e Cyberbullismo

Nel nostro Istituto, il Referente per il Bullismo e Cyberbullismo:

- Organizza **incontri periodici** con studenti e genitori per sensibilizzare sui rischi del cyberbullismo e sulle strategie di prevenzione.
- Collabora con il **Team Antibullismo** per gestire tempestivamente le segnalazioni e attivare percorsi di supporto psicologico e educativo.
- Promuove campagne di informazione, come la **Giornata Nazionale contro il Bullismo e il Cyberbullismo**, coinvolgendo tutta la comunità scolastica.

I Docenti

I docenti del nostro Istituto:

- Integrano nel proprio insegnamento **moduli specifici** sull'educazione digitale, utilizzando risorse come il **Framework DigComp** e le linee guida del **PNSD**.
- Partecipano a **corsi di formazione** sull'uso consapevole delle tecnologie e sulla prevenzione dei rischi online, condividendo buone pratiche con i colleghi.
- Osservano e segnalano comportamenti a rischio, collaborando con il Referente per il Cyberbullismo e il Team Antibullismo per definire strategie di intervento condivise.

Gli Studenti e le Studentesse

Nel nostro Istituto, gli studenti e le studentesse sono chiamati a:

- Partecipare attivamente a **progetti di peer education**, diventando ambasciatori di un uso positivo e responsabile delle tecnologie digitali.
- Segnalare tempestivamente episodi di cyberbullismo o comportamenti inappropriati online, utilizzando i canali predisposti dalla scuola.
- Rispettare le regole dell'ePolicy e del **Patto di Corresponsabilità**, contribuendo a creare un ambiente scolastico sicuro e inclusivo.

I Genitori e gli Adulti di Riferimento

I genitori del nostro Istituto sono invitati a:

- Partecipare a **incontri formativi** sull'uso consapevole delle tecnologie digitali, organizzati in collaborazione con esperti e associazioni del territorio.
- Collaborare con i docenti per monitorare l'uso che i figli fanno di smartphone, social network e altri dispositivi digitali.
- Condividere con la scuola eventuali preoccupazioni o segnalazioni relative a comportamenti online a rischio.

Il Personale ATA

Il personale ATA del nostro Istituto:

- Supporta la gestione delle strumentazioni digitali, garantendo il corretto funzionamento delle infrastrutture ICT.
- Partecipa alle iniziative di formazione sulla sicurezza online, contribuendo a creare un ambiente scolastico sicuro e protetto.
- Segnala tempestivamente al Dirigente Scolastico eventuali problematiche tecniche o comportamentali rilevate durante l'uso delle tecnologie digitali.

Collaborazione con Enti Esterni

Il nostro Istituto collabora con:

- **Forze dell'Ordine**: per organizzare incontri di sensibilizzazione sui rischi del cyberbullismo e dell'adescamento online.
- **Associazioni del territorio**: per promuovere progetti educativi e laboratori pratici sull'uso consapevole delle tecnologie.
- **Enti di formazione**: per garantire ai docenti e al personale scolastico un aggiornamento costante sulle nuove sfide digitali.

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.

Integrazione dell'ePolicy nei Documenti Istituzionali

Nel nostro Istituto, l'ePolicy non è solo un documento programmatico, ma uno **strumento operativo** che guida le scelte educative, organizzative e formative in materia di cittadinanza digitale. Per garantire una piena integrazione dell'ePolicy

nella vita scolastica, abbiamo previsto le seguenti azioni:

Aggiornamento del Regolamento d'Istituto

Il Regolamento d'Istituto è stato aggiornato, a partire dall'anno scolastico 23/24, con il Regolamento per l'utilizzo dei siti internet e dei social network e, a partire dall'anno scolastico 2024/25 con il Regolamento sull'uso dei laboratori e con il Regolamento sull'uso dell'intelligenza artificiale. Tanto per includere:

- **Norme comportamentali** specifiche per l'uso delle tecnologie digitali, sia in ambito didattico che extracurricolare.
- **Procedure chiare** per la gestione delle situazioni di rischio online, come il cyberbullismo o l'accesso a contenuti inappropriati.
- **Linee guida** per l'utilizzo responsabile dei laboratori, dei dispositivi personali (BYOD) e degli strumenti di comunicazione online (PUA).

Integrazione nel Patto di Corresponsabilità

Il Patto di Corresponsabilità è stato arricchito con una specifica sezione che mira alla prevenzione del bullismo e cyberbullismo e che vuole rendere espliciti i dirittti e i doveri delle parti chiamate in gioco nel fondamentale proceso di co-costruzione:

- **Impegni specifici** per le famiglie, tra cui la partecipazione attiva a incontri formativi sull'uso consapevole delle tecnologie digitali e la collaborazione con la scuola per monitorare i comportamenti online dei propri figli.
- **Indicazioni per gli studenti**, che si impegnano a rispettare le regole dell'ePolicy e a segnalare tempestivamente episodi di disagio o comportamenti inappropriati.
- **Obiettivi condivisi** per la comunità educante, tra cui la promozione di un clima scolastico inclusivo e rispettoso, anche negli ambienti digitali.

Inserimento nel Piano Triennale dell'Offerta Formativa (PTOF)

Il PTOF del nostro Istituto include:

- **Progetti didattici** trasversali per lo sviluppo delle competenze digitali, in linea con il **Framework DigComp** e le indicazioni del **Piano Nazionale Scuola Digitale (PNSD)**.
- **Azioni di sensibilizzazione** sui temi della sicurezza online, rivolte a studenti, docenti e famiglie, con il supporto di esperti e associazioni del territorio.

- **Monitoraggio periodico** delle attività legate all'ePolicy, per valutarne l'efficacia e apportare eventuali miglioramenti.

Coerenza con il RAV e il PdM

L'ePolicy è strettamente collegata al **Rapporto di Autovalutazione (RAV)** e al **Piano di Miglioramento (PdM)** del nostro Istituto, in particolare per quanto riguarda:

- **Obiettivo 4 (Competenze di cittadinanza)**: promuovere un uso consapevole e responsabile delle tecnologie digitali come competenza chiave per la cittadinanza attiva.
- **Obiettivo 5 (Inclusione e benessere)**: prevenire e contrastare fenomeni di cyberbullismo e disagio online, garantendo un ambiente scolastico sicuro e inclusivo.

Collaborazione con il Territorio

Per rafforzare l'integrazione dell'ePolicy, il nostro Istituto collabora con:

- **Enti locali e associazioni**: per organizzare eventi formativi e campagne di sensibilizzazione sui rischi e le opportunità del digitale.
- **Forze dell'Ordine**: per fornire agli studenti e alle famiglie strumenti concreti per la prevenzione dei rischi online.
- **Università e centri di ricerca**: per aggiornare costantemente le competenze digitali del personale scolastico e sperimentare nuove metodologie didattiche.

Monitoraggio e Valutazione

Per garantire l'efficacia dell'ePolicy, il nostro Istituto si impegna a:

- **Valutare periodicamente** le attività realizzate, attraverso questionari di gradimento e indicatori di risultato.
- **Coinvolgere tutta la comunità educante** nel processo di miglioramento, raccogliendo feedback e suggerimenti.
- **Aggiornare il documento** in base alle nuove esigenze e alle evoluzioni normative e tecnologiche.

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.

Informazione e Coinvolgimento della Comunità Educante

Nel nostro Istituto, la creazione e la condivisione dell'epolicy sono considerate **prioritarie** per garantire un approccio condiviso e consapevole all'uso delle tecnologie digitali. Di seguito, vengono descritte le azioni specifiche che abbiamo previsto per informare e coinvolgere la comunità educante:

Versione Sintetica per Studenti

- La versione sintetica dell'ePolicy verrà integrata nel **curricolo di educazione civica**, con attività didattiche mirate a far comprendere agli studenti l'importanza di un uso responsabile della Rete.
- Sono organizzati, anche con il supporto del team per la prevenzione e contrasto del bullismo e del cyberbullismo, dei **laboratori interattivi** in cui gli studenti, guidati dai docenti, analizzano casi pratici e simulano situazioni di rischio online.
- Gli studenti sono coinvolti in **progetti di peer education**, diventando ambasciatori delle buone pratiche digitali all'interno della scuola e del territorio.

Versione Sintetica per le Famiglie

- La scuola intende distribuire una versione sintetica per le famiglie durante i **colloqui scuola-famiglia** e pubblicare sul **sito web dell'Istituto** la versione integrale per una consultazione più approfondita del documento.
- Saranno organizzati **incontri formativi** dedicati ai genitori, con la partecipazione di esperti in educazione digitale e psicologi, per approfondire temi come la sicurezza online, la privacy e la gestione del tempo davanti agli schermi.

Comunicazione e Condivisione con gli Attori Esterni

Il nostro Istituto si impegna a collaborare con **enti pubblici, aziende e associazioni** per promuovere progetti di cittadinanza digitale e sensibilizzare la comunità sui rischi e le opportunità del mondo online. Le iniziative includono:

- **Partnership con le Forze dell'Ordine**: organizzazione di incontri periodici con la Polizia Postale per informare studenti e famiglie sui pericoli del cyberbullismo, dell'adescamento online e della dipendenza digitale.
- **Collaborazione con Associazioni del Territorio**: realizzazione di campagne di sensibilizzazione, come la **Giornata della Sicurezza in Rete**, in collaborazione con enti no-profit e centri di aggregazione giovanile.
- **Progetti con Aziende Tecnologiche**: partecipazione a programmi di formazione sull'uso consapevole delle tecnologie, promossi da aziende leader nel settore digitale.

Strumenti di Comunicazione

Per garantire una diffusione efficace dell'ePolicy, il nostro Istituto utilizza:

- **Sito Web e Social Media**: pubblicazione di articoli, video e infografiche sui temi della cittadinanza digitale
- **Eventi Aperti al Territorio**: organizzazione di conferenze, workshop e seminari per coinvolgere l'intera comunità locale.

Monitoraggio e Feedback

Per valutare l'efficacia delle azioni intraprese, il nostro Istituto:

- **Raccoglie feedback** attraverso questionari anonimi rivolti a studenti, genitori e docenti.
- **Monitora i risultati** delle attività formative e dei progetti realizzati, utilizzando indicatori quantitativi e qualitativi.
- **Aggiorna l'ePolicy** in base alle nuove esigenze emerse e alle evoluzioni normative e tecnologiche.

1.5 - I Piani di Azione dell'ePolicy

I piani di azione rappresentano il **programma triennale** di obiettivi che la scuola intende realizzare per promuovere la conoscenza delle regole e dei protocolli di intervento che sono stati adottati con il documento di ePolicy nella comunità scolastica.

Nei Piani di Azione sono riportati **gli impegni e le responsabilità** che la scuola si assume per promuovere sui temi dell'educazione civica digitale e dell'utilizzo sicuro e consapevole delle tecnologie e della rete:

- la rilevazione dei bisogni
- le iniziative informative e formative,
- la formazione di docenti, studenti e studentesse, e famiglie,
- il monitoraggio e la valutazione delle azioni (laddove possibile, anche all'interno del RAV);

I Piani di Azione si distinguono tra standard, comuni ad ogni scuola che ha adottato l'ePolicy, e autoprodotti ovvero definiti dalla scuola sulla base del proprio contesto territoriale e delle collaborazioni in essere con Istituzioni, associazioni e aziende.

1° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

- Realizzare un evento di presentazione dell'ePolicy ai docenti dell'Istituto;
- Realizzare un evento di diffusione dell'ePolicy in occasione degli Open Day e/o in occasione del SID dell'Istituto dedicato alle famiglie ed a studenti/esse;
- Diffondere l'ePolicy negli ambienti scolastici, a studenti e studentesse, docenti e famiglie attraverso le versioni friendly dell'ePolicy;

MODULO II

- Effettuare una rilevazione del fabbisogno formativo dei docenti sui temi dell'educazione civica digitale;
- Effettuare una rilevazione di interessi, bisogni e comportamenti delle famiglie sull' uso positivo del digitale;
- Avviare l'introduzione dell kit didattico come metodo e risorsa di lavoro in alcune classi pilota;

MODULO III

- Integrare l'ePolicy (norme, regolamenti e procedure) nei documenti dell'Istituto;
- Aggiornare la Politica d'Uso Accettabile (PUA) della scuola ed il regolamento BYOD dell'Istituto;

MODULO IV

- Definizione, a partire da quanto definito nell'ePolicy, delle procedure di segnalazione anche con linguaggio child/youth friendly perché possano essere accessibili a studenti e studentesse;
- Realizzare una reportistica delle segnalazioni ricevute e dei relativi esiti.

2° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

- Realizzare una formazione rivolta ai docenti dell'Istituto, sulla base dei risultati della rilevazione svolta nel corso del primo anno, anche attraverso il supporto di esperti/associazioni esterne o avvalendosi del percorso disponibile sul sito di Generazioni Connesse. La formazione deve coprire almeno il 60% del corpo docente.

MODULO II

- L'istituto utilizza il kit didattico come pratica metodologica e risorse a disposizione dei docenti per i percorsi di ECD attraverso la formazione specifica sviluppata per i docenti attraverso il sito di Generazioni Connesse;
- Effettuare una rilevazione di interessi, bisogni, comportamenti, abitudini di studenti e studentesse sui temi dell'educazione civica digitale;
- Realizzare una formazione rivolta agli studenti e alle studentesse attraverso il percorso previsto sulla piattaforma di Generazioni Connesse;
- Realizzare una formazione rivolta alle famiglie attraverso il percorso previsto sulla piattaforma di Generazioni Connesse

Piani di Azione Triennali del Nostro Istituto

I Piani di Azione triennali del nostro Istituto sono stati progettati per rispondere alle esigenze specifiche del nostro contesto scolastico e territoriale, con l'obiettivo di promuovere un uso **consapevole, sicuro e positivo** delle tecnologie digitali. Di seguito, vengono descritte le azioni prioritarie che abbiamo previsto per ciascun anno.

Primo Anno di Attività

MODULO I – Presentazione e Diffusione dell'ePolicy

- Organizzazione di un **evento di lancio** dell'ePolicy rivolto a docenti, studenti e famiglie, con la partecipazione di esperti in educazione digitale e rappresentanti delle istituzioni locali.
- Creazione di **versioni friendly** dell'ePolicy, con linguaggi e formati adatti a studenti e genitori, distribuite durante gli Open Day e pubblicate sul sito web dell'Istituto.
- Inserimento dell'ePolicy nel **Patto di Corresponsabilità** e nel **Regolamento d'Istituto**, per garantire una piena integrazione nella vita scolastica.

MODULO II – Rilevazione dei Bisogni

- Somministrazione di **questionari** a docenti e famiglie per rilevare il fabbisogno formativo e le esigenze specifiche in materia di educazione civica digitale.

MODULO III – Integrazione e Aggiornamento

- Aggiornamento del **Regolamento BYOD**, con l'introduzione di norme chiare per l'uso responsabile delle tecnologie in ambito scolastico.
- Integrazione dell'ePolicy nei documenti istituzionali, tra cui il **PTOF** e il **RAV**, per garantire coerenza con gli obiettivi educativi e formativi dell'Istituto.

MODULO IV – Segnalazione e Monitoraggio

- Creazione di un **sistema di segnalazione** accessibile e user-friendly, con linguaggio adatto a studenti e studentesse, per facilitare la segnalazione di episodi di cyberbullismo o altri comportamenti a rischio.
- Avvio di un **monitoraggio periodico** per monitorare le segnalazioni ricevute e valutare l'efficacia delle azioni intraprese.

Secondo Anno di Attività

MODULO I – Formazione Docenti

- Realizzazione di **percorsi formativi** per i docenti, con il supporto di esperti esterni e risorse della piattaforma Generazioni Connesse.

- Coinvolgimento di un crescente numero di docenti in attività di formazione, con l'obiettivo di sviluppare competenze digitali trasversali e metodologie didattiche innovative.

MODULO II – Formazione Studenti e Famiglie

- Utilizzo del **kit didattico** di Generazioni Connesse come risorsa principale per i percorsi di educazione civica digitale, con attività pratiche e laboratoriali rivolte agli studenti.

- Organizzazione di **incontri formativi** per le famiglie, con focus su temi come la sicurezza online, la privacy e la gestione del tempo davanti agli schermi.

- Realizzazione di un **sondaggio** tra gli studenti per rilevare interessi, bisogni e comportamenti legati all'uso delle tecnologie digitali.

Terzo Anno di Attività

MODULO I – Consolidamento e Valutazione

- **Monitoraggio** delle attività realizzate nei primi due anni, con l'obiettivo di valutare l'efficacia delle azioni intraprese e identificare eventuali aree di miglioramento.

- **Aggiornamento** dell'ePolicy in base ai risultati del monitoraggio e alle nuove esigenze emerse.

MODULO II – Espansione e Collaborazione

- Estensione delle attività formative a **tutta la comunità educante**.

- Rafforzamento delle **collaborazioni con il territorio**, attraverso progetti condivisi con enti locali, associazioni e aziende del settore tecnologico.

MODULO III – Innovazione e Sperimentazione

- Implementazione di **nuove metodologie didattiche**, come il coding, la robotica educativa e il digital storytelling, per promuovere un uso creativo e consapevole delle tecnologie.

- Sperimentazione di **strumenti digitali avanzati**, come piattaforme di apprendimento online e ambienti virtuali, per arricchire l'offerta formativa dell'Istituto.

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

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

Utilizzo delle Risorse di Generazioni Connesse nel Nostro Istituto

Il nostro Istituto riconosce il valore delle risorse messe a disposizione da **Generazioni Connesse** per supportare l'educazione civica digitale e l'uso responsabile delle tecnologie. Di seguito, vengono descritte le modalità con cui intendiamo utilizzare queste risorse per raggiungere i nostri obiettivi.

Kit Didattico

- Il **Kit Didattico** di Generazioni Connesse sarà integrato nel curricolo scolastico come strumento principale per l'educazione civica digitale.
- Verrà utilizzato in **classi pilota** durante il primo anno, per sperimentare attività pratiche e laboratoriali su temi come il cyberbullismo, la privacy online e l'uso consapevole dei social network.
- I docenti saranno formati sull'uso del kit attraverso **workshop dedicati**, organizzati in collaborazione con il Team per l'Innovazione Digitale.

Area Formazione

- L'**Area Formazione** di Generazioni Connesse sarà utilizzata per garantire una formazione continua a docenti, studenti e famiglie.
- I docenti parteciperanno ai **percorsi formativi online** per acquisire competenze specifiche sull'educazione civica digitale e sulle metodologie didattiche innovative.
- Gli studenti saranno coinvolti in **moduli interattivi** per approfondire temi come la sicurezza online e la gestione delle relazioni digitali.
- Le famiglie avranno accesso a **materiali informativi** e webinar per supportare i figli nell'uso responsabile delle

tecnologie.

Canali Social e Video

- I **canali YouTube, TikTok, Instagram e Facebook** di Generazioni Connesse saranno integrati nelle attività di sensibilizzazione dell'Istituto.
- I video-stimolo e i webinar saranno utilizzati durante le **lezioni di educazione civica** per stimolare il dibattito e la riflessione critica tra gli studenti.
- I contenuti dei social media saranno condivisi con le famiglie attraverso il **sito dell'Istituto**, per promuovere una cultura digitale condivisa.

Progetti e Collaborazioni

- Il nostro Istituto parteciperà attivamente alle **campagne nazionali** promosse da Generazioni Connesse, come il **Safer Internet Day (SID)**, organizzando eventi e attività coinvolgenti per studenti e famiglie.
- Collaboreremo con il **team di Generazioni Connesse** per realizzare progetti specifici, come laboratori di digital storytelling e percorsi di peer education.
- I materiali prodotti dagli studenti durante questi progetti saranno condivisi sui **canali social dell'Istituto**, per amplificare l'impatto delle iniziative e coinvolgere l'intera comunità educante.

Monitoraggio e Valutazione

- L'utilizzo delle risorse di Generazioni Connesse sarà monitorato attraverso **questionari di gradimento** e **indicatori di risultato**, per valutarne l'efficacia e apportare eventuali miglioramenti.
- I feedback raccolti saranno utilizzati per **aggiornare l'ePolicy** e definire nuove priorità per i Piani di Azione triennali.

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.

Sensibilizzazione e Prevenzione nel Nostro Istituto

Il nostro Istituto si impegna a promuovere una cultura digitale consapevole e responsabile, attraverso **azioni formative e preventive** rivolte a studenti, docenti e famiglie. Di seguito, vengono descritte le iniziative specifiche che abbiamo previsto per raggiungere questo obiettivo.

Azioni Formative per Studenti

- **Laboratori Didattici**: organizzazione di laboratori pratici su temi come il cyberbullismo, la privacy online e l'uso consapevole dei social network, utilizzando il **kit didattico** di Generazioni Connesse.
- **Percorsi di Peer Education**: coinvolgimento degli studenti in progetti di peer education, in cui diventano ambasciatori delle buone pratiche digitali all'interno della scuola e del territorio.

Azioni Formative per Docenti

- **Corsi di Formazione**: organizzazione di corsi di formazione sui temi dell'educazione civica digitale, con il supporto di esperti e risorse della piattaforma Generazioni Connesse.
- **Workshop e Seminari**: realizzazione di workshop e seminari per condividere buone pratiche e metodologie didattiche innovative, come il digital storytelling e il coding.

Azioni Formative per Famiglie

- **Incontri Informativi**: organizzazione di incontri periodici con esperti in educazione digitale, per sensibilizzare le famiglie sui rischi e le opportunità del mondo online.
- **Materiali Didattici**: pubblicazione di materiali informativi, come guide pratiche e video tutorial, per supportare i genitori nella gestione dell'uso delle tecnologie da parte dei figli.

Riferimenti Normativi e Obiettivi

Le azioni di sensibilizzazione e prevenzione del nostro Istituto sono in linea con la **Legge 92/2019** sull'educazione civica digitale e con le **Linee Guida del Miur** per la prevenzione del cyberbullismo. Gli obiettivi principali includono:

- **Breve Termine**: aumentare la consapevolezza sui rischi online e promuovere un uso responsabile delle tecnologie digitali.
- **Lungo Termine**: sviluppare competenze digitali trasversali e favorire una partecipazione attiva e responsabile nella rete.

Monitoraggio e Valutazione

Per garantire l'efficacia delle azioni intraprese, il nostro Istituto:

- **Raccoglie feedback** attraverso questionari anonimi rivolti a studenti, genitori e docenti.
- **Monitora i risultati** delle attività formative e dei progetti realizzati, utilizzando indicatori quantitativi e qualitativi.
- **Aggiorna l'ePolicy** in base alle nuove esigenze emerse e alle evoluzioni normative e tecnologiche.

2.2 - Il Curricolo Digitale

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

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

Al suo interno vengono identificati alcuni temi sui quali è costruita una proposta specifica per le famiglie e gli studenti

(formazione). Tale cornice trova poi sviluppo specifico, per gli studenti, nel curricolo di educazione alla Cittadinanza Digitale previsto dalla L. 92/2019. Il curricolo prende forma attorno all'ePolicy e le attività didattiche sono legate al documento ed alle scelte dell'Istituto al suo interno.

Nel curricolo va previsto in ogni classe un appuntamento didattico specifico, calibrato sull'età degli alunni, e l'utilizzo dei kit didattici per favorire da parte degli studenti una maggiore conoscenza e consapevolezza delle finalità del presente documento.

I regolamenti e le attività sviluppate sul tema della prevenzione presenti nell'ePolicy sono parte, costante ma non esclusiva, delle azioni di disseminazione e sensibilizzazione descritte ed attuate dall'Istituto.

Il Curricolo Digitale nel Nostro Istituto

Il nostro Istituto, che già da anni sperimenta l'insegnamento delle varie discipline attraverso il supporto di ausilii tecnologici, intende dotarsi di un **Curricolo Digitale** integrato, basato sul **Framework DigComp 2.2** e in linea con la **Legge 92/2019** sull'educazione civica digitale. Questo curricolo sarà progettato per garantire che tutti gli studenti acquisiscano le competenze necessarie per navigare in modo consapevole e responsabile nel mondo digitale. Di seguito, vengono descritte le scelte didattiche e le attività previste.

Struttura del Curricolo Digitale

Sviluppo di competenze avanzate, come la gestione della reputazione online, la creazione di contenuti digitali e la partecipazione attiva nella rete, con un focus sull'etica digitale e la sicurezza informatica.

Metodologie Didattiche

- **Apprendimento Basato su Progetti (PBL)**: realizzazione di progetti interdisciplinari che integrano le competenze digitali con altre materie, come la storia, la geografia e le scienze.
- **Flipped Classroom**: utilizzo di video-lezioni e risorse online per l'apprendimento autonomo, seguiti da attività pratiche in classe per consolidare le conoscenze.
- **Peer Education**: coinvolgimento degli studenti in attività di tutoraggio, in cui diventano insegnanti per i loro compagni su temi specifici della cittadinanza digitale.
- **Didattica orientativa**: realizzazione di percorsi di didattica orientativa che, attraverso il supporto di strumenti digitali e con l'affiancamento di docenti tutor per l'orientamento, possano consentire agli studenti la realizzazione di capolavori anche di natura digitale secondo quanto normato dalle Linee guida per l'orientamento.

Risorse e Strumenti

- **Kit Didattici**: utilizzo dei kit didattici di Generazioni Connesse per supportare le attività in classe e fornire materiali

pratici e coinvolgenti.

- **Piattaforme Digitali**: integrazione di piattaforme di apprendimento online, come Google Classroom e Moodle, per facilitare l'accesso alle risorse e la collaborazione tra studenti.

- **Laboratori Tecnologici**: organizzazione di laboratori di coding, robotica educativa e digital storytelling, per sviluppare competenze digitali avanzate in modo creativo e divertente anche con il ricorso, laddove previsti, a ulteriori finanziamenti di cui la scuola potrà essere beneficiaria.

Formazione per Docenti e Famiglie

- **Corsi di Formazione**: organizzazione di corsi di formazione per i docenti, basati sul Framework DigComp 2.2, per garantire che siano preparati a insegnare le competenze digitali in modo efficace.

- **Incontri per le Famiglie**: realizzazione di incontri informativi e workshop per le famiglie, per sensibilizzarle sui temi della cittadinanza digitale e supportarle nella gestione dell'uso delle tecnologie da parte dei figli.

Monitoraggio e Valutazione

- **Valutazione delle Competenze**: somministrazione di test, questionari e realizzazione di compiti di realtà autentici per valutare il livello di competenze digitali degli studenti e identificare eventuali aree di miglioramento.

- **Feedback Continuo**: raccolta di feedback da parte di studenti, docenti e famiglie, per monitorare l'efficacia del curricolo e apportare eventuali modifiche.

- **Aggiornamento Periodico**: revisione e aggiornamento del curricolo digitale in base alle nuove esigenze emerse e alle evoluzioni normative e tecnologiche.

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.

Utilizzo del Kit Didattico nel Nostro Istituto

Il nostro Istituto ha scelto di integrare il **Kit Didattico di Generazioni Connesse** come risorsa fondamentale per promuovere un uso consapevole e responsabile delle tecnologie digitali. Di seguito, vengono descritte le modalità con cui il Kit sarà utilizzato nelle diverse classi e le iniziative specifiche che abbiamo previsto.

Integrazione nel Curricolo

Sviluppo di competenze avanzate, come la critica agli algoritmi e la comprensione della datafication, con un focus sull'etica digitale e la sicurezza informatica.

Metodologie Didattiche

- **Apprendimento Basato su Problemi (PBL)**: utilizzo del Kit per affrontare problemi reali legati all'uso delle tecnologie, stimolando il pensiero critico e la collaborazione tra studenti.
- **Flipped Classroom**: impiego di video-lezioni e risorse online del Kit per l'apprendimento autonomo, seguiti da attività pratiche in classe per consolidare le conoscenze.
- **Peer Education**: coinvolgimento degli studenti in attività di tutoraggio, in cui diventano insegnanti per i loro compagni su temi specifici della cittadinanza digitale.

Formazione per Docenti

- **Workshop e Seminari**: organizzazione di workshop e seminari per formare i docenti sull'uso del Kit Didattico e sulle metodologie didattiche innovative.

Iniziative Specifiche

- **Giornate Tematiche**: organizzazione di giornate tematiche dedicate alla sicurezza online, con attività e laboratori basati sul Kit Didattico e partecipazione al Safer Internet Day.
- **Progetti Interdisciplinari**: realizzazione di progetti interdisciplinari che integrano le competenze digitali con le discipline curricolari.

- **Eventi per le Famiglie**: organizzazione di incontri informativi e workshop per le famiglie, per sensibilizzarle sui temi della cittadinanza digitale e supportarle nella gestione dell'uso delle tecnologie da parte dei figli.

Monitoraggio e Valutazione

- **Valutazione delle Competenze**: somministrazione di test e questionari e realizzazione di compiti di realtà autentici, individuali e/o di gruppo, per valutare il livello di competenze digitali degli studenti e identificare eventuali aree di miglioramento.

- **Feedback Continuo**: raccolta di feedback da parte di studenti, docenti e famiglie, per monitorare l'efficacia del Kit e apportare eventuali modifiche.

- **Aggiornamento Periodico**: revisione e aggiornamento delle attività basate sul Kit Didattico in base alle nuove esigenze emerse e alle evoluzioni normative e tecnologiche.

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.

Protezione dei Dati Personali e GDPR nel Nostro Istituto

Il nostro Istituto si impegna a garantire la massima protezione dei dati personali di studenti, docenti, famiglie e personale scolastico, in conformità al **Regolamento Generale sulla Protezione dei Dati (GDPR)** e al **Codice Privacy (Dlgs 196/2003)**. Di seguito, vengono descritte le misure e le procedure adottate per rispettare gli obblighi normativi e tutelare la privacy di tutti i membri della comunità educante.

Organigramma Privacy

- **Designazione del DPO**: il nostro Istituto ha nominato un **Responsabile della Protezione dei Dati (DPO)**, che svolge un ruolo chiave nel monitoraggio e nell'applicazione delle norme sulla privacy.

- **Formazione del Personale**: tutti i dipendenti dell'Istituto partecipano a corsi di formazione obbligatori sulla protezione dei dati e sul GDPR, per garantire una corretta gestione delle informazioni sensibili.

Informativa e Consenso

- **Informativa Chiara e Trasparente**: al momento della raccolta dei dati, viene fornita un'informativa dettagliata

sulle finalità del trattamento, i diritti degli interessati e le modalità di esercizio di tali diritti.

- **Consenso Informato**: per i trattamenti che richiedono il consenso, come l'uso di immagini per la disseminzazione delle attività didattiche, viene ottenuto un consenso esplicito e documentato da parte degli interessati o dei loro tutori legali.

Registro dei Trattamenti

- **Tenuta del Registro**: il nostro Istituto mantiene un **registro dei trattamenti** aggiornato, in cui sono elencate tutte le attività di trattamento dei dati personali, le finalità e le misure di sicurezza adottate.

- **Monitoraggio Continuo**: il registro viene revisionato periodicamente per garantire che tutte le attività siano conformi al GDPR e per identificare eventuali aree di miglioramento.

Misure di Sicurezza

- **Protezione delle Infrastrutture**: saranno implementate misure tecniche e organizzative per proteggere i dati personali, come l'uso di firewall, sistemi di crittografia e accessi protetti da password.

- **Gestione degli Accessi**: l'accesso ai dati personali è limitato al personale autorizzato, in base al principio del **minimo privilegio**.

- **Backup e Ripristino**: vengono effettuati backup regolari dei dati per prevenire perdite accidentali e garantire il ripristino in caso di incidenti.

Diritti degli Interessati

- **Esercizio dei Diritti**: gli interessati possono esercitare i propri diritti (accesso, rettifica, cancellazione, limitazione del trattamento, portabilità dei dati) attraverso un modulo dedicato disponibile sul sito web dell'Istituto.

- **Tempi di Risposta**: l'Istituto si impegna a rispondere alle richieste degli interessati entro i termini previsti dal GDPR (30 giorni).

Collaborazione con il Territorio

- **Partnership con Esperti**: il nostro Istituto collabora con esperti in protezione dei dati e avvocati specializzati in privacy per garantire un aggiornamento costante sulle normative e sulle migliori pratiche.

- **Coinvolgimento delle Famiglie**: vengono organizzati incontri informativi per le famiglie, per spiegare le misure adottate dall'Istituto e sensibilizzarle sull'importanza della protezione dei dati.

Monitoraggio e Valutazione

- **Audit Periodici**: vengono condotti audit interni per verificare la conformità alle norme sulla privacy e identificare eventuali criticità.

- **Feedback e Miglioramento**: i feedback raccolti da studenti, famiglie e personale vengono utilizzati per migliorare continuamente le procedure e le misure di sicurezza.

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.

Politica d'Uso Accettabile (PUA) nel Nostro Istituto

La **Politica d'Uso Accettabile (PUA)** del nostro Istituto è uno strumento fondamentale per garantire un uso sicuro, responsabile e consapevole della rete e delle tecnologie digitali da parte di studenti, docenti, personale scolastico e professionisti esterni. Di seguito, vengono descritte le regole, le iniziative e le modalità di applicazione della PUA nel nostro contesto scolastico.

Regole di Utilizzo della Rete

- **Accesso alla Rete**: l'accesso alla rete internet è consentito solo per scopi didattici e formativi. È vietato l'uso per attività personali, come giochi online, social network non autorizzati o download di materiale non pertinente.

- **Protezione della Privacy**: è proibito condividere dati personali propri o altrui senza autorizzazione, violare la privacy di compagni o docenti, o pubblicare immagini e video senza consenso.

- **Rispetto del Copyright**: gli studenti e il personale sono tenuti a rispettare i diritti d'autore, evitando di scaricare o condividere materiale protetto da copyright senza autorizzazione.

- **Comportamento Etico**: sono vietati comportamenti illeciti o inappropriati, come il cyberbullismo, l'adescamento online o la diffusione di contenuti offensivi o discriminatori.

Modalità di Applicazione

- **Filtri di Navigazione**: sono stati implementati filtri per bloccare l'accesso a siti non appropriati o potenzialmente pericolosi, garantendo una navigazione sicura per studenti e personale.

- **Monitoraggio Attivo**: l'uso della rete è monitorato per identificare eventuali violazioni della PUA e intervenire tempestivamente.

- **Sanzioni e Misure Disciplinari**: in caso di violazione delle regole, sono previste sanzioni disciplinari proporzionate alla gravità dell'infrazione, che vanno dal richiamo verbale alla sospensione dell'accesso alla rete.

Iniziative di Sensibilizzazione

- **Formazione per Studenti**: organizzazione di laboratori e attività didattiche per insegnare agli studenti a navigare in modo sicuro e responsabile, utilizzando esempi pratici e casi reali.

- **Incontri per le Famiglie**: auspicabile la realizzazione di incontri informativi per spiegare ai genitori le regole della PUA e fornire consigli su come supportare i figli nell'uso della rete.

- **Campagne di Comunicazione**: diffusione di materiali informativi, come poster, brochure e video, per promuovere un uso positivo della rete e sensibilizzare sui rischi online.

Integrazione con il Documento Programmatico sulla Sicurezza (DPS)

La PUA è integrata con il **Documento Programmatico sulla Sicurezza (DPS)**, che definisce le misure tecniche e organizzative per garantire la sicurezza delle informazioni e dei dati personali. In particolare:

- **Protezione delle Infrastrutture**: sono state implementate misure di sicurezza avanzate, come firewall, sistemi di crittografia e accessi protetti da password.

- **Gestione degli Incidenti**: è in fase di definizione un protocollo per la gestione degli incidenti di sicurezza, che prevede la segnalazione tempestiva e l'intervento del team di sicurezza.

Coinvolgimento della Comunità Educante

- **Docenti e Personale**: i docenti e il personale della comunità educante, durante l'anno scolastico, saranno formati sull'uso responsabile della rete e sulle regole della PUA, per garantire un'applicazione coerente e uniforme.
- **Studenti**: gli studenti saranno coinvolti in progetti di peer education, in cui diventano ambasciatori delle buone pratiche digitali all'interno della scuola.
- **Famiglie**: le famiglie sono invitate a partecipare attivamente alle iniziative di sensibilizzazione e a collaborare con la scuola per promuovere un uso consapevole della rete.

Monitoraggio e Valutazione

- **Feedback Continuo**: vengono raccolti feedback da parte di studenti, docenti e famiglie per valutare l'efficacia della PUA e identificare eventuali aree di miglioramento.
- **Aggiornamento Periodico**: la PUA viene revisionata e aggiornata periodicamente, in base alle nuove esigenze emerse e alle evoluzioni normative e tecnologiche.

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.

Regolamentazione BYOD nel Nostro Istituto

Il nostro Istituto riconosce il potenziale didattico dei dispositivi personali (BYOD, "Bring Your Own Device") e ha adottato una **regolamentazione specifica** per garantirne un uso responsabile, sicuro e finalizzato all'apprendimento. Di seguito, vengono descritte le regole, le modalità di applicazione e le iniziative previste per integrare i dispositivi personali nella didattica.

Regole per l'Uso dei Dispositivi Personali

- **Autorizzazione all'Uso**: l'uso dei dispositivi personali in classe è consentito solo previa autorizzazione del docente e per scopi didattici specifici, come la ricerca online, la partecipazione a piattaforme di apprendimento o la realizzazione di progetti digitali.
- **Connessione alla Rete**: i dispositivi personali possono connettersi solo alla rete Wi-Fi dedicata agli studenti, protetta da filtri di navigazione e monitorata per garantire la sicurezza.
- **Responsabilità dello Studente**: gli studenti sono responsabili della custodia e del corretto utilizzo dei propri dispositivi. La scuola non risponde di eventuali danni, furti o smarrimenti.
- **Divieti**: è vietato l'uso dei dispositivi per attività non autorizzate, come giochi, social network non pertinenti o la registrazione di audio e video senza consenso.

Modalità di Applicazione

- **Registro delle Autorizzazioni**: i docenti tengono un registro delle autorizzazioni concesse per l'uso dei dispositivi personali, specificando le attività didattiche per cui sono stati utilizzati.
- **Monitoraggio Attivo**: l'uso dei dispositivi è monitorato per garantire il rispetto delle regole e intervenire tempestivamente in caso di violazioni.
- **Sanzioni**: in caso di uso improprio dei dispositivi, sono previste sanzioni disciplinari proporzionate alla gravità dell'infrazione, che vanno dal richiamo verbale alla sospensione temporanea del privilegio BYOD.

Iniziative di Sensibilizzazione

- **Formazione per Studenti**: organizzazione di laboratori e attività didattiche per insegnare agli studenti a utilizzare i dispositivi personali in modo sicuro e responsabile, con un focus sulla privacy, la sicurezza online e il rispetto delle regole.
- **Incontri per le Famiglie**: realizzazione di incontri informativi per spiegare ai genitori le regole del BYOD e fornire consigli su come supportare i figli nell'uso responsabile dei dispositivi.
- **Campagne di Comunicazione**: diffusione di materiali informativi, come poster, brochure e video, per promuovere un uso positivo dei dispositivi personali e sensibilizzare sui rischi associati.

Integrazione con la Didattica

- **Progetti Digitali**: i dispositivi personali sono utilizzati per realizzare progetti interdisciplinari, come ricerche online, presentazioni multimediali e attività di coding.
- **Piattaforme di Apprendimento**: gli studenti accedono a piattaforme di apprendimento online, come Google Classroom o Moodle, per svolgere compiti, partecipare a discussioni e collaborare con i compagni.
- **Metodologie Innovative**: i docenti integrano i dispositivi personali in metodologie didattiche innovative, come il flipped classroom, il project-based learning e il digital storytelling.

Coinvolgimento della Comunità Educante

- **Docenti**: i docenti sono formati sull'uso didattico dei dispositivi personali e sulle regole del BYOD, per garantire un'applicazione coerente e uniforme.
- **Studenti**: gli studenti sono coinvolti in progetti di peer education, in cui diventano ambasciatori delle buone pratiche digitali all'interno della scuola.
- **Famiglie**: le famiglie sono invitate a partecipare attivamente alle iniziative di sensibilizzazione e a collaborare con la scuola per promuovere un uso consapevole dei dispositivi personali.

Monitoraggio e Valutazione

- **Feedback Continuo**: vengono raccolti feedback da parte di studenti, docenti e famiglie per valutare l'efficacia della regolamentazione BYOD e identificare eventuali aree di miglioramento.
- **Aggiornamento Periodico**: la regolamentazione BYOD viene revisionata e aggiornata periodicamente, in base alle nuove esigenze emerse e alle evoluzioni normative e tecnologiche.

Cap 4 - Segnalazione e gestione dei casi

4.1 - Cosa Segnalare

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire). Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Queste, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola.

Nelle procedure sono indicate le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso, nonché le modalità di coinvolgimento del Dirigente Scolastico e del Referente per il contrasto al bullismo e al cyberbullismo. Inoltre, la scuola individua le figure che costituiranno un team preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica. La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

A seguire, le problematiche a cui fanno riferimento le procedure allegate:

Cyberbullismo: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).

Adescamento online: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

Sexting: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere, per quanto possibile, la rimozione del materiale on-line e il blocco della sua diffusione per mezzo dei dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete.

Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;
- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

Procedure di Segnalazione e Gestione dei Casi nel Nostro Istituto

Il nostro Istituto ha adottato **procedure chiare e standardizzate** per la segnalazione e la gestione dei casi legati a comportamenti online a rischio, come il cyberbullismo, l'adescamento online e il sexting. Di seguito, vengono descritte le modalità operative, le figure coinvolte e le iniziative per garantire un intervento tempestivo ed efficace.

Figure Preposte alla Segnalazione

- **Referente per il Cyberbullismo**: è la figura di riferimento per la gestione delle segnalazioni e il coordinamento delle azioni di intervento. Collabora con il Dirigente Scolastico e il Team Antibullismo per garantire una risposta rapida e appropriata.

- **Team Antibullismo**: composto da docenti, personale ATA e, se necessario, da psicologi o esperti esterni, il team si occupa della presa in carico dei casi e della definizione delle strategie di intervento.

- **Docenti e Personale Scolastico**: tutti i docenti e il personale sono formati per riconoscere i segnali di disagio e per accogliere le segnalazioni degli studenti, garantendo un approccio empatico e riservato.

Modalità di Segnalazione

- **Canali di Segnalazione**: gli studenti e le famiglie possono segnalare episodi di cyberbullismo, adescamento online o sexting attraverso:
    - Un **modulo online** disponibile sul sito web dell'Istituto.
    - Una **cassetta delle segnalazioni** posizionata in un'area accessibile ma discreta della scuola.
    - Un colloquio diretto con il Referente per il Cyberbullismo o un docente di fiducia.

- **Linguaggio Child/Youth Friendly**: le procedure di segnalazione sono presentate in un linguaggio semplice e accessibile, con esempi pratici e istruzioni chiare, per facilitare la comprensione da parte degli studenti.

Gestione dei Casi

- **Valutazione Iniziale**: il Referente per il Cyberbullismo e il Team Antibullismo valutano la gravità della situazione, raccolgono informazioni e identificano le figure coinvolte (vittima, autore, testimoni) secondo quantom in maniera molto chiara emerge dal Codice Interno per la prevenzione del bullismo e del cyberbullismo di cui la scuola si è dotata.
- **Intervento Immediato**: in caso di emergenza, viene attivato un protocollo di intervento rapido, che può includere il supporto psicologico, la mediazione tra le parti e la segnalazione alle autorità competenti.
- **Coinvolgimento delle Famiglie**: le famiglie delle parti coinvolte sono informate tempestivamente e coinvolte nel processo di risoluzione del caso, nel rispetto della privacy e della riservatezza.
- **Collaborazione con il Territorio**: per situazioni particolarmente complesse, l'Istituto si avvale della collaborazione di enti esterni, come le Forze dell'Ordine, i servizi sociali e le associazioni specializzate.

Iniziative di Prevenzione e Sensibilizzazione

- **Formazione per Studenti**: organizzazione di laboratori e attività didattiche per insegnare agli studenti a riconoscere i comportamenti online a rischio e a segnalarli tempestivamente.
- **Incontri per le Famiglie**: realizzazione di incontri informativi per spiegare ai genitori come riconoscere i segnali di disagio e supportare i figli in caso di problemi online.
- **Campagne di Comunicazione**: diffusione di materiali informativi, come poster, brochure e video, per promuovere un uso positivo della rete e sensibilizzare sui rischi associati.

Monitoraggio e Valutazione

- **Registro delle Segnalazioni**: viene tenuto un registro dettagliato di tutte le segnalazioni ricevute, delle azioni intraprese e degli esiti, per garantire trasparenza e tracciabilità.
- **Feedback Continuo**: vengono raccolti feedback da parte di studenti, docenti e famiglie per valutare l'efficacia delle procedure e identificare eventuali aree di miglioramento.
- **Aggiornamento Periodico**: le procedure di segnalazione e gestione dei casi vengono revisionate e aggiornate periodicamente, in base alle nuove esigenze emerse e alle evoluzioni normative e tecnologiche.

Servizi di Supporto

Il nostro Istituto collabora con i seguenti servizi per garantire un supporto completo e professionale:

- **Helpline 19696 e Chat di Telefono Azzurro**: per supporto ed emergenze legate a situazioni di disagio online.
- **Clicca e Segnala di Telefono Azzurro e STOP-IT di Save the Children**: 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 minorenne.

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

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

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

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

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

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

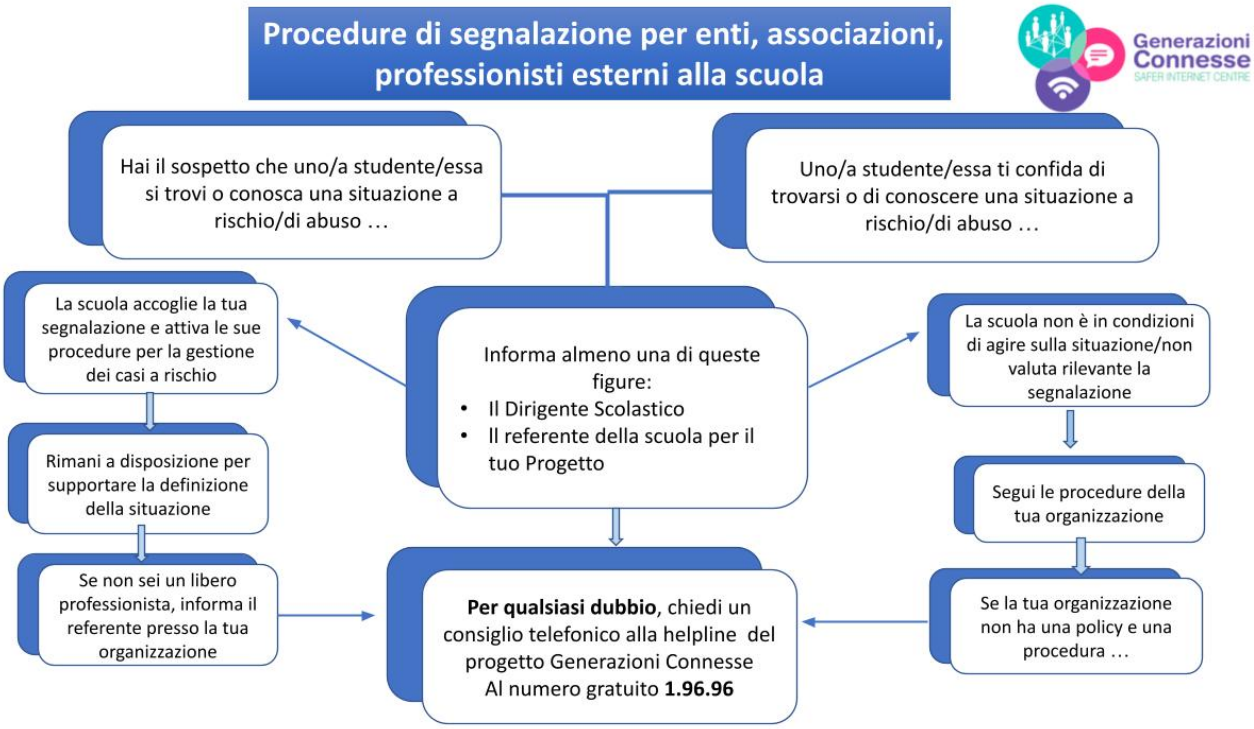
Strumenti a disposizione di studenti/esse

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

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

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

Procedure



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

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

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

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

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

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

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo

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

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

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

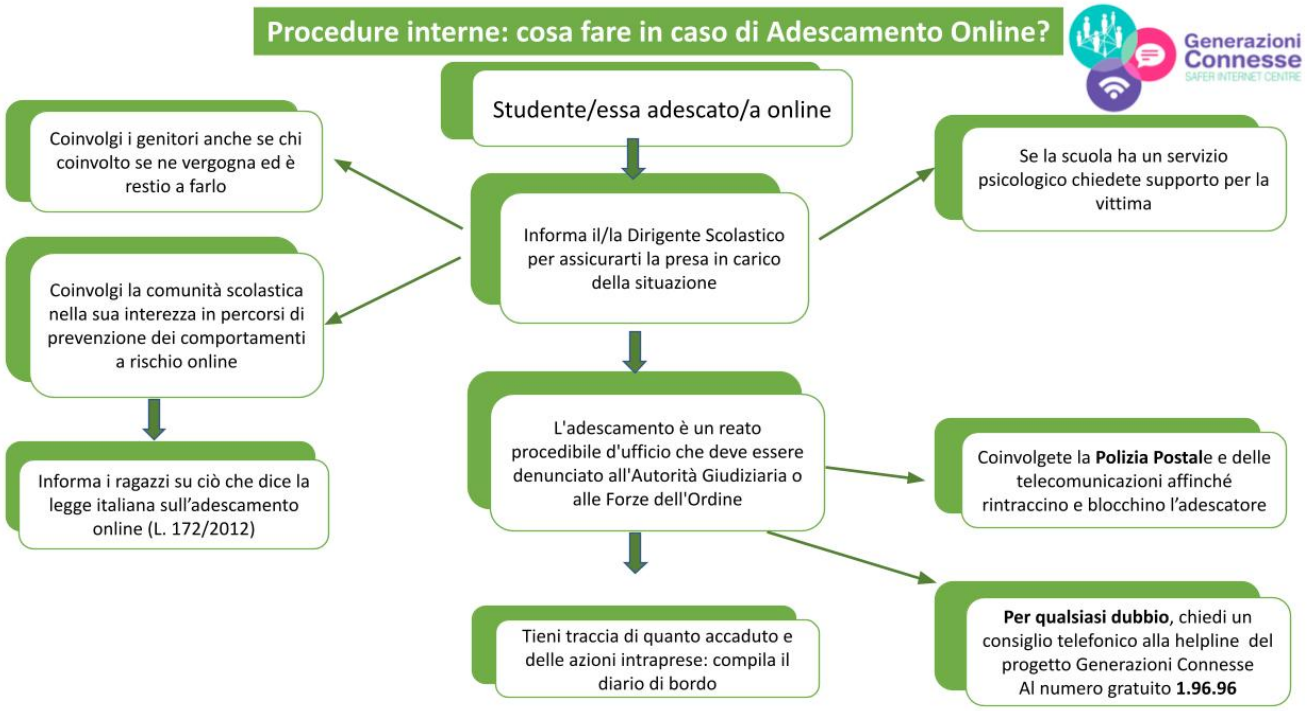
Se emergono evidenze passa allo schema successivo

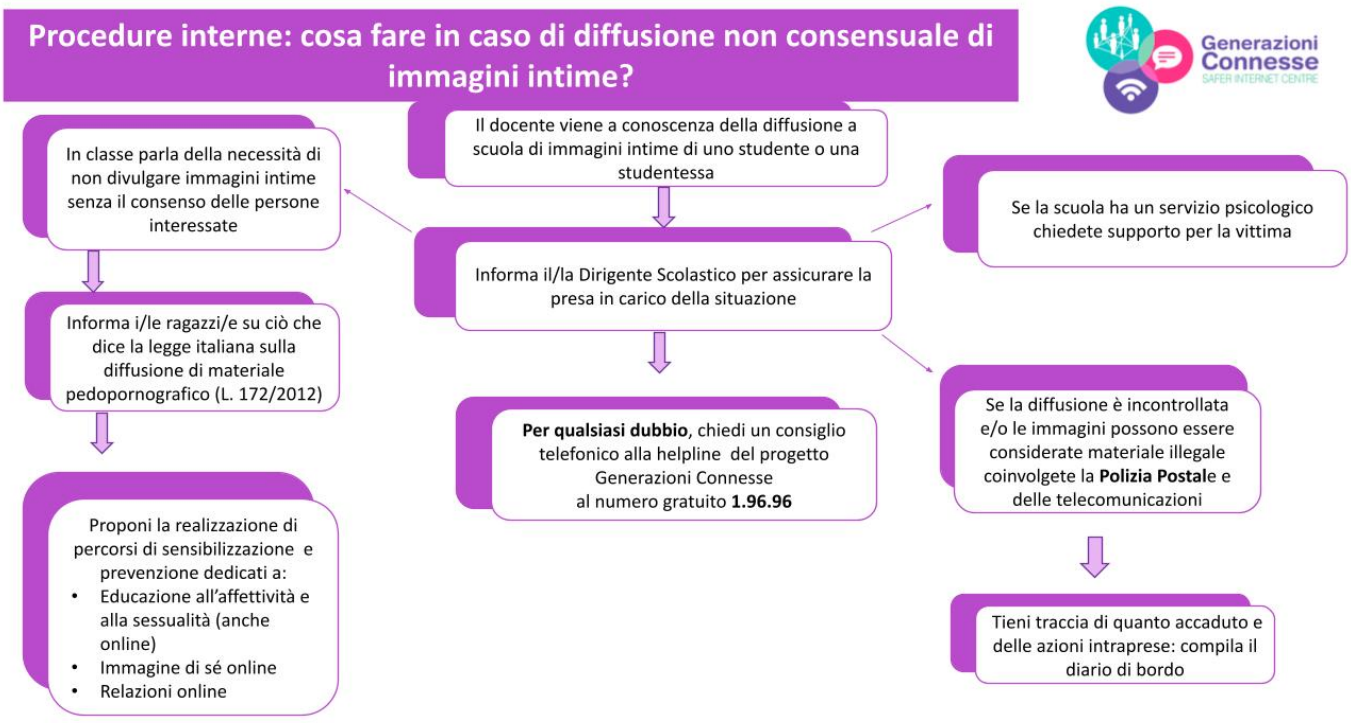
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

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

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

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





Strumenti e Procedure di Segnalazione nel Nostro Istituto

Il nostro Istituto ha adottato **strumenti e procedure chiare** per facilitare la segnalazione di comportamenti online a rischio, come il cyberbullismo, l'adescamento online e il sexting. Di seguito, vengono descritte le modalità operative, le

figure coinvolte e le iniziative per garantire un intervento tempestivo ed efficace.

Strumenti di Segnalazione

- **Indirizzo E-mail Dedicato**: è stato creato un indirizzo e-mail specifico (es. segnalazioni@scuola.it) per ricevere segnalazioni da parte di studenti, genitori e docenti. Le segnalazioni vengono gestite in modo riservato e tempestivo.
- **Cassetta delle Segnalazioni**: è stata posizionata una cassetta delle segnalazioni in un'area accessibile ma discreta della scuola, per permettere agli studenti di segnalare episodi in modo anonimo.
- **Sportello di Ascolto**: la scuola si impegna a creare uno sportello di ascolto gestito da psicologi e professionisti, disponibile per studenti e famiglie che necessitano di supporto o consulenza.

Figure Preposte alla Gestione delle Segnalazioni

- **Referente per il Cyberbullismo**: è la figura di riferimento per la gestione delle segnalazioni e il coordinamento delle azioni di intervento. Collabora con il Dirigente Scolastico e il Team Antibullismo per garantire una risposta rapida e appropriata.
- **Team Antibullismo**: composto da docenti, personale ATA e, se necessario, da psicologi o esperti esterni, il team si occupa della presa in carico dei casi e della definizione delle strategie di intervento.
- **Docenti e Personale Scolastico**: tutti i docenti e il personale sono formati per riconoscere i segnali di disagio e per accogliere le segnalazioni degli studenti, garantendo un approccio empatico e riservato.

Procedure di Gestione dei Casi

- **CASO A (SOSPETTO)**: quando un docente o un membro del personale sospetta un episodio di cyberbullismo, adescamento online o sexting, deve inoltrare una **comunicazione scritta** al Referente per il Cyberbullismo e al Team Antibullismo. La comunicazione deve essere dettagliata e oggettiva. Il team valuta la situazione e decide se avviare percorsi di sensibilizzazione o coinvolgere le autorità competenti.
- **CASO B (EVIDENZA)**: in caso di evidenza certa di un episodio, il Referente e il Team Antibullismo allertano immediatamente il Dirigente Scolastico e avviano una **valutazione approfondita**. Se il caso ha rilevanza penale, viene attivata la procedura giudiziaria con denuncia all'autorità competente (Procura Ordinaria o Minorile).

Collaborazione con le Autorità Competenti

- **Procura Ordinaria**: nel caso in cui il presunto autore del reato sia maggiorenne, la segnalazione viene inoltrata alla Procura Ordinaria.
- **Procura Minorile**: se il presunto autore è minorenne, la segnalazione viene inviata alla Procura Minorile.
- **Segnalazione Obbligatoria**: in caso di situazioni di grave pregiudizio per i minori, l'Istituto è tenuto alla segnalazione obbligatoria alle autorità competenti, come previsto dalla Legge 216/1991.

Supporto Psicologico e Mediazione

- **Colloqui Individuali**: vengono attivati colloqui individuali con le vittime, i testimoni e gli autori degli episodi, per valutare il loro stato emotivo e fornire supporto psicologico.
- **Mediazione**: in casi appropriati, vengono organizzati incontri di mediazione tra le parti coinvolte, con il coinvolgimento dei genitori e la supervisione di professionisti.
- **Coinvolgimento delle Famiglie**: le famiglie delle parti coinvolte sono informate tempestivamente e coinvolte nel processo di risoluzione del caso, nel rispetto della privacy e della riservatezza.

Iniziative di Prevenzione e Sensibilizzazione

- **Formazione per Studenti**: organizzazione di laboratori e attività didattiche per insegnare agli studenti a riconoscere i comportamenti online a rischio e a segnalarli tempestivamente.
- **Incontri per le Famiglie**: realizzazione di incontri informativi per spiegare ai genitori come riconoscere i segnali di disagio e supportare i figli in caso di problemi online.
- **Campagne di Comunicazione**: diffusione di materiali informativi, come poster, brochure e video, per promuovere un uso positivo della rete e sensibilizzare sui rischi associati.

Monitoraggio e Valutazione

- **Registro delle Segnalazioni**: viene tenuto un registro dettagliato di tutte le segnalazioni ricevute, delle azioni intraprese e degli esiti, per garantire trasparenza e tracciabilità.
- **Feedback Continuo**: vengono raccolti feedback da parte di studenti, docenti e famiglie per valutare l'efficacia delle

procedure e identificare eventuali aree di miglioramento.

- **Aggiornamento Periodico**: le procedure di segnalazione e gestione dei casi vengono revisionate e aggiornate periodicamente, in base alle nuove esigenze emerse e alle evoluzioni normative e tecnologiche.

MILENA SIRACUSA
28.05.2025 12:19:30
CEST