

Documento di ePolicy

GIORGI - WOOLF

VIALE P. TOGLIATTI 1161 - 00155 - ROMA

Roma (RM) - Lazio

Data di approvazione: 10/07/2026 - 18:19

Cap 1 - Lo scopo della ePolicy

1.1 Scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

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

Capitolo 2 - Sensibilizzazione e prevenzione

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

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

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

Capitolo 4 - Segnalazione e gestione dei casi

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

1.1 Scopo dell'ePolicy

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

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

La competenza digitale è una competenza chiave del cittadino europeo come indicato dal Consiglio Europeo

(Raccomandazione del 2018) che permette ad ogni cittadino di esercitare i propri diritti all'interno degli ambienti digitali (ONU - [Commento Generale 25](#): I diritti dei minori negli ambienti digitali).

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

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

Attraverso l'E-policy, il nostro Istituto si dota di uno strumento operativo e di riferimento per l'intera comunità educante, volto ad assicurare un approccio alle tecnologie che sia consapevole, critico ed efficace. Il documento definisce le linee guida per promuovere il benessere in Rete, regolamentare l'utilizzo delle TIC (Tecnologie dell'Informazione e della Comunicazione) a scuola e porre le basi per azioni continue di formazione, educazione e sensibilizzazione.

Oggi gli studenti vivono immersi in un ecosistema virtuale in cui operano nella doppia veste di fruitori e creatori di contenuti. Pur essendo nativi digitali, necessitano di una guida adulta e autorevole per sviluppare un atteggiamento vigile e responsabile verso le risorse e i rischi del web. La cittadinanza digitale ci impone, infatti, di accrescere e consolidare le competenze necessarie per muoversi nella complessità dei nuovi sistemi comunicativi. Per questo motivo, l'E-policy valorizza l'uso sicuro e creativo della rete, delineando al contempo rigorose politiche preventive e di sensibilizzazione per contrastare i comportamenti a rischio.

In questo scenario in rapida evoluzione, l'E-policy del nostro Istituto accoglie e regola l'introduzione dei sistemi di Intelligenza Artificiale (IA) nella didattica e nella quotidianità scolastica. L'IA rappresenta una straordinaria opportunità per personalizzare l'apprendimento, stimolare la creatività e supportare lo studio; tuttavia, richiede un livello superiore di responsabilità e senso critico.

Il nostro Istituto si impegna a guidare gli studenti nel comprendere non solo le potenzialità algoritmiche, ma anche i rischi connessi all'IA, quali il plagio automatizzato, la diffusione di *deepfake*, la dipendenza da risposte preconfezionate e la tutela della privacy e dei dati personali. L'obiettivo è formare cittadini digitali capaci di utilizzare l'IA come un amplificatore dell'intelligenza umana e del pensiero critico, e non come un suo sostituto, garantendo un uso etico, trasparente e sicuro di queste nuove tecnologie all'interno della comunità scolastica.

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

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

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

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

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

IL DIRIGENTE SCOLASTICO

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

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

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

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

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

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

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

In coerenza con le Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo del Ministero

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

Il Team ha il compito di:

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

I/LE DOCENTI

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

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

RESPONSABILE DELLA PROTEZIONE DEI DATI

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

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

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

GLI STUDENTI E LE STUDENTESSE

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

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

I GENITORI/ADULTI DI RIFERIMENTO

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

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

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

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

L'Istituto ha definito, all'interno della propria organizzazione, una chiara articolazione di **ruoli e responsabilità**, individuando specifiche figure di riferimento al fine di garantire un sistema efficace e coordinato di prevenzione e informazione sull'uso consapevole delle TIC e delle tecnologie emergenti, quali l'IA.

Il Dirigente Scolastico

Il Dirigente Scolastico detiene la responsabilità di garantire la sicurezza e il benessere di tutta la comunità scolastica, estendendo tale tutela anche alla dimensione digitale e agli ambienti di apprendimento virtuali. Nell'esercizio di tali funzioni, e coadiuvato dal DPO (Data Protection Officer) per gli aspetti legati alla conformità e alla tutela dei dati personali, il Dirigente Scolastico assolve ai seguenti compiti:

- **Promozione della cultura digitale e della sicurezza:** Promuove e garantisce l'attivazione di percorsi formativi sistematici rivolti a studenti, docenti e personale ATA sull'uso consapevole delle TIC. Tale azione viene sviluppata in

sinergia con il Referente per il contrasto al Bullismo e al Cyberbullismo e con l'Animatore Digitale, al fine di sensibilizzare la comunità scolastica sui rischi della rete e sulle relative misure di prevenzione.

- **Funzione regolativa e disciplinare:** Regola l'utilizzo dei dispositivi e delle tecnologie all'interno dell'Istituto, applicando le sanzioni disciplinari previste dal Regolamento d'Istituto e dallo Statuto delle studentesse e degli studenti in caso di condotte scorrette o uso improprio delle risorse tecnologiche.
- **Gestione degli episodi di disagio e dei comportamenti a rischio:** Nei casi in cui venga a conoscenza di comportamenti digitali a rischio o di episodi di bullismo e cyberbullismo che non integrino gli estremi di un reato, provvede a informare tempestivamente le famiglie dei minori coinvolti. Contribuisce, inoltre, a pianificare e favorire interventi socio-educativi mirati all'interno dei singoli gruppi classe e dei Consigli di classe interessati.
- **Governance e indirizzo etico dell'Intelligenza Artificiale (IA):** Definisce le linee di indirizzo strategico per l'introduzione e l'utilizzo dei sistemi di Intelligenza Artificiale nella didattica e nella gestione amministrativa. Promuove la formazione specifica del personale sull'uso etico dell'IA, ne monitora l'impatto sull'autonomia di studio degli alunni e ne vigila l'impiego per prevenire violazioni della proprietà intellettuale (plagio automatizzato) o rischi connessi al trattamento dei dati personali attraverso algoritmi esterni.

Il Direttore dei Servizi Generali e Amministrativi (DSGA)

Il Direttore dei Servizi Generali e Amministrativi (DSGA) sovrintende ai servizi amministrativi, contabili e generali dell'Istituzione Scolastica, curando la corretta gestione delle risorse finanziarie e del personale ATA, in stretta sinergia con gli indirizzi del Dirigente Scolastico. Nell'ambito dell'E-policy, assolve ai seguenti compiti:

- **Gestione finanziaria e manutenzione del patrimonio tecnologico:** Assicura, nei limiti delle risorse iscritte nel Programma Annuale e dei finanziamenti disponibili, la manutenzione ordinaria e straordinaria delle infrastrutture informatiche, dei server, della rete dell'Istituto e dei dispositivi in dotazione. Tale azione è finalizzata a garantire la continuità del servizio, l'efficienza delle misure di sicurezza digitale e la protezione da usi impropri o non autorizzati delle attrezzature.
- **Organizzazione del personale e supporto ai laboratori:** Garantisce, compatibilmente con l'organico di fatto e i vincoli di bilancio, l'efficiente allocazione e la presenza del personale ATA di supporto (con particolare riferimento agli Assistenti Tecnici e Collaboratori Scolastici) all'interno dei laboratori didattici e dei locali multimediali, al fine di assicurarne la corretta vigilanza e la funzionalità operativa.

Il Responsabile della Protezione dei Dati (DPO - Data Protection Officer)

Il DPO (Data Protection Officer / Responsabile della Protezione dei Dati) è la figura di consulenza specialistica e di vigilanza che assicura la conformità dell'Istituzione Scolastica alle normative vigenti in materia di privacy, con particolare riferimento al Regolamento Europeo (GDPR 2016/679) e al Codice in materia di protezione dei dati personali. Nell'ambito dell'E-policy e dell'uso delle TIC, il DPO assolve ai seguenti compiti:

- **Consulenza e vigilanza sul trattamento dei dati:** Offre supporto e consulenza tecnica al Dirigente Scolastico (Titolare del trattamento) nella gestione, archiviazione e tutela dei dati personali di tutta la comunità scolastica (studenti, famiglie, personale docente e ATA), vigilando sulla corretta applicazione delle misure di sicurezza informatiche e organizzative.

- **Valutazione dell'impatto tecnologico (DPIA):** Conduce analisi preventive sui rischi legati all'introduzione di nuove piattaforme didattiche, registri elettronici, software gestionali o servizi cloud, al fine di garantire che l'uso delle TIC non leda i diritti e le libertà fondamentali degli interessati.
- **Gestione delle violazioni e dei diritti:** Interviene tempestivamente in caso di violazioni della sicurezza dei dati (*data breach*) all'interno dell'ambiente digitale scolastico, supportando l'Istituto nelle comunicazioni all'Autorità Garante e ai soggetti coinvolti, e gestisce le istanze relative all'esercizio dei diritti sulla privacy.
- **Valutazione etica e conformità dei sistemi di Intelligenza Artificiale (IA):** Effettua la valutazione d'impatto e di conformità sui software e sulle piattaforme di IA adottate dall'Istituto per finalità didattiche o amministrative. Verifica che l'inserimento di dati, elaborati o informazioni personali all'interno di tali sistemi non comporti la profilazione indebita degli studenti, la cessione di dati a terzi o la violazione della privacy algoritmica, garantendo che i sistemi utilizzati rispettino il principio di trasparenza e i diritti di proprietà intellettuale.

L'Animatore Digitale

L'Animatore Digitale è la figura di sistema deputata a favorire il processo di digitalizzazione dell'Istituto, coordinando la diffusione dell'innovazione metodologica e tecnologica all'interno della comunità scolastica, in coerenza con le linee guida del Piano Nazionale Scuola Digitale (PNSD). Nell'ambito dell'E-policy, assolve ai seguenti compiti:

- **Supporto tecnico-metodologico al personale:** Offre consulenza e supporto continuo a tutto il personale scolastico (docente e ATA) nell'utilizzo efficace delle TIC, promuovendo lo sviluppo delle competenze digitali e l'integrazione delle tecnologie nella didattica quotidiana e nei processi organizzativi.
- **Presidio della sicurezza e monitoraggio dell'infrastruttura:** Collabora con le figure tecniche preposte per garantire la sicurezza interna della rete d'Istituto, definendo i protocolli di accesso e monitorando l'ambiente digitale scolastico per rilevare tempestivamente anomalie o problematiche emergenti legate all'uso insicuro di Internet e delle TIC.
- **Ricerca e diffusione di soluzioni innovative:** Promuove la sperimentazione e l'adozione di metodologie didattiche d'avanguardia e di strumenti tecnologici innovativi, curandone la diffusione e l'efficace trasferimento di competenze all'interno dell'intero corpo docente.
- **Gestione del patrimonio tecnologico:** Sovrintende, in coordinamento con l'ufficio tecnico e il DSGA, all'aggiornamento costante e alla manutenzione delle componenti hardware e software in dotazione all'Istituto, assicurando l'efficienza dei laboratori, delle aule multimediali e dei dispositivi di rete.
- **Integrazione e sperimentazione dell'Intelligenza Artificiale (IA) nella didattica:** Promuove e coordina l'introduzione sperimentale di strumenti di IA generativa e assistenti virtuali a supporto dell'insegnamento. Si occupa di selezionare le piattaforme di IA didattica più idonee, di formare il corpo docente sul *prompt engineering* (la formulazione efficace di istruzioni per i modelli linguistici) e sulla progettazione di lezioni che educino gli studenti a verificare le fonti, contrastando le allucinazioni algoritmiche e stimolando il pensiero critico.

La Funzione Strumentale per l'Innovazione Tecnologica e Didattica

La Funzione Strumentale per l'Innovazione Tecnologica e Didattica opera come figura di raccordo strategico e operativo

all'interno del Collegio dei Docenti, finalizzata a ottimizzare l'uso degli ambienti digitali d'apprendimento e a tradurre le risorse tecnologiche in opportunità metodologiche. Nell'ambito dell'E-policy, assolve ai seguenti compiti:

- **Formazione e sviluppo delle competenze sulla piattaforma d'Istituto:** Promuove, coordina e realizza attività di formazione e supporto continuo rivolte al corpo docente per l'utilizzo avanzato e l'ottimizzazione delle funzionalità della piattaforma istituzionale (es. ecosistema Microsoft 365 o equivalenti), standardizzando i flussi di lavoro didattici e comunicativi.
- **Coordinamento normativo e organizzativo della DDI:** Cura la redazione, l'aggiornamento e il monitoraggio del *Regolamento per la Didattica Digitale Integrata (DDI)*, assicurando la coerenza del documento con le evoluzioni normative ministeriali e con le specifiche esigenze dell'Istituzione Scolastica.
- **Sicurezza, Compliance e Policy di utilizzo:** Predispone i protocolli comportamentali, i regolamenti d'accesso e le misure operative necessarie a garantire la sicurezza informatica e la tutela della privacy all'interno della piattaforma d'Istituto, lavorando in stretta sinergia con il Titolare del trattamento (DS) e con il DPO.
- **Definizione dei codici di comportamento (Netiquette):** Elabora e diffonde il documento sulla *Netiquette* interna, definendo le regole di condotta, i canali ufficiali e le buone prassi comunicative digitali a cui devono attenersi tutti i membri della comunità scolastica (docenti, studenti, famiglie).
- **Definizione delle linee guida e della Netiquette per l'uso dell'Intelligenza Artificiale (IA):** Integra la *netiquette* d'Istituto e i regolamenti digitali con una sezione specifica sull'uso etico e corretto dell'IA generativa e dei software di ausilio allo studio. Si occupa di definire le linee guida per gli studenti sul corretto utilizzo dei modelli linguistici (esplicitando il divieto di plagio e l'obbligo di citazione dell'IA come fonte).

Il Referente per il contrasto al Bullismo e al Cyberbullismo

Il Referente per il contrasto al Bullismo e al Cyberbullismo è la figura di sistema incaricata di coordinare le azioni di prevenzione, monitoraggio e contrasto dei fenomeni di disagio relazionale e d'illegalità digitale all'interno dell'Istituto. Operando in stretta sinergia con la Presidenza, lo staff di direzione e le agenzie educative del territorio, assolve ai seguenti compiti:

- **Coordinamento e promozione delle iniziative di prevenzione:** Promuove e coordina i progetti, le campagne di sensibilizzazione e le iniziative didattiche finalizzate al contrasto del bullismo, del cyberbullismo e alla promozione della cittadinanza digitale, supportando i Consigli di classe nella pianificazione di interventi mirati.
- **Formazione del personale scolastico:** Progetta e dirige percorsi formativi e di aggiornamento periodico rivolti al personale docente e ATA, fornendo gli strumenti pedagogici, giuridici e informatici necessari per riconoscere tempestivamente i segnali di disagio e gestire correttamente le dinamiche di inclusione ed esclusione nei gruppi classe.
- **Presidio, vigilanza e segnalazione d'emergenza:** Monitora la vita scolastica e le segnalazioni provenienti dalla comunità educante, provvedendo a informare con massima tempestività il Dirigente Scolastico in merito a situazioni a rischio online, condotte digitali inappropriate o episodi conclamati di bullismo e cyberbullismo.
- **Rete interistituzionale e alleanze territoriali:** Cura i rapporti e coordina le iniziative di prevenzione e legalità

attivate in sinergia con soggetti esterni, quali le Forze di Polizia (es. Polizia Postale), le autorità sanitarie, i servizi sociali, le associazioni di settore e i centri di aggregazione giovanile presenti sul territorio.

- **Supporto e orientamento alle famiglie e agli studenti:** Offre un punto di primo ascolto e orientamento per gli studenti e le studentesse vittime o autori di comportamenti vessatori, nonché per i loro genitori, indirizzandoli tempestivamente e supportandoli nell'accesso allo sportello di ascolto psicologico o ad altri servizi specialistici attivati dall'Istituto.

I Docenti

I docenti dell'Istituto sono i primi garanti dell'efficacia pedagogica dell'E-policy, operando quotidianamente come mediatori tra gli studenti e le tecnologie digitali per trasformare la Rete in un ambiente di apprendimento sicuro e inclusivo. Nell'ambito delle loro funzioni, i docenti si impegnano a:

- **Formazione e aggiornamento continuo:** Partecipare attivamente ai percorsi di formazione e aggiornamento, promossi dall'Istituto o da enti accreditati, sull'uso metodologico delle TIC, sull'ottimizzazione delle funzionalità della piattaforma d'Istituto (es. Microsoft 365) e sulla sicurezza informatica, approfondendo gli aspetti etici, legali e di tutela del diritto d'autore (*copyright*) legati al digitale.
- **Guida e orientamento degli studenti:** Supportare gli alunni e le alunne nello sviluppo di un approccio critico, consapevole e creativo alla Rete e alle tecnologie multimediali utilizzate per scopi didattici, educandoli alla valutazione delle fonti e alla corretta gestione dell'identità digitale.
- **Tutela della privacy e riservatezza dei dati:** Rispettare rigorosamente l'obbligo di riservatezza e i protocolli sul trattamento dei dati personali (sensibili e non) di cui vengono a conoscenza nell'esercizio delle proprie funzioni, operando in piena conformità con il Regolamento Europeo sulla Privacy (GDPR 2016/679) e con la normativa nazionale vigente.
- **Vigilanza comportamentale e segnalazione istituzionale:** Monitorare la condotta degli studenti negli ambienti digitali scolastici e segnalare tempestivamente al Dirigente Scolastico, o ai suoi collaboratori, eventuali violazioni dei regolamenti e delle norme di comportamento stabilite dall'Istituzione Scolastica.
- **Prevenzione del disagio e dei fenomeni vessatori:** Rilevare tempestivamente le dinamiche relazionali anomale all'interno del gruppo classe e comunicare con immediatezza al Coordinatore di classe e al Referente per il contrasto al Bullismo e al Cyberbullismo qualsiasi sospetto o episodio conclamato di vessazione, sia essa fisica o virtuale.
- **Integrazione metodologica e vigilanza etica sull'Intelligenza Artificiale (IA):** Integrare l'uso dei sistemi di IA generativa all'interno dei percorsi didattici in modo mirato, educando gli studenti a considerare l'IA come uno strumento di supporto alla ricerca e non come un sostituto del pensiero autonomo. Si impegnano a promuovere il principio dell'onestà intellettuale, guidando la classe a citare in modo trasparente l'eventuale utilizzo di assistenti algoritmici nei propri elaborati e a verificarne criticamente l'attendibilità per contrastare il fenomeno delle informazioni false o distorte.

Il Personale A.T.A. (Amministrativo, Tecnico e Ausiliario)

Il Personale ATA concorre, nell'ambito delle specifiche competenze professionali e mansioni, a garantire la sicurezza,

l'efficienza e la corretta tenuta degli ambienti fisici e digitali dell'Istituzione Scolastica. Nell'ambito dell'E-policy, è tenuto ad assolvere ai seguenti compiti:

- **Consapevolezza e conformità sulla sicurezza informatica:** Acquisire e mantenere una piena consapevolezza in merito alle problematiche della sicurezza digitale, alle disposizioni dell'E-policy d'Istituto e alle buone pratiche per la protezione dei dati, applicandole rigorosamente nella gestione quotidiana dei flussi di lavoro, delle postazioni informatiche e delle credenziali d'accesso istituzionali.
- **Vigilanza ambientale e segnalazione delle violazioni:** Monitorare, per quanto di propria competenza e durante il regolare svolgimento del servizio nei vari plessi, l'utilizzo dei dispositivi e dei laboratori. Il personale si impegna a segnalare tempestivamente al Dirigente Scolastico, o ai suoi collaboratori, qualsiasi abuso, anomalia tecnica, comportamento scorretto online o tentativo di violazione dei sistemi informatici dell'Istituto.
- **Supporto tecnico e operativo (Profilo Assistenti Tecnici):** Collaborare attivamente con l'Animatore Digitale e la Funzione Strumentale per garantire il corretto funzionamento hardware e software dei laboratori e dei dispositivi mobili, applicando i filtri di navigazione e i sistemi di protezione necessari a tutelare i minori da contenuti inappropriati.
- **Gestione sicura dei dati e transizione digitale (Profilo Assistenti Amministrativi):** Assicurare la massima riservatezza nella gestione dei dati sensibili degli utenti attraverso il protocollo informatico, il registro elettronico e le piattaforme ministeriali, evitando la dispersione di credenziali e l'accesso non autorizzato ai terminali della segreteria.

Gli Studenti e le Studentesse

Gli studenti e le studentesse sono i protagonisti attivi della vita scolastica digitale e sono chiamati a esercitare i propri diritti di cittadinanza in Rete con responsabilità, etica e rispetto del benessere altrui. Nell'ambito dell'E-policy dell'Istituto, si impegnano a:

- **Conoscenza delle norme comunitarie:** Prendere visione e rispettare il Regolamento d'Istituto e le disposizioni digitali adottate dalla scuola, interiorizzandone il valore per una convivenza civile e democratica sia all'interno delle aule sia negli spazi virtuali.
- **Uso responsabile delle tecnologie e rispetto della didattica:** Utilizzare i dispositivi tecnologici personali (es. smartphone) e d'Istituto esclusivamente per scopi didattici, uniformandosi rigorosamente alle indicazioni dei docenti e astenendosi da utilizzi impropri o fonte di distrazione durante le ore di lezione.
- **Sviluppo del pensiero critico e verifica delle fonti:** Imparare a valutare criticamente le informazioni presenti sul web, distinguendo, grazie alla guida dei docenti, le fonti attendibili dalle notizie false o manipolate, al fine di sviluppare una conoscenza autonoma e oggettiva.
- **Consapevolezza dei rischi e tutela della privacy:** Maturare una chiara consapevolezza dei rischi della Rete, impegnandosi a non diffondere informazioni riservate, notizie false, video o immagini senza l'esplicito consenso delle persone coinvolte, rispettando il diritto alla riservatezza, all'immagine e alla dignità di ciascuno.
- **Contrasto al bullismo e legalità digitale:** Riconoscere la gravità dei fenomeni di bullismo e cyberbullismo e

astenersi da qualsiasi comportamento vessatorio online. Gli studenti sono consapevoli che condotte lesive dell'incolumità psicofisica altrui costituiscono gravi violazioni del Regolamento d'Istituto e del Patto di Corresponsabilità e che, nei casi più gravi, configurano reati perseguibili dalla Magistratura minorile.

Gli Ambasciatori di Internet (Peer Educators per la Cittadinanza Digitale)

Gli "Ambasciatori di Internet" costituiscono un gruppo selezionato di studenti e studentesse che, attraverso una metodologia di educazione tra pari (*peer education*), opera come presidio attivo di cittadinanza digitale all'interno dell'Istituto. Previa frequenza di percorsi di formazione specialistica, questo gruppo d'avanguardia assolve ai seguenti compiti:

- **Formazione avanzata e continua:** Partecipare a percorsi formativi specifici, coordinati dall'Animatore Digitale e dai Referenti d'Istituto, incentrati sull'uso sicuro, critico e consapevole della Rete, sulla tutela della privacy, sulle dinamiche dei social media e sulle nuove frontiere dell'Intelligenza Artificiale.
- **Divulgazione e sensibilizzazione tra pari (Peer Education):** Progettare e realizzare interventi informativi e formativi rivolti alle altre classi dell'Istituto, traducendo le competenze acquisite in un linguaggio accessibile e vicino alla sensibilità dei propri coetanei.
- **Sviluppo di risorse digitali informative:** Ideare e curare la creazione di strumenti digitali divulgativi, quali siti web tematici, blog d'istituto, infografiche e vademecum digitali, finalizzati a diffondere le buone pratiche della navigazione e della convivenza online.
- **Produzione di contenuti multimediali ed eventi:** Realizzare presentazioni efficaci, podcast o brevi video-esplicativi da utilizzare durante le assemblee di istituto, le ore di Educazione Civica o eventi tematici (es. il *Safer Internet Day*), promuovendo attivamente la cultura della legalità online.
- **Promozione dell'uso etico e della cultura dell'Intelligenza Artificiale (IA):** Operare come promotori della cultura dell'IA all'interno della scuola, mostrando concretamente ai propri compagni come utilizzare i modelli generativi in modo etico per lo studio e la creatività. Si occupano inoltre di sensibilizzare i coetanei sui rischi dei *deepfake*, dei bias algoritmici e della disinformazione automatizzata, aiutando la comunità studentesca a sviluppare lo spirito critico necessario per interagire con le tecnologie del futuro.

I Genitori

I genitori e i titolari della responsabilità genitoriale svolgono un ruolo primario e insostituibile nel garantire che gli studenti e le studentesse maturino una piena consapevolezza sulla necessità di un utilizzo sicuro, etico e appropriato dei dispositivi digitali e della Rete. Nell'ottica di un'alleanza educativa scuola-famiglia, i genitori prendono visione dell'E-policy d'Istituto e si impegnano a:

- **Corresponsabilità e collaborazione con l'Istituzione Scolastica:** Sostenere l'azione pedagogica dei docenti e collaborare attivamente alle iniziative formative promosse dall'Istituto, condividendo le linee guida sull'uso consapevole, critico e sicuro delle TIC.
- **Sensibilizzazione e dialogo educativo in famiglia:** Contribuire all'educazione digitale dei propri figli all'interno delle mura domestiche, dialogando apertamente sui rischi connessi alla navigazione (quali l'adescamento online, l'esposizione a contenuti inappropriati e la dipendenza da schermo) e promuovendo il rispetto della privacy altrui.

- **Prevenzione e contrasto dei comportamenti scorretti:** Cooperare tempestivamente con il corpo docente e la dirigenza per intercettare, scoraggiare e contrastare ogni forma di utilizzo non responsabile, offensivo o pericoloso delle tecnologie (comprese le chat di classe e i social network), arginando sul nascere dinamiche di cyberbullismo o di esclusione.
- **Vigilanza e sicurezza nell'ambiente domestico:** Incoraggiare l'uso delle TIC come prezioso strumento di studio per lo svolgimento dei compiti a casa, vigilando affinché la fruizione dei dispositivi digitali in ambito domestico avvenga in totale sicurezza, adottando se necessario adeguati sistemi di filtro (*parental control*) e concordando tempi di utilizzo equilibrati.

Gli Enti Educativi Esterni e le Associazioni

Gli Enti del Terzo Settore, le associazioni, gli esperti esterni e le agenzie educative che, a vario titolo, collaborano con l'Istituzione Scolastica o realizzano progetti all'interno dell'Istituto (es. FSL ex-PCTO, laboratori e seminari di orientamento, progetti di inclusione), concorrono a preservare l'integrità dell'ambiente di apprendimento digitale. Nell'ambito delle attività concordate, essi si impegnano a:

- **Conformità alle policy e ai regolamenti d'Istituto:** Conoscere e rispettare rigorosamente le politiche interne dell'Istituto, le disposizioni dell'E-policy e i regolamenti relativi all'uso consapevole delle TIC, della rete Wi-Fi scolastica e dei dispositivi multimediali concessi in uso.
- **Tutela dei minori e presidio della sicurezza:** Garantire l'adozione di comportamenti e protocolli operativi improntati alla massima sicurezza e alla protezione integrale delle studentesse e degli studenti durante lo svolgimento delle attività progettuali, vigilando affinché l'interazione con gli strumenti digitali non esponga i minori a rischi informatici o relazionali.
- **Riservatezza, copyright e tutela dell'immagine:** Rispettare i vincoli di riservatezza e i protocolli d'Istituto relativi alla privacy dei minori, astenendosi dal raccogliere, registrare o diffondere immagini, video o dati personali degli studenti senza le preventive e formali autorizzazioni sottoscritte dalle famiglie e autorizzate dal Dirigente Scolastico.

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.

L'E-policy non costituisce un documento isolato, bensì un pilastro programmatico strutturalmente interconnesso con l'intera architettura regolamentare dell'Istituzione Scolastica. Si sottolinea che tutti i documenti sotto menzionati, inclusa la presente E-policy, sono ufficialmente pubblicati sul sito web istituzionale della scuola, garantendo la massima trasparenza e la piena accessibilità per la consultazione da parte delle famiglie, degli studenti e di tutto il personale scolastico.

L'E-policy si integra e si coordina in perfetta sinergia con i seguenti documenti ufficiali:

- **Il Regolamento d'Istituto:** Di cui l'E-policy rappresenta l'estensione operativa per la dimensione digitale, definendo i diritti, i doveri e le sanzioni legati all'uso delle tecnologie.
- **Il Piano Triennale dell'Offerta Formativa (PTOF):** Nel quale si inserisce come scelta strategica e metodologica per l'innovazione didattica, la transizione digitale e il successo formativo degli studenti.
- **Il Curricolo d'Istituto di Educazione Civica:** All'interno del quale l'E-policy declina gli obiettivi di apprendimento e le competenze chiave afferenti al nucleo concettuale della "Cittadinanza Digitale".
- **Il Regolamento e la Netiquette della Piattaforma d'Istituto:** Il protocollo comportamentale specifico adottato per l'ecosistema digitale d'Istituto (es. Microsoft 365), finalizzato a disciplinare, tracciare e mettere in sicurezza i flussi comunicativi ufficiali e le interazioni digitali tra tutte le componenti della comunità scolastica: *docenti-docenti, docenti-studenti, docenti-famiglie ed enti esterni*.
- **Il Regolamento Disciplinare d'Istituto:** Con il quale l'E-policy si raccorda in modo vincolante per la definizione e l'applicazione delle sanzioni disciplinari. Questo documento qualifica la gravità delle infrazioni commesse negli ambienti digitali o attraverso l'uso improprio delle TIC e dell'Intelligenza Artificiale (es. atti di cyberbullismo, violazione della privacy, alterazione di documenti digitali, plagio algoritmico), ricalibrando i provvedimenti sanzionatori in chiave formativa e riparatoria, in conformità con lo Statuto delle studentesse e degli studenti.

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

1. il curriculum sulle competenze digitali per la comunità educante (il DigComp2.2);
2. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative;
3. Come comunicare e condividere l'ePolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

1. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative;

L'efficacia dell'ePolicy è direttamente proporzionale a livello di conoscenza e diffusione all'interno della comunità scolastica ivi comprese le famiglie. Il documento rappresenta il canale interno privilegiato per informare, responsabilizzare e collaborare sui temi della rete e delle tecnologie a scuola con l'intera comunità scolastica.

In tal senso, il documento è accompagnato da versioni, allegate e sintetiche, all'interno delle quali sono individuati gli elementi principali del documento; una versione è diretta agli studenti ed una è diretta alle famiglie con un linguaggio e una presentazione dei contenuti adeguata, flessibile e chiara. La versione sintetica rivolta agli studenti è inserita all'interno delle attività didattiche dell'educazione alla cittadinanza mentre la versione per le famiglie è consegnata nel corso dei colloqui scuola-famiglia.

Il documento è altresì pubblicato sul sito della scuola ed inserito nel Patto di corresponsabilità.

2. Come comunicare e condividere l'ePolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

La presenza dell'ePolicy nell'Istituto scolastico è garanzia, per il territorio, della presenza di un presidio informato, sensibile e attento sulla rete e le tecnologie in relazione con i più giovani.

In questo senso l'Istituto può rappresentare per le Istituzioni del territorio, le aziende, e le realtà del Terzo Settore un luogo di confronto privilegiato e di sperimentazione per tutti coloro che intendono costruire progetti di cittadinanza digitale rivolte ai più giovani.

A tal fine l'adozione dell'ePolicy è comunicata all'USR di riferimento e al Municipio (servizi istruzione e servizi sociali) attraverso gli allegati sintetici progettati che indicano gli elementi del documento e le prospettive per la comunità.

Al fine di garantire la massima trasparenza e favorire l'effettiva interiorizzazione delle regole di condotta digitale, l'E-policy viene ufficialmente condivisa, comunicata e resa vincolante per tutta la comunità scolastica attraverso i seguenti canali istituzionali:

- **Approvazione e formalizzazione degli Organi Collegiali:** Il documento viene preventivamente sottoposto al vaglio, all'approvazione e alla delibera del Collegio dei Docenti e del Consiglio d'Istituto, acquisendo pieno valore legale e regolamentare.
- **Pubblicazione e pubblicità legale:** Il testo integrale viene pubblicato sul sito web istituzionale dell'Istituto

all'interno dell'apposita sezione documentale e diffuso capillarmente a tutto il personale, alle famiglie e agli studenti tramite circolare interna e sulla piattaforma ufficiale d'Istituto (Microsoft Teams). Trova inoltre spazio all'interno del giornalino scolastico per incentivarne la lettura partecipata.

- **Integrazione con il Patto di Corresponsabilità Educativa:** L'adesione ai principi dell'E-policy viene sancita formalmente all'inizio di ciascun anno scolastico attraverso la sottoscrizione, da parte delle famiglie e degli studenti, del *Patto di Corresponsabilità Educativa*, consolidando l'alleanza tra scuola e casa.
- **Affissione e comunicazione visiva negli ambienti scolastici:** Una versione sintetica e visuale del regolamento (estratto infografico) viene esposta in modo visibile nei vari plessi dell'Istituto e, in particolar modo, all'interno dei laboratori informatici, delle aule multimediali e in tutti gli spazi dotati di postazioni connesse alla Rete.
- **Informazione sul monitoraggio e supporto alla navigazione:** Gli studenti e le studentesse vengono esplicitamente e preventivamente informati dai docenti circa la presenza di sistemi di protezione e monitoraggio della navigazione online attivi all'interno della rete scolastica. Tale presidio viene presentato non in chiave punitiva, bensì come strumento di tutela, volto a supportarli nell'acquisizione delle corrette regole di condotta in Rete e a garantire una navigazione protetta e assistita.

1.5 - I Piani di Azione dell'ePolicy

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

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

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

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

1° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

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

MODULO II

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

MODULO III

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

MODULO IV

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

2° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

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

MODULO II

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

Di seguito si delineano le azioni strategiche, i regolamenti da implementare e gli eventi formativi programmati per l'Anno Scolastico 2026/2027 e per il successivo triennio di validità del documento.

Le Novità dell'Anno Scolastico 2026/2027 (Azioni Prioritarie)

- **Costituzione del Gruppo "Ambasciatori di Internet":** Istituzione e formazione di un nucleo selezionato di

studenti operanti come *peer educators* sui temi della cittadinanza digitale, della sicurezza online e dell'uso etico dell'IA.

- **Aggiornamento Regolamentare (*Netiquette* e IA):** Redazione, approvazione e pubblicazione dei nuovi protocolli di comportamento online, con la differenziazione tra la *Netiquette* d'Istituto standard e le linee guida specifiche per l'utilizzo dell'Intelligenza Artificiale Generativa (*Netiquette IA*).
- **Campagna di Lancio:** Realizzazione di eventi mirati di formazione e sensibilizzazione degli studenti sull'E-policy e sulle implicazioni didattiche, etiche e legali connesse all'uso delle TIC e dei sistemi di IA.

Pianificazione degli Eventi e delle Attività nel Triennio di Validità

Al fine di garantire la piena efficacia dell'E-policy, nel corso del triennio verranno attivati percorsi formativi, laboratoriali e di monitoraggio declinati per le diverse componenti della comunità scolastica.

1. Azioni Rivolte al Corpo Docente e al Personale Scolastico

- **Presentazione dell'E-policy:** Organizzazione di un evento informativo iniziale volto a illustrare i contenuti, le procedure e le linee guida del documento di E-policy.
- **Formazione sulle TIC e sulla Cybersecurity:** Promozione di incontri di aggiornamento sull'integrazione didattica delle TIC e sull'uso sicuro delle tecnologie (cybersecurity).
- **Incontri con Esperti del Settore:** Organizzazione di seminari informativi per la prevenzione dei rischi digitali emergenti, con il supporto di specialisti esterni.
- **Formazione sulla Protezione dei Dati:** Attivazione di moduli formativi sulla tutela della privacy e sulla gestione dei dati personali all'interno delle piattaforme scolastiche, con la partecipazione diretta del DPO.

2. Azioni Rivolte alle Studentesse e agli Studenti

- **Consultazione Attiva e Focus Group:** Organizzazione di incontri di ascolto con gli studenti per raccogliere bisogni e mappare i comportamenti in Rete che necessitano di una regolamentazione stringente.
- **Analisi sull'Uso dei Dispositivi:** Conduzione di un'indagine statistica interna (survey) sull'utilizzo dei dispositivi digitali personali (*BYOD - Bring Your Own Device*) all'interno dell'ambiente scolastico.
- **Formazione su Cybersecurity e Rischi Online:** Attivazione di incontri di sensibilizzazione incentrati sull'accesso sicuro a Internet, la difesa dalle truffe digitali e la gestione consapevole della propria identità virtuale.
- **Laboratori di Educazione Civica Digitale:** Promozione di percorsi laboratoriali stabili inseriti nel curriculum di Educazione Civica, con particolare attenzione all'etica digitale e alla verifica delle fontes.
- **Laboratori di Affettività e Sessualità:** Realizzazione di interventi formativi mirati a esplorare la dimensione

dell'affettività e della sessualità anche in rapporto ai media digitali (prevenzione di dinamiche quali *sexting*, molestie online e distorsione dell'immagine corporea).

- **Laboratori sul Contrasto alla Violenza di Genere:** Attivazione di percorsi specifici e laboratori dedicati alla prevenzione e al contrasto della violenza di genere, volti a scardinare stereotipi e a promuovere la cultura del consenso, del rispetto e dell'uguaglianza. Gli interventi affronteranno in modo mirato anche le manifestazioni digitali di tale fenomeno, quali il cyber-stalking, il controllo ossessivo tramite smartphone e la diffusione non consensuale di materiale intimo (*revenge porn*).

3. Azioni Rivolte ai Genitori e alle Famiglie

- **Presentazione Istituzionale:** Organizzazione di un evento dedicato per illustrare alle famiglie l'E-policy d'Istituto e favorire la firma consapevole del Patto di Corresponsabilità.

Adeguamenti Normativi e Strumenti di Comunicazione (Spazio Web)

Per dare esecuzione formale al piano e garantire gli obblighi di trasparenza, si procederà alle seguenti azioni strutturali sul portale d'Istituto e sui regolamenti vigenti:

- **Armonizzazione dei Testi:** Integrazione formale del *Regolamento d'Istituto* alla luce delle nuove disposizioni introdotte dall'E-policy.
- **Pubblicità Legalità dell'E-policy:** Pubblicazione in primo piano del documento definitivo sul sito web istituzionale.
- **Sportello e Segnalazione Bullismo/Cyberbullismo:** Creazione e pubblicazione sul sito di un'area dedicata contenente la modulistica ufficiale scaricabile per la segnalazione di episodi di bullismo e cyberbullismo.
- **Contatto Diretto:** Pubblicazione permanente sul portale scolastico dell'indirizzo email istituzionale riservato al *Referente d'Istituto per il contrasto al Bullismo e al Cyberbullismo*, al fine di agevolare le segnalazioni tempestive da parte di famiglie e studenti.

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](#)

Nell'ambito delle azioni di promozione della cittadinanza digitale e della sicurezza online, l'Istituto intende predisporre **un'apposita area dedicata all'interno del sito istituzionale**, nella quale saranno raccolti e resi facilmente accessibili i collegamenti alle principali risorse del progetto **Generazioni Connesse**, iniziativa di riferimento a livello nazionale per l'educazione all'uso consapevole e responsabile delle tecnologie digitali.

Tra gli strumenti principali disponibili si segnalano:

- il **Kit Didattico**, costituito da materiali strutturati e modulabili, finalizzati a supportare l'attività didattica e a favorire lo sviluppo delle competenze digitali e civiche degli/delle studenti/sse;
- l'**Area Formazione**, dedicata a docenti, famiglie e studenti/sse, che include percorsi formativi articolati e integrati con la piattaforma ePolicy, finalizzati alla costruzione di una cultura condivisa della sicurezza in rete;
- il **Canale YouTube**, che ospita webinar, video-stimolo e serie tematiche differenziate per target, utili per l'approfondimento e l'aggiornamento continuo;
- i canali social ufficiali (**TikTok, Instagram e Facebook**), che rappresentano strumenti di comunicazione e sensibilizzazione, in grado di raggiungere in modo diretto e immediato le diverse componenti della comunità educante.

In tale contesto, la **Commissione ePolicy** svolge un ruolo strategico di coordinamento, promozione e diffusione delle iniziative connesse all'educazione digitale all'interno dell'Istituzione scolastica.

In particolare, la Commissione è incaricata di:

- curare la **diffusione, mediante apposite comunicazioni ufficiali (circolari)**, delle opportunità formative promosse da Generazioni Connesse, assicurando un'informazione puntuale e sistematica rivolta a tutto il personale scolastico, al fine di favorire la partecipazione ai percorsi di aggiornamento e formazione;
- garantire l'**informazione ai Consigli di classe** in merito a progetti, iniziative e concorsi promossi dal medesimo programma, promuovendone l'integrazione nella progettazione didattica e nei percorsi educativi, in coerenza con gli obiettivi dell'educazione civica digitale.

Attraverso tali azioni, la Commissione contribuisce a rafforzare l'adozione di pratiche educative consapevoli e inclusive, favorendo la costruzione di un ambiente digitale sicuro, responsabile e partecipato, in linea con le indicazioni nazionali ed europee in materia.

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.

A partire dall'anno scolastico 2020/2021, i Docenti dell'Istituto hanno elaborato un **curricolo verticale di Educazione civica**, in coerenza con la Legge n. 92 del 20 agosto 2019 e con le Linee guida emanate con il D.M. n. 35 del 22 giugno 2020. Tale impianto curricolare ha introdotto l'insegnamento trasversale dell'Educazione civica, integrando i nuclei fondanti **Costituzione, Sviluppo sostenibile e Cittadinanza digitale**, con particolare attenzione alle dimensioni di **sensibilizzazione e prevenzione** nell'uso delle tecnologie.

Nell'ambito delle **TIC, di Internet e dell'Intelligenza Artificiale**, la competenza digitale si configura come insieme articolato di conoscenze, abilità e atteggiamenti finalizzati a un utilizzo consapevole, critico e responsabile degli strumenti digitali, favorendo processi di apprendimento, comunicazione, collaborazione e partecipazione attiva alla vita sociale.

In tale prospettiva, l'Istituto promuove azioni sistematiche rivolte all'intera comunità educante, articolate come segue.

STUDENTI E STUDENTESSE

Per gli studenti e le studentesse, le attività sono orientate prioritariamente alla **sensibilizzazione** e alla **prevenzione dei rischi connessi all'ambiente digitale**, attraverso:

- lo sviluppo dell'**alfabetizzazione digitale, mediatica e informativa**, con particolare riferimento alla comprensione critica dei contenuti online e generati anche mediante sistemi di Intelligenza Artificiale;
- la promozione di comportamenti responsabili nell'uso di Internet e dei social network, nel rispetto delle regole di **netiquette** e della convivenza civile;
- la conoscenza delle problematiche connesse alla **protezione dei dati personali**, alla privacy, al cyberbullismo, alla disinformazione e all'uso improprio delle tecnologie;
- l'educazione al **rispetto del copyright e delle proprietà intellettuali**, anche in relazione ai contenuti digitali e ai prodotti generati mediante strumenti di IA;
- la realizzazione, al termine di ciascun anno scolastico, di **prodotti e attività significative**, coerenti con il curricolo di Educazione civica, finalizzati a rendere evidenti le competenze maturate in uscita.

DOCENTI E PERSONALE ATA

Il personale docente e il personale ATA svolgono un ruolo fondamentale nella costruzione di un ambiente digitale sicuro e inclusivo. In tale ottica, l'Istituto promuove:

- il **rafforzamento delle competenze digitali e metodologiche dei docenti**, affinché le TIC e le tecnologie emergenti, inclusa l'Intelligenza Artificiale, siano integrate in modo consapevole nella didattica;
- la capacità di **progettare, gestire e valutare** processi di insegnamento-apprendimento mediati dalle tecnologie, con attenzione all'inclusione e al supporto degli studenti con bisogni educativi speciali;
- percorsi di **formazione e aggiornamento continuo**, sia interni sia esterni, finalizzati all'uso efficace e sicuro delle tecnologie digitali;
- il supporto tecnico-organizzativo del personale ATA, quale componente essenziale per il corretto funzionamento delle infrastrutture digitali e per la tutela dei dati trattati;
- la diffusione di una cultura della **prevenzione dei rischi digitali**, anche in relazione all'uso improprio degli strumenti tecnologici in ambito scolastico.

A tal fine, l'Istituto ha implementato dotazioni tecnologiche, tra cui le **Digital Board**, favorendo l'accesso diffuso ai contenuti digitali e l'innovazione metodologica.

FAMIGLIE

Le famiglie rappresentano un interlocutore imprescindibile nel processo educativo e nella promozione di un uso consapevole delle tecnologie. L'Istituto:

- coinvolge le famiglie attraverso il **Patto di corresponsabilità educativa**, quale strumento di condivisione di principi, regole e comportamenti per la prevenzione dei rischi digitali;
- rende disponibili sul sito istituzionale informazioni e risorse utili, al fine di sostenere un'azione educativa coerente tra scuola e contesto familiare.

Attraverso tali azioni integrate, l'Istituto si impegna a promuovere una **cultura digitale consapevole, critica e responsabile**, orientata alla prevenzione dei rischi e alla valorizzazione delle opportunità offerte dalle TIC, da Internet e dall'Intelligenza Artificiale, in linea con il quadro normativo nazionale ed europeo.

2.2 - Il Curricolo Digitale

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

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

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

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

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

Il nostro Istituto, caratterizzato dalla presenza di una pluralità di indirizzi di studio, riconosce il curriculum digitale come elemento strutturale e trasversale della progettazione didattica, in coerenza con il quadro normativo nazionale ed europeo e con gli obiettivi dell'Educazione civica digitale.

In particolare, l'insegnamento delle discipline informatiche è previsto come obbligatorio nel primo biennio per i diversi indirizzi dell'Istituto, al fine di garantire a tutti gli studenti e le studentesse una base comune di competenze digitali, orientate non solo all'utilizzo tecnico degli strumenti, ma anche alla consapevolezza critica e alla prevenzione dei rischi connessi all'uso delle tecnologie.

Gli indirizzi Liceo Scientifico – opzione Scienze Applicate, Istituto Tecnico Tecnologico Ambientale – Informatica, Grafica e Comunicazione, Automazione e Meccatronica integrano nei rispettivi percorsi curriculari l'uso delle TIC, di Internet e delle tecnologie emergenti, inclusa l'Intelligenza Artificiale, promuovendo lo sviluppo di competenze avanzate in ambito digitale, comunicativo e tecnico-scientifico.

Tali percorsi prevedono:

- l'acquisizione di competenze nell'uso consapevole degli strumenti digitali e dei sistemi informatici;
- lo sviluppo del pensiero computazionale e delle capacità di problem solving;
- l'utilizzo critico delle fonti digitali e dei contenuti online, anche in relazione ai sistemi di Intelligenza Artificiale;
- la sensibilizzazione rispetto ai temi della sicurezza informatica, della protezione dei dati e della prevenzione dei rischi digitali;
- la produzione di contenuti digitali, nel rispetto delle normative vigenti in materia di copyright e proprietà intellettuale.

Per quanto riguarda gli indirizzi del triennio professionale "Made in Italy – Industria e Artigianato (Moda)" e dell'Istituto Tecnico Tecnologico – Elettronica, l'Istituto prevede, nel corso del triennio, la progressiva definizione e strutturazione di un curriculum digitale specifico, finalizzato allo sviluppo di competenze coerenti con i profili in uscita e con le esigenze dei settori produttivi di riferimento.

Tale percorso sarà orientato a:

- integrare le competenze digitali nei processi professionali e laboratoriali di settore;
- promuovere un uso consapevole delle tecnologie digitali e degli strumenti innovativi nei contesti produttivi;
- sviluppare competenze legate alla progettazione, gestione e comunicazione digitale dei prodotti;
- rafforzare le capacità di utilizzo critico e responsabile delle tecnologie, anche in relazione all'evoluzione dell'Intelligenza Artificiale nei contesti professionali.

Attraverso la definizione e l'implementazione del curriculum digitale, l'Istituto si impegna a garantire una formazione completa e aggiornata, capace di coniugare competenze tecniche, consapevolezza critica e responsabilità nell'uso delle tecnologie, in un'ottica di sensibilizzazione e prevenzione e in linea con le trasformazioni della società digitale contemporanea.

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.

Nell'ambito delle azioni di sensibilizzazione e prevenzione nell'uso consapevole delle TIC, di Internet e delle tecnologie emergenti, l'Istituto intende predisporre un'apposita area dedicata all'interno del sito istituzionale, nella quale saranno raccolti e resi facilmente accessibili i collegamenti alle principali risorse del progetto Generazioni Connesse.

Tale sezione sarà concepita come uno spazio di riferimento organico e aggiornato, a disposizione dei Consigli di classe, al fine di favorire l'integrazione sistematica delle tematiche di cittadinanza digitale nella progettazione didattica.

In particolare, l'area metterà a disposizione il Kit Didattico, costituito da materiali strutturati, flessibili e modulabili, progettati per:

- supportare l'attività didattica dei docenti nell'ambito dell'educazione civica digitale;
- promuovere lo sviluppo delle competenze digitali, civiche e sociali degli studenti e delle studentesse;
- favorire percorsi di sensibilizzazione e prevenzione rispetto ai rischi connessi all'uso delle tecnologie digitali, tra cui l'uso improprio di Internet, dei social media e degli strumenti di Intelligenza Artificiale;
- facilitare l'adozione di metodologie didattiche attive e partecipative, coerenti con i bisogni formativi delle diverse classi.

Inoltre, l'Istituto prevede la creazione di un'area di condivisione interna dedicata alla documentazione delle attività didattiche svolte, nella quale confluiranno:

- i materiali e i prodotti realizzati nelle singole classi, quali esiti dei percorsi di Educazione civica digitale;
- strumenti e modalità per la verifica delle attività svolte, al fine di garantire coerenza, qualità e miglioramento continuo dei percorsi educativi;
- spazi di confronto e riflessione professionale tra docenti, finalizzati allo scambio di buone pratiche, esperienze didattiche e strategie di prevenzione.

I materiali ritenuti maggiormente significativi saranno selezionati dalla Commissione ePolicy e, previo opportuno vaglio, resi disponibili in una sezione dedicata del sito istituzionale, al fine di favorirne la diffusione e la condivisione con famiglie e studenti/studentesse, nel rispetto delle normative vigenti in materia di privacy e tutela dei dati.

L'utilizzo del Kit Didattico e delle risorse condivise sarà promosso quale pratica sistemica, finalizzata a garantire coerenza e continuità nell'attuazione del curriculum di Educazione civica e nella diffusione di comportamenti digitali responsabili all'interno della comunità scolastica.

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

3.1 - Protezione dei dati personali e GDPR

La protezione dei dati personali delle persone fisiche costituisce un diritto fondamentale. L'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea e l'art. 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Le principali normative di riferimento sono il Regolamento Generale sulla Protezione dei Dati 2016/679 noto anche come GDPR, e il Dlgs 196/2003 conosciuto come Codice Privacy.

Il settore dell'istruzione è particolarmente impattato dalla tematica privacy in considerazione del fatto che gli Istituti Scolastici sono chiamati, necessariamente, a trattare un'enorme mole di dati personali.

Con l'entrata in vigore del GDPR è stato introdotto l'obbligo per ciascun Istituto scolastico di provvedere alla designazione di un Responsabile della protezione dei dati personali (RPD o DPO).

I principali obblighi in materia di protezione dei dati personali consistono nella definizione di un "organigramma privacy", nel rilascio dell'informativa al momento della raccolta dei dati e nella tenuta di un registro dei trattamenti.

L'Istituzione scolastica, nell'ambito delle attività connesse alla gestione dell'infrastruttura digitale e dei servizi ICT, assicura il trattamento dei dati personali nel pieno rispetto della normativa vigente, in particolare del Regolamento (UE) 2016/679 (GDPR) e delle disposizioni nazionali in materia.

Il trattamento dei dati personali avviene esclusivamente per il perseguimento di finalità istituzionali, educative e amministrative, nel rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione e sicurezza. A tal fine, l'Istituto adotta misure tecniche e organizzative adeguate volte a garantire la protezione e la riservatezza dei dati, prevenendo accessi non autorizzati, perdita o utilizzi impropri delle informazioni.

A tutti i soggetti interessati - studenti e studentesse, famiglie, personale docente e personale ATA - viene fornita una informativa chiara e completa relativamente alle modalità e alle finalità del trattamento dei dati personali, nonché all'identità del Titolare del trattamento e dei responsabili eventualmente designati. Nei casi previsti dalla normativa, è richiesto un consenso libero, specifico e informato, acquisito mediante apposita modulistica, limitando la raccolta ai soli dati strettamente necessari.

È garantito il pieno esercizio dei diritti dell'interessato, tra cui il diritto di accesso, rettifica, aggiornamento e, ove previsto, cancellazione dei dati personali trattati dall'Istituto.

In un'ottica di sensibilizzazione e prevenzione, la scuola promuove la diffusione di comportamenti corretti e responsabili nella gestione dei dati e nell'utilizzo delle tecnologie digitali, favorendo la consapevolezza dei rischi connessi alla circolazione delle informazioni online, anche in relazione all'utilizzo di Internet e delle tecnologie emergenti, inclusa l'Intelligenza Artificiale.

L'Istituto è dotato di un Regolamento interno che disciplina l'accesso e l'utilizzo dei laboratori, degli spazi di apprendimento

alternativi e della rete LAN, definendo regole di comportamento finalizzate alla tutela della sicurezza informatica e dei dati trattati.

Al fine di garantire un accesso sicuro e controllato ai servizi digitali, il personale docente, il personale ATA e gli studenti e le studentesse dispongono di credenziali personali per l'accesso alla piattaforma istituzionale Office 365 e di un account di posta elettronica con dominio istituzionale. Tali strumenti sono utilizzati nel rispetto delle policy interne e delle normative vigenti, promuovendo un uso responsabile, consapevole e conforme ai principi di protezione dei dati.

Attraverso tali misure, l'Istituto intende assicurare un ambiente digitale sicuro, affidabile e conforme, contribuendo allo sviluppo di una cultura della protezione dei dati personali e della cittadinanza digitale responsabile all'interno dell'intera comunità scolastica.

3.2 - Strumenti di comunicazione online (PUA)

La Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) è un documento che racchiude una serie di regole legate all'utilizzo della rete a scuola e a casa da parte di studenti e di tutto il personale (compresi i professionisti esterni che lavorano in contesto scolastico), integrante il DPS (Documento programmatico sulla Sicurezza). Il documento, che funge da raccordo, si compone di punti strategici riguardanti non solo i vantaggi di internet a scuola ma anche i rischi connessi all'online, nella valutazione di quei contenuti presenti in rete e di quelle azioni negative che possono comprometterne l'uso positivo. Fra queste attività: ricercare materiale non consono allo stile educativo della scuola; produrre vere e proprie azioni illecite; giocare online con la rete scolastica; violare la privacy e i diritti d'autore, etc... Nella Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) vengono definite, dunque, le regole di utilizzo fra tutti gli attori in gioco, nel rispetto dei dati sensibili di ciascuno, in particolar modo degli alunni e delle alunne.

L'Istituto, articolato nelle diverse sedi, dispone di una dotazione tecnologica diffusa e capillare, implementata anche attraverso finanziamenti europei e nazionali (PON) e nell'ambito delle azioni previste dal Piano Nazionale Scuola Digitale (PNSD). Tale infrastruttura consente l'erogazione di servizi digitali funzionali sia alle attività didattiche sia a quelle amministrative.

La connettività di rete, garantita sia in modalità cablata sia tramite rete Wi-Fi, assicura l'accesso a Internet in condizioni di sicurezza controllata, favorendo l'utilizzo consapevole delle tecnologie digitali nei diversi contesti scolastici. La rete didattica consente l'accesso ai servizi digitali nelle aule dotate di strumentazione tecnologica, nei laboratori scientifici e multimediali, nelle biblioteche e negli spazi polifunzionali dedicati alla didattica e alla progettazione educativa.

In tali ambienti, l'utilizzo del registro elettronico (Spaggiari - ClasseViva) rappresenta uno strumento centrale per la gestione delle attività scolastiche e per la comunicazione istituzionale, nel rispetto delle normative vigenti in materia di protezione dei dati personali.

L'accesso alle infrastrutture tecnologiche e alla rete è regolamentato da specifiche procedure interne che prevedono:

- l'accesso alla rete è disciplinato attraverso modalità differenziate: accesso alla rete WLAN mediante credenziali configurate dall'Animatore Digitale e accesso alla rete LAN tramite collegamento cablato (cavo Ethernet), nel rispetto delle procedure interne finalizzate alla sicurezza e al corretto utilizzo delle infrastrutture digitali;
- l'accesso degli studenti e delle studentesse alla rete esclusivamente in contesti didattici strutturati e sotto la supervisione dei docenti o del personale tecnico;

- la definizione di criteri di utilizzo finalizzati a garantire la sicurezza delle informazioni e la corretta fruizione delle risorse digitali.

Gli assistenti tecnici informatici, in collaborazione con l'Animatore Digitale, assicurano l'aggiornamento periodico dei software e dei sistemi operativi, al fine di prevenire vulnerabilità, ridurre i rischi di attacchi informatici e garantire un ambiente digitale protetto.

In coerenza con le politiche di sicurezza e protezione dei dati, l'Istituto utilizza la piattaforma Office 365, adottando criteri stringenti di gestione delle utenze e degli accessi, quali:

- gestione e monitoraggio delle credenziali di accesso;
- sistemi di protezione delle password e procedure di backup;
- criteri di archiviazione sicura dei documenti digitali.

Tali misure si inseriscono in un quadro più ampio di policy interne per la sicurezza informatica, finalizzate a prevenire usi impropri degli strumenti digitali e a garantire la tutela dei dati trattati.

Parallelamente, il curriculum di Educazione civica sviluppato dall'Istituto promuove, per ciascuna annualità, percorsi di riflessione e approfondimento sui temi della cittadinanza digitale, fornendo agli studenti e alle studentesse strumenti per una lettura critica delle opportunità e dei rischi connessi all'uso delle tecnologie.

In particolare, viene valorizzato il principio secondo cui la familiarità con gli strumenti digitali non implica automaticamente una competenza consapevole: pertanto, si ritiene fondamentale sviluppare specifiche competenze di utilizzo critico e responsabile, contrastando l'idea che i cosiddetti "nativi digitali" non necessitino di un adeguato percorso formativo.

Attraverso l'integrazione tra infrastrutture tecnologiche, strumenti di comunicazione online e percorsi educativi, l'Istituto si propone di garantire un ambiente digitale sicuro, regolamentato e orientato alla prevenzione, promuovendo al contempo un uso consapevole, efficace e responsabile delle tecnologie dell'informazione e della comunicazione.

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.

Nell'ambito delle politiche di utilizzo consapevole delle tecnologie digitali e degli strumenti di comunicazione, l'Istituto disciplina l'impiego dei dispositivi personali (BYOD - Bring Your Own Device) al fine di garantire un uso coerente con le finalità educative, nel rispetto delle norme vigenti e dei principi di sicurezza e tutela della persona.

STUDENTI E STUDENTESSE

Durante le attività didattiche, agli studenti e alle studentesse è consentito l'utilizzo di dispositivi personali (smartphone, tablet, computer portatili), esclusivamente per finalità didattiche e previa autorizzazione del docente, sotto la sua vigilanza.

In conformità alla normativa vigente, in particolare al D.P.R. 249/1998 (Statuto delle studentesse e degli studenti) e successive modifiche, nonché alle disposizioni ministeriali in materia di uso dei dispositivi mobili in ambito scolastico, è fatto divieto di:

- utilizzare i telefoni cellulari per finalità non didattiche durante le lezioni e l'orario scolastico;
- effettuare telefonate, scattare fotografie o registrare video e audio senza esplicita autorizzazione del docente;
- diffondere contenuti digitali in modo illecito o non appropriato, con particolare riferimento a immagini, registrazioni o messaggi lesivi della dignità delle persone.

È altresì vietato inviare o condividere contenuti non conformi alle norme di comportamento e alle disposizioni di legge.

L'eventuale accesso a Internet tramite dispositivi personali avviene attraverso connessione autonoma (rete personale), ferma restando la responsabilità individuale nell'utilizzo delle risorse digitali.

DOCENTI E PERSONALE

Per il personale docente, durante lo svolgimento delle attività didattiche non è consentito l'utilizzo del telefono cellulare per finalità personali, salvo casi eccezionali debitamente motivati. L'uso dei dispositivi personali è ammesso esclusivamente per scopi didattici, organizzativi o funzionali all'insegnamento.

È consentito l'impiego di altri dispositivi elettronici personali (quali computer portatili e tablet), purché utilizzati in modo coerente con le esigenze didattiche e in integrazione con le dotazioni tecnologiche dell'Istituto.

Durante il restante orario di servizio, nel rispetto delle disposizioni organizzative interne, è permesso l'utilizzo di dispositivi personali per attività connesse alla funzione docente (programmazione, documentazione, comunicazione istituzionale), con accesso alla rete Wi-Fi negli spazi comuni abilitati, secondo le modalità previste dalla configurazione della rete scolastica.

FINALITÀ EDUCATIVE E PREVENZIONE

Le disposizioni relative all'utilizzo dei dispositivi personali si inseriscono in un più ampio quadro di educazione alla cittadinanza digitale, finalizzato a:

- promuovere un uso consapevole, responsabile e critico delle tecnologie digitali;
- prevenire comportamenti a rischio, quali il cyberbullismo, la violazione della privacy e l'uso improprio delle risorse digitali;
- sviluppare nei soggetti della comunità scolastica competenze di autonomia, responsabilità e rispetto delle regole negli ambienti digitali.

L'Istituto si impegna a garantire un equilibrio tra l'innovazione didattica e la tutela dei diritti, promuovendo un uso regolamentato dei dispositivi personali in coerenza con le finalità educative e con il quadro normativo di riferimento.

Cap 4 - Segnalazione e gestione dei casi

4.1 - Cosa Segnalare

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

All'interno della comunità scolastica, tutti i soggetti coinvolti – Dirigente scolastico, docenti, personale ATA, studenti e studentesse, famiglie – sono chiamati, ciascuno in relazione al proprio ruolo e alle proprie competenze, a contribuire attivamente alle azioni di prevenzione, individuazione, segnalazione e gestione di episodi riconducibili a fenomeni di bullismo e cyberbullismo, nonché ad altre forme di uso improprio delle tecnologie digitali.

L'Istituto promuove una cultura della responsabilità condivisa, orientata alla costruzione di un ambiente scolastico sicuro, inclusivo e rispettoso, nel quale sia possibile riconoscere tempestivamente situazioni di disagio e attivare adeguati interventi educativi e di tutela.

Sono oggetto di segnalazione, a titolo esemplificativo ma non esaustivo:

- comportamenti di prevaricazione, intimidazione o esclusione reiterata ai danni di uno o più studenti;
- episodi di cyberbullismo, quali la diffusione di contenuti offensivi, denigratori o lesivi tramite social network, piattaforme digitali o strumenti di messaggistica;
- utilizzo improprio delle tecnologie digitali, inclusa la condivisione non autorizzata di immagini, video o dati personali;
- situazioni riconducibili a violazioni della privacy, del rispetto della persona e della convivenza civile negli ambienti digitali e scolastici;
- comportamenti a rischio connessi all'uso di Internet e delle tecnologie emergenti.

Al fine di garantire un presidio costante e una gestione coordinata delle segnalazioni, in ogni classe viene individuato annualmente un referente per il bullismo e il cyberbullismo per ciascuna componente (docente, studenti/studentesse e genitori), con funzione di raccordo e primo ascolto. Tali figure operano in sinergia con il Referente d'Istituto per il bullismo e il cyberbullismo, al quale competono il coordinamento delle azioni di intervento, la gestione dei casi e l'attivazione delle procedure previste.

Il sistema di segnalazione si fonda su principi di riservatezza, tempestività e tutela delle persone coinvolte, nel rispetto delle normative vigenti e delle procedure interne dell'Istituto.

Attraverso la strutturazione di procedure chiare e condivise, l'Istituto intende rafforzare le azioni di prevenzione e contrasto, promuovendo nei diversi attori della comunità scolastica una maggiore consapevolezza dei fenomeni e delle modalità corrette di intervento.

4.2 - Quali strumenti e a chi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Strumenti a disposizione di studenti/esse

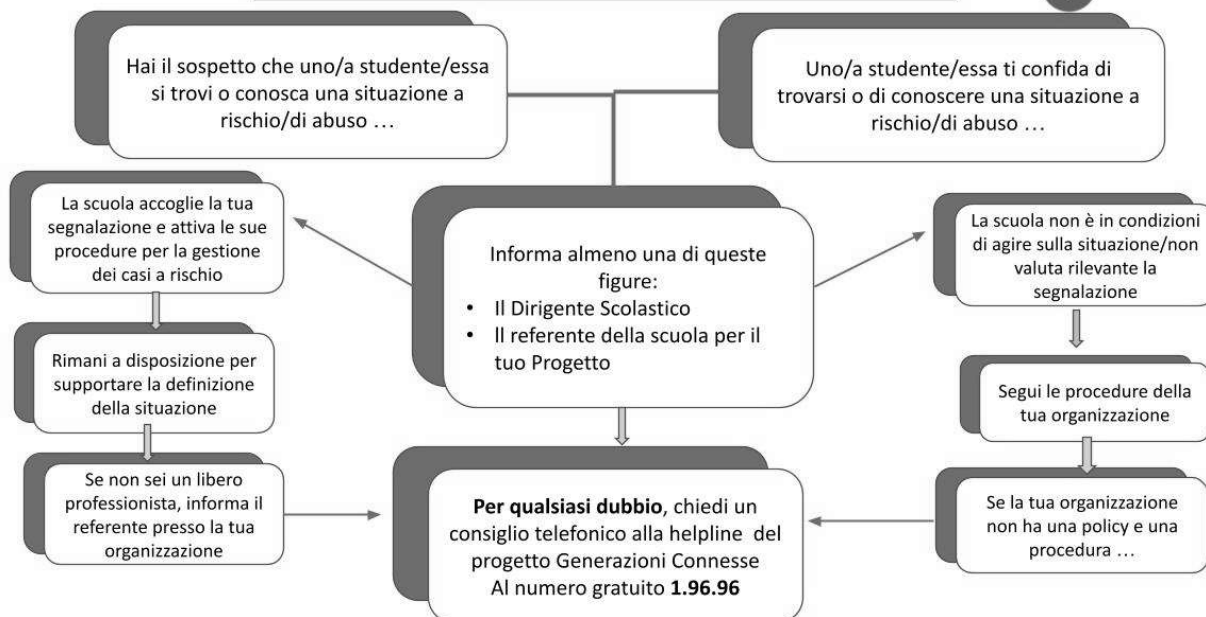
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

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

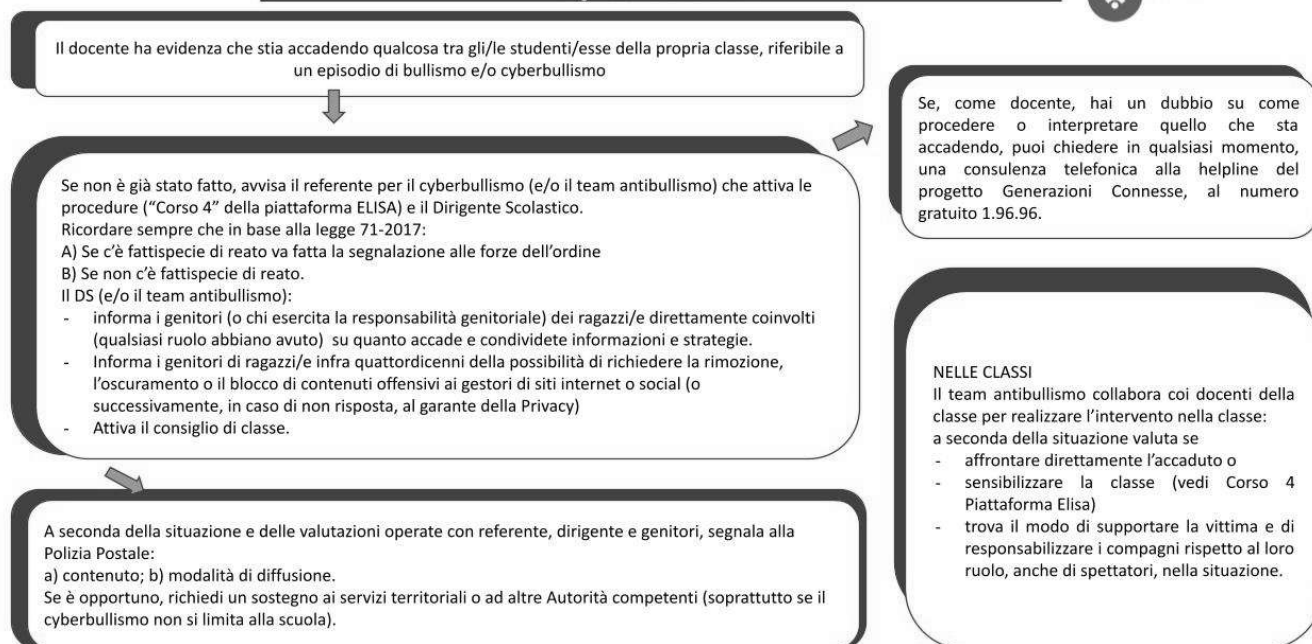
Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle [Linee di Orientamento per la prevenzione e il contrasto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

Procedure

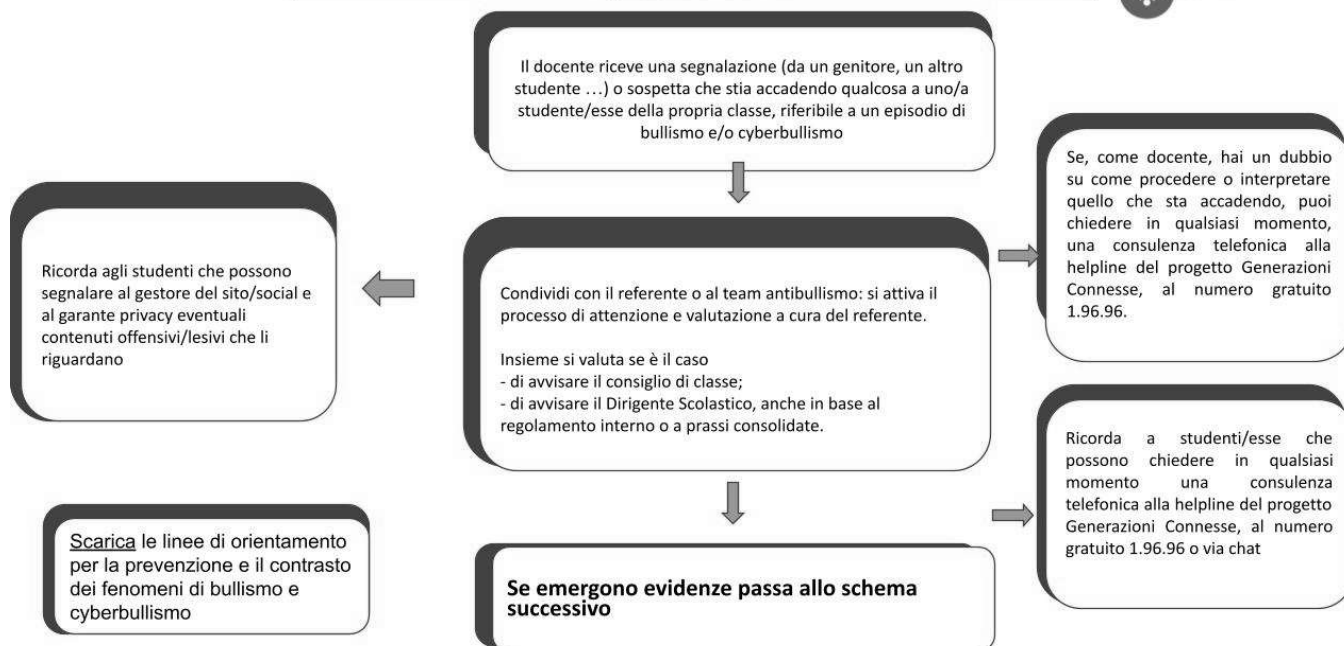
Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola



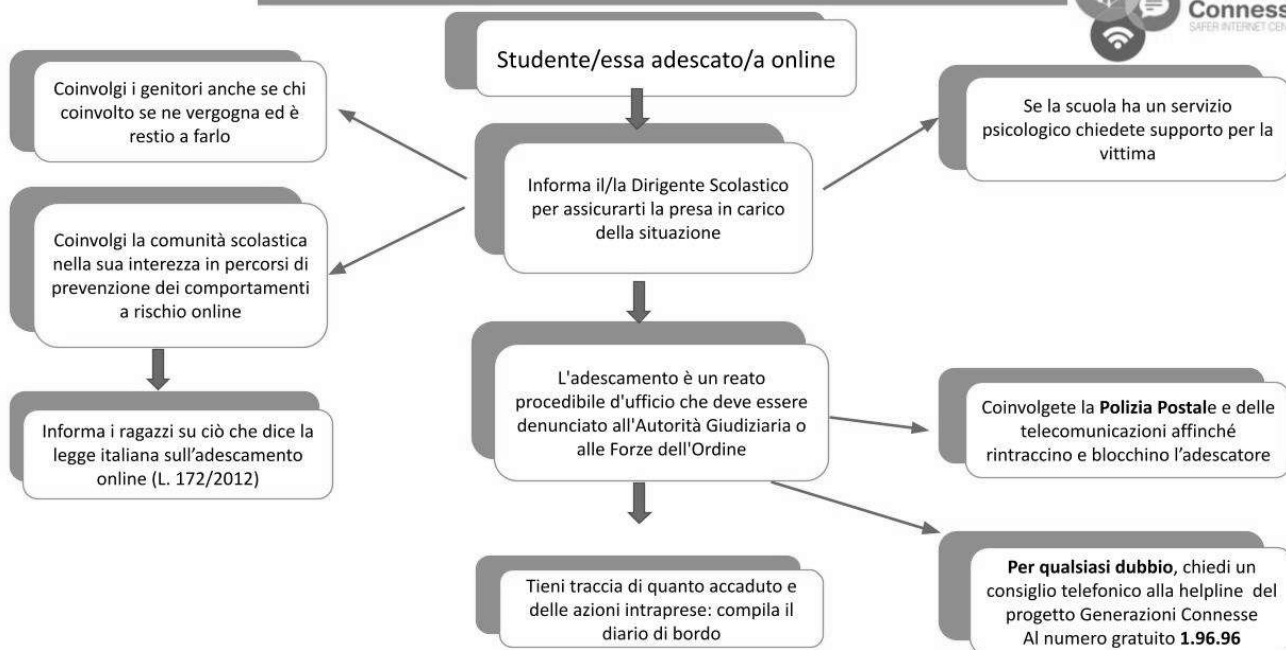
Procedure interne: cosa fare in caso di evidenza di Cyberbullismo



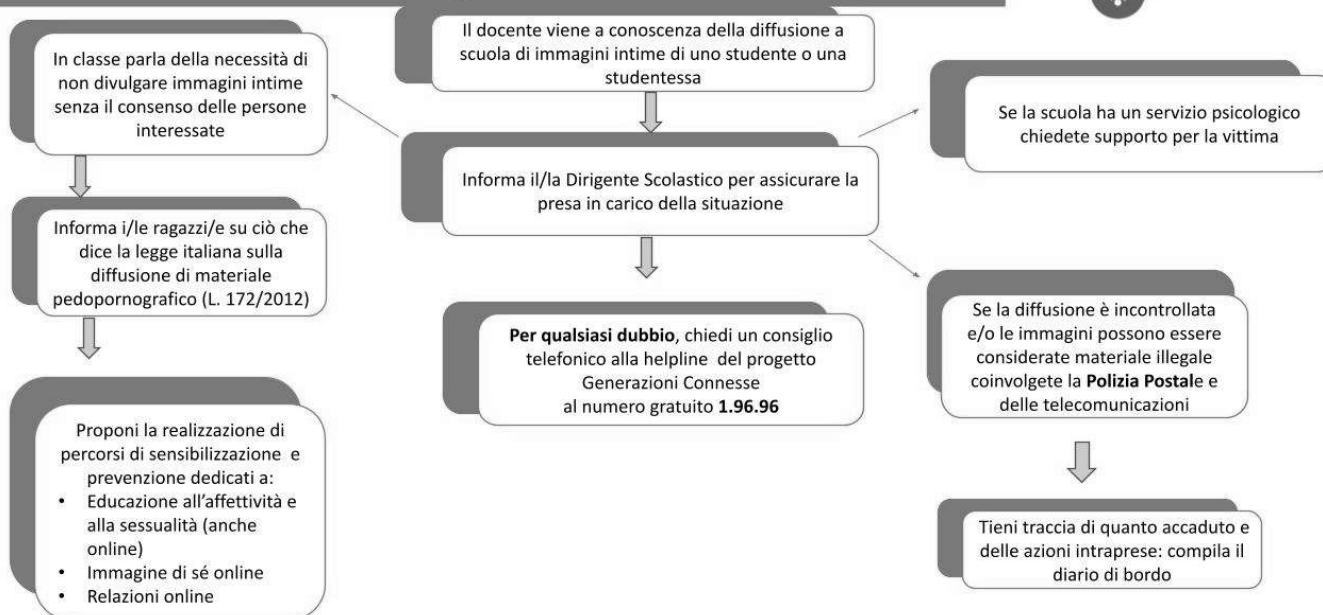
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



Procedure interne: cosa fare in caso di Adescamento Online?



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



Al fine di favorire l'emersione tempestiva di situazioni problematiche e garantire un adeguato sistema di tutela, l'Istituto promuove l'adozione di strumenti strutturati per la segnalazione, rivolti in particolare a studenti e studentesse, ma accessibili all'intera comunità scolastica.

In tale contesto, la scuola mette a disposizione canali diversificati, finalizzati a intercettare, in modo efficace e nel rispetto della riservatezza, eventuali situazioni di disagio, episodi di bullismo e cyberbullismo o altre forme di utilizzo improprio delle tecnologie digitali.

In particolare, sono previsti i seguenti strumenti di segnalazione:

- un indirizzo e-mail istituzionale dedicato, pubblicato sul sito della scuola, riferito al Referente per il bullismo e il cyberbullismo, al quale possono rivolgersi tutti i soggetti (studenti/studentesse, famiglie, docenti, personale ATA), indipendentemente dal dominio della propria casella di posta elettronica;
- la possibilità, per gli studenti e le studentesse, di rivolgersi ai referenti di classe per il bullismo, individuati annualmente per ciascuna componente (docente, alunni, genitori), quale primo livello di ascolto e supporto;
- ulteriori strumenti di supporto, quali sportelli di ascolto e, ove attivati, modalità di segnalazione anche anonima (ad esempio box di raccolta), finalizzati a facilitare l'espressione di situazioni di disagio.

Per quanto riguarda il personale docente, la gestione delle situazioni problematiche è regolata dal Regolamento d'Istituto per la prevenzione e il contrasto del bullismo e cyberbullismo, pubblicato sul sito istituzionale, che definisce le procedure operative da seguire in caso di rilevazione o sospetto di episodi all'interno della classe.

Il sistema di segnalazione adottato dall'Istituto si fonda sui principi di:

- accessibilità, per garantire a tutti i soggetti la possibilità di segnalare in modo semplice e diretto;
- riservatezza, a tutela delle persone coinvolte;
- tempestività, al fine di attivare rapidamente le azioni di intervento;

- responsabilità condivisa, promuovendo il coinvolgimento attivo di tutte le componenti della comunità scolastica.

Attraverso tali strumenti, l'Istituto intende rafforzare le azioni di prevenzione, monitoraggio e intervento, favorendo un clima scolastico improntato al rispetto, alla sicurezza e al benessere di tutti.