Documento di ePolicy
I.C. GIUSEPPE VERDI -PA

VIA A. CASELLA N. 33/35 - 90145 - PALERMO
Palermo (PA) - Sicilia
Data di approvazione: 29/12/2025 - 13:12

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.

Per il nostro Istituto dotarsi di una e-policy è un passo fondamentale per dare coerenza, sistematicità e visione condivisa alle pratiche di educazione digitale già previste nel *Curricolo Verticale di Educazione Civica*.

Nel nostro Curricolo verticale l'educazione alla cittadinanza digitale è individuata come una delle competenze chiave per la formazione del cittadino consapevole, responsabile e attivo. Il percorso formativo promosso dalla nostra istituzione scolastica mira, infatti, a sviluppare nei bambini e negli alunni conoscenze, abilità e atteggiamenti che consentano loro di usare le tecnologie in modo critico, sicuro, inclusivo e rispettoso degli altri, nel quadro dei valori costituzionali e degli obiettivi dell'Agenda 2030.

In questa prospettiva, la ePolicy diventa uno strumento strategico che offre a docenti, alunni e famiglie linee guida chiare per l'uso consapevole, sicuro e responsabile delle tecnologie digitali. Previene e contrasta fenomeni di rischio, come il cyberbullismo, la violazione della privacy, la disinformazione e le dipendenze digitali, in coerenza con le finalità di tutela e di educazione alla legalità proprie della nostra scuola. Favorisce un approccio trasversale e inclusivo all'educazione digitale, in continuità verticale tra i diversi ordini di scuola. Promuove, altresì, la partecipazione e la corresponsabilità educativa tra scuola, famiglie e territorio, creando una comunità educante capace di condividere regole, linguaggi e valori comuni anche nell'ambiente digitale. La nostra Istituzione scolastica sostiene l'innovazione metodologica e organizzativa, valorizzando le potenzialità delle tecnologie come strumenti di apprendimento collaborativo, creativo, inclusivo e orientato alla cittadinanza attiva.

Parallelamente, il nostro *Regolamento per la prevenzione e il contrasto del bullismo e del cyberbullismo* definisce in modo chiaro le responsabilità educative e operative di tutte le componenti scolastiche, valorizzando la collaborazione tra scuola, famiglie, studenti, enti territoriali e forze dell'ordine. In esso si afferma con forza che la vera sicurezza digitale non nasce dalla repressione, ma dalla conoscenza, dalla formazione e dalla promozione di una cultura dell'ascolto e del rispetto in rete.

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

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

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

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

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

IL DIRIGENTE SCOLASTICO

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

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

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

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

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

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

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

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

Il Team ha il compito di:

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

I/LE DOCENTI

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

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

RESPONSABILE DELLA PROTEZIONE DEI DATI

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

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

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

GLI STUDENTI E LE STUDENTESSE

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

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

I GENITORI/ADULTI DI RIFERIMENTO

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

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

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

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

Il Patto di corresponsabilità educativa, adottato dal nostro Istituto, riconosce che scuola e famiglia, insieme, costituiscono una comunità educativa. Tale alleanza garantisce ai bambini e agli alunni un percorso di crescita sereno, armonioso e inclusivo, fondato sul rispetto reciproco, sul benessere e sull'inclusione. La collaborazione tra genitori e scuola favorisce un ambiente accogliente e stimolante, in cui ciascuno può esprimere pienamente i propri talenti.

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.

Il nostro Istituto, in linea con il Piano Nazionale Scuola Digitale e grazie alle azioni del PNRR, ha avviato la formazione dei docenti e di tutto il personale ATA nell'ambito dell'innovazione digitale per la didattica e per l'amministrazione con l'obiettivo di potenziare le competenze digitali sia dei docenti che del personale amministrativo. Sono stati infatti attivati corsi formazione sull' intelligenza artificiale e la didattica e sulla didattica STEM.

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

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

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

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

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

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

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

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

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

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

L'E-policy viene condivisa e comunicata al personale della scuola, ai genitori e alla comunità scolastica attraverso:

-la pubblicazione del documento sul sito istituzionale della scuola;

- la pubblicazione come allegato al Piano Triennale dell'Offerta Formativa, al Regolamento di Istituto e al Patto di corresponsabilità.

1.5 - I Piani di Azione dell'ePolicy

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

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

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

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

1° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

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

MODULO II

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

MODULO III

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

MODULO IV

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

2° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

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

MODULO II

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

Attraverso tali azioni, l'Istituto si impegna a guidare e supportare gli alunni nella navigazione online consapevole e sicura, nella gestione responsabile degli spazi digitali e scolastici, e nel rispetto delle regole di condotta da tenere in Rete, al fine di favorire comportamenti corretti e responsabili nella comunità scolastica.

In linea con il Piano Nazionale Scuola Digitale e grazie alle azioni del PNRR, il nostro Istituto ha altresì avviato e realizzato un piano di formazione dei docenti e di tutto il personale ATA nell'ambito dell'innovazione digitale per la didattica e per l'amministrazione con l'obiettivo di potenziare le competenze digitali sia dei docenti che del personale amministrativo. Sono stati infatti attivati corsi formazione sull' intelligenza artificiale e la didattica e sulla didattica STEM.

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

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

Cap 2 - Sensibilizzazione e prevenzione

2.1 - Sensibilizzazione e prevenzione

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

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

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

L'Istituto realizza regolarmente interventi di prevenzione e contrasto al bullismo e al cyberbullismo attraverso attività finalizzate a informare gli alunni sulle caratteristiche e sulle diverse tipologie dei fenomeni, sulle strategie di tutela personale, sulle modalità per riconoscere tempestivamente situazioni di rischio e sulle risorse interne ed esterne alla scuola. Durante tali interventi vengono inoltre presentati i numeri utili e i servizi territoriali a cui rivolgersi in caso di bisogno, offrendo agli alunni un quadro chiaro e accessibile degli strumenti di supporto.

Vengono altresì proposti percorsi dedicati alla gestione delle emozioni e allo sviluppo delle competenze relazionali, riconosciute come fondamentali per favorire comportamenti corretti ed equilibrati anche negli ambienti digitali. Parallelamente, l'Istituto organizza incontri rivolti alle famiglie per sensibilizzare sui rischi della rete, sull'uso consapevole dei dispositivi e dei social network, e per fornire indicazioni educative pratiche che permettano una continuità di intervento tra scuola e contesto domestico.

L'Istituto collabora stabilmente con la Polizia Postale e con associazioni specializzate nella prevenzione dei rischi digitali, promuovendo attività di informazione, testimonianza e sensibilizzazione rivolte agli alunni della scuola primaria e secondaria. Tali collaborazioni contribuiscono a rafforzare un approccio integrato, concreto e condiviso alla sicurezza digitale.

Accanto agli interventi rivolti a studenti e famiglie, l'Istituto promuove anche la formazione continua del personale docente sui temi della cittadinanza digitale, della tutela online, della prevenzione del cyberbullismo, della gestione dei comportamenti a rischio e dell'educazione all'uso consapevole delle tecnologie.

2.2 - Il Curricolo Digitale

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

Il DigComp 2.2, framework europeo sulle competenze digitali, permette di costruire una cornice precisa in cui inquadrare i

temi e le corrispondenti competenze da proporre nell' Istituto non solo per gli studenti.

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

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

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

CITTADINANZA DIGITALE				
Traguardo per lo sviluppo delle competenze	**Obiettivi di apprendimento**	**Conoscenze / Argomenti da trattare**	**Abilità**	**CLASSI e DISCIPLINE**
1) Sviluppare la capacità di accedere alle informazioni, alle fonti, ai contenuti digitali, in modo critico, responsabile e consapevole.	1 Ricercare in rete semplici informazioni, distinguendo dati veri e falsi.			**4 - 5 Italiano – Matematica – Tecnologia - Storia**
	2) Utilizzare le tecnologie per elaborare semplici prodotti digitali.			**4 - 5 Italiano – Tecnologia -**
	3) Riconoscere semplici fonti di informazioni digitali.			**4 - 5 Italiano – Tecnologia -**
2) Interagire con gli altri attraverso le tecnologie digitali consentite, individuando forme di comunicazione adeguate ai diversi contesti di relazione, adottando e rispettando le regole comportamentali proprie di ciascun contesto comunicativo.	1) Interagire con strumenti di comunicazione digitale, quali tablet e computer.			**3 - 4 - 5 Italiano – Tecnologia - Matematica**
	2) Conoscere e applicare semplici regole per l'utilizzo corretto di strumenti di comunicazione digitale, quali tablet e computer.			**3 - 4 - 5 Italiano – Tecnologia - Matematica**
	3) Conoscere e applicare le principali regole di partecipazione alle classi virtuali e alle piattaforme didattiche.			**3 - 4 - 5 Italiano – Tecnologia - Matematica**
3) Gestire l'identità digitale e i dati della rete, salvaguardando la propria e altrui sicurezza negli	1) Conoscere il significato di identità e di informazioni personali in semplici contesti digitali di uso quotidiano.			**4 - 5 Italiano – Tecnologia - Matematica**
ambienti digitali, evitando minacce per la salute e il benessere fisico e psicologico di sé e degli altri.	2) Conoscere i rischi connessi con l'utilizzo degli strumenti digitali in termini di sicurezza personale.			**4 - 5 Italiano – Tecnologia - Matematica**
	3) Conoscere semplici modalità per evitare rischi per la salute e minacce al benessere psico-fisico quando si utilizzano le tecnologie digitali. Riconoscere, evitare e contrastare le varie forme di bullismo e cyberbullismo.			**4 - 5 Italiano – Tecnologia - Matematica**

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.

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.

Il nostro Istituto dispone di una strumentazione tecnologica a supporto della didattica che soddisfa pienamente le esigenze didattiche.Tutte le aule sono attrezzate con LIM collegate a un pc e connesse alla rete wireless. Il nostro Istituto è dotato nel plesso centrale e nel plesso succursale di un' aula informatica con collegamento internet sia via cavo che wireless. Ogni plesso dispone di un'aula informatica con collegamento Internet sia via cavo sia wireless, utilizzate dagli alunni per attività didattiche e laboratoriali nel rispetto del Regolamento d’Istituto. Il collegamento Internet in classe è riservato ai docenti, per garantire un uso sicuro e controllato della rete. Per quanto riguarda gli uffici amministrativi, ogni postazione è dotata di pc connesso alla rete. Il collegamento ad intenet è disponibile solo per i docenti in classe. La risoluzione delle problematiche relative alle dotazioni tecnologiche dell'Istituto è affidata ad un tecnico specializzato esterno. La gestione e la risoluzione delle problematiche legate alla piattaforma GSuite o al registro elettronico Argo DidUp è affidata all'animatore digitale d'Istituto. La manutenzione e la risoluzione delle problematiche tecniche relative alle dotazioni informatiche sono affidate a un tecnico specializzato esterno, mentre la gestione delle piattaforme digitali (Google Workspace for Education e registro elettronico Argo DidUp) è curata dall’Animatore Digitale d’Istituto.

Per quanto riguarda le modalità di trattamento dei dati personali del Registro Elettronico (ex artt. 13 e 14 Regolamento UE 2016/679 "GDPR"), il Trattamento avviene nel rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, così come previsti dagli articoli 5 e 32 del GDPR.
In particolare:
• I dati sono trattati principalmente con strumenti informatici e telematici, mediante l'utilizzo di una piattaforma digitale messe a disposizione da un fornitore selezionato e contrattualizzato dalla scuola quale Responsabile del Trattamento ai sensi della normativa vigente e nel rispetto delle misure di sicurezza previste dal Regolamento.
• L’accesso al registro elettronico è protetto da credenziali personali attribuite univocamente a ciascun utente (docente, studente, genitore o tutore), al fine di garantirel’autenticazione sicura e il tracciamento degli accessi.
• Il personale scolastico è autorizzato al trattamento in base alle funzioni svolte ed è appositamente istruito per operare nel

rispetto della normativa vigente in materia di protezione dei dati personali.
• Il sistema registra le attività svolte (log di accesso e modifica) per finalità di sicurezza e tracciabilità. La piattaforma di Registro Elettronica adottata integra in maniera nativa i più
moderni sistemi di tracciabilità delle operazioni effettuate dagli utenti, nel rispetto della loro privacy: i log di tracciamento sono accessibili esclusivamente su richiesta delle autorità
giudiziarie.
• I dati sono trattati in modo da garantire la riservatezza e la protezione contro accessi non
autorizzati, alterazioni, divulgazioni o distruzioni. Sono adottate misure tecniche e organizzative adeguate, tra cui:

- crittografia dei dati e delle comunicazioni, ove applicabile;

- sistemi di backup periodico e disaster recovery; - aggiornamenti regolari dei software e sistemi antivirus;

- segregazione dei profili utente in base ai ruoli e alle funzioni.
  • In alcune situazioni, il trattamento può avvenire anche in modalità cartacea, qualora necessario o previsto da specifiche disposizioni normative (es. verbali, certificati, deleghe, ecc.), sempre nel rispetto delle medesime garanzie di sicurezza e riservatezza.
  I dati personali saranno conservati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono trattati.
- In sintesi:
  • Dati didattici (valutazioni, assenze, note disciplinari): Termine di conservazione: 5 anni scolastici (salvo casi particolari), data la necessità di documentare il percorso scolastico e rispondere a eventuali richieste o contenziosi.
  • Dati amministrativi (iscrizione, anagrafica, certificazioni): termine di conservazione: 10 anni, come previsto per gli atti amministrativi generali.
  • Conservazione a lungo termine: alcuni dati/documenti (ad esempio voti finali, titoli conseguiti) devono essere versati in conservazione digitale permanente, come previsto dalle Linee Guida AgID.

I dati possono essere comunicati, oltre che ai soggetti nominati Responsabili del trattamento ex art. 28 GDPR, a:
• Personale scolastico autorizzato;

• Ministero dell'Istruzione e del Merito;
• Altre Pubbliche Amministrazioni, nei limiti previsti dalla normativa;
È esclusa la diffusione di dati personali.
Non si effettuano trattamenti automatizzati.

Dati tratti dall' Informativa per il trattamento dei dati personali – Registro Elettronico ex artt. 13 e 14 Regolamento UE 2016/679 ("GDPR") del p05/05/2025

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'accesso alle aule informatiche è regolamentato da precise norme di utilizzo, poiché rappresentano una risorsa didattica e formativa a disposizione dei docenti, degli alunni e degli utenti della scuola.

REGOLAMENTO ACCESSO AULA INFORMATICA

Il Laboratorio di Informatica è una risorsa didattica e formativa a disposizione dei docenti, degli alunni e degli utenti della scuola. Le due aule informatiche presenti nel nostro Istituto possono essere utilizzate, in orario scolastico ed extrascolastico, per attività legate alla diffusione della pratica e/o della cultura informatica. In particolare, le attrezzature devono essere adoperate prioritariamente per le attività didattiche curricolari e, quindi, per le finalità istituzionali e formative della scuola.

Tutti i fruitori sono responsabili del corretto e dell' appropriato uso delle risorse hardware e software loro assegnate per l'attività programmata.

MODALITA' DI ACCESSO

Per accedere al laboratorio il docente deve prendere in consegna la relativa chiave e obbligatoriamente registrare il proprio nome e l'eventuale classe nell'apposito "Registro delle presenze e di segnalazione guasti" indicando l'orario d'ingresso, quello di uscita, la classe e firma del docente presente segnalando nell'apposito spazio note ed eventuali problemi riscontrati per un tempestivo intervento.

L'accesso delle classi in orario curricolare è consentito solo con la presenza del docente. Le chiavi e il registro rimarranno in custodia presso il personale ATA.

NORME DI COMPORTAMENTO PER GLI ALUNNI

1. Gli alunni dovranno utilizzare esclusivamente il pc che gli verrà assegnato dal docente(i pc sono numerati).

2. Gli alunni sono tenuti ad utilizzare i PC solo ed esclusivamente per le attività didattiche proposte dagli insegnanti e a seguire le procedure di lavoro indicate dai docenti stessi.

3. Agli alunni è assolutamente vietato spostarsi da una postazione all'altra senza l'autorizzazione del docente.

4. Gli alunni devono segnalare immediatamente al docente eventuali guasti o anomalie e non sono in nessun caso autorizzati a tentare di risolvere l'eventuale problema di propria iniziativa.

5. Gli alunni non possono alterare le configurazioni del desktop, installare, modificare, scaricare software senza l'autorizzazione del docente, considerando inoltre che la copiatura dei programmi che non siano di pubblico dominio costituisce reato punibile ai sensi della vigente normativa penale;

6. Gli alunni non possono navigare in Internet senza autorizzazione del docente presente in aula e comunque su siti che non siano di comprovata valenza didattica;

7. Gli alunni devono aprire e chiudere correttamente la sessione di lavoro sui pc e spegnere la macchina in modo adeguato.

8. Gli alunni devono salvare i propri lavori:

- sul proprio drive, usando l' account scolastico Google Workspace.

- sul PC, in apposite cartelle intestate a nome della classe (es.: cl.1A sec., cl.5a pr.). A fine anno i docenti selezioneranno i lavori utili per il successivo anno scolastico che salveranno su un supporto USB personale e cancelleranno il resto, lasciando la cartella vuota.

9. Non possono essere scaricati programmi sui PC tranne quelli in uso per le diverse discipline e dovrà sempre essere il docente responsabile della classe ad effettuare le diverse operazioni.

10. La ricreazione deve essere sempre effettuata nella propria classe e non in aula informatica dove è fatto divieto di mangiare, masticare gomme e usare bevande.

NORME COMPORTAMENTO INSEGNANTI

1. I docenti che si recano in aula informatica devono compilare in ogni sua parte il registro dell'aula e apporre la propria firma. Ogni alunno si deve sedere alla postazione a lui assegnata dal docente e annotata sul registro dell'aula di informatica

2. Tutti gli insegnanti che accedono all'aula informatica hanno letto e accettato in toto questo Regolamento e si impegnano a spiegare e a far rispettare agli alunni le norme di seguito elencate.

3. Ogni insegnante è tenuto ad aprire e chiudere l'aula personalmente, assicurandosi al termine dell'utilizzo della stessa, che le chiavi vengano consegnate al personale ATA.

4. Gli insegnanti sono responsabili dell'uso di attrezzature, programmi o quant'altro presenti nel laboratorio. Gli insegnanti possono chiedere di installare nuovi software sui PC del laboratorio, previa autorizzazione del Dirigente o dell'Animatore Digitale.

5. Gli alunni non devono mai essere lasciati senza sorveglianza, e non possono essere impegnati in lavori diversi da quelli proposti dal docente; la mancata sorveglianza degli alunni o del rispetto del presente Regolamento comporta la corresponsabilità su eventuali danni o disfunzioni alle macchine.

6. L'insegnante all'entrata ed all'uscita dall'aula, dovrà verificarne lo stato (danni, manomissioni, ordine ecc.) e comunicare tempestivamente eventuali anomalie al responsabile dell'aula informatica o all'Animatore Digitale.

7. L'insegnante farà terminare la sessione di lavoro con qualche minuto di anticipo per verificare personalmente che il laboratorio sia lasciato in ordine e che le periferiche siano spente.

8. In qualunque momento, l'insegnante che verifica un uso della connessione contrario a disposizioni di legge o del regolamento, e comunque non coerente con i principi che regolano la scuola, può disattivarla senza indugio; in tal caso, darà comunicazione al Coordinatore del Consiglio di Classe per concordare l'adozione di eventuali provvedimenti disciplinari.

VALIDITA' DEL REGOLAMENTO

Tutti i fruitori interni all'istituto ed esterni all'ambito scolastico devono attenersi al presente regolamento, che potrà essere integrato nel corso dell'anno scolastico. Eventuali deroghe a quanto stabilito dal regolamento sono ammesse solo se concordate esplicitamente e preventivamente con il Dirigente Scolastico e con il responsabile referente di laboratorio.

3.3 - BYOD

La presente ePolicy conterrà indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device"). Risulta infatti fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

Il nostro Istituto promuove una formazione digitale consapevole, favorendo l'uso responsabile dei dispositivi mobili personali (Bing Your Own Device) come supporto alle attività didattiche.

L'utilizzo dei dispositivi per fini educativi è regolamentato in modo chiaro, al fine di tutelare gli alunni dai rischi della rete, sviluppare competenze di cittadinanza digitale e promuovere la sicurezza informatica.

Il nostro "Regolamento per l'utilizzo dei dispositivi digitali personali a scuola"dispone che:

ART. 1 - DISPOSITIVI AMMESSI

In tutte le classi sono ammessi i seguenti dispositivi mobili: tablet, notebook, e-reader,cellulare. L'uso di altri dispositivi a scuola non è consentito e si rimanda al Regolamento disciplinare di Istituto.

ART. 2 - USO DEI DISPOSITIVI

I dispositivi ammessi, di cui all'art. 1, devono essere usati a scuola soltanto per scopi didattici. Non è permesso il loro uso per motivi personali o per gioco durante l'orario di lezione, nelle pause, negli intervalli, durante le uscite didattiche, visite guidate, viaggi d'istruzione, attività facoltative extracurricolari, manifestazioni sportive, ecc., se non con l'esplicita autorizzazione del docente responsabile della classe.

- Lo studente è tenuto a portare il dispositivo carico in modo da poterlo utilizzare a scuola senza cavi di alimentazione; è consentito però l'uso di caricabatterie portatili.
- È vietato l'uso delle applicazioni di registrazione audio/video e della fotocamera se non espressamente autorizzate dal docente in servizio e senza il consenso dei soggetti coinvolti.
- È vietato l'uso di Internet o dei social network per scopi diversi da quelli didattici e senza la supervisione del docente; non è consentito scaricare musica, video, programmi o qualsiasi file senza il consenso del docente
- Non è consentito giocare al computer in rete o offline, se non come parte di una lezione.

- È vietato registrare o filmare le lezioni.
- L'uso dei libri in formato digitale è consentito durante tutte le ore di lezione in modalità offline.

Qualsiasi uso improprio e non autorizzato prevede il ritiro e la consegna del dispositivo al Dirigente scolastico ed eventuale sanzione di cui si rimanda al regolamento di disciplina.

ART. 3 - RESPONSABILITÀ INDIVIDUALE

- Ogni studente è responsabile della custodia e del corretto utilizzo del proprio dispositivo;
- la scuola non è responsabile dello smarrimento, furto o danneggiamento del bene che, in nessun caso, dovrà essere lasciato a scuola oltre l'orario delle lezioni o incustodito durante lo svolgimento delle stesse;
- è vietato prendere in prestito dispositivi di altri studenti; la scuola non è responsabile della custodia dei dispositivi e di eventuali danni ad essi procurati dal proprietario o da altri studenti;
- colui che, volontariamente o per negligenza, procura un danno a un dispositivo della scuola o di un compagno, dovrà risarcire il danno, secondo quanto stabilito nel regolamento di disciplina;
- è responsabilità dell'allievo riportare a casa il dispositivo al termine delle attività.

ART. 4 - USO DI INTERNET

La connessione alla rete Wi-Fi d'Istituto da dispositivi mobili è consentita solo previa autorizzazione del Dirigente Scolastico o dell' Animatore Digitale in considerazione di particolari esigenze didattiche; l'utilizzo del dispositivo a scuola avverrà soltanto attraverso la connessione alla rete Wi-Fi dell'Istituto, con le modalità indicate dall'animatore digitale.

Agli studenti è consentito:

- usare Internet (scaricare musica, video, programmi, utilizzare i social network didattici quali, Google Classroom ecc., navigare in rete) solo per scopi didattici e con la supervisione dell'insegnante;
- usare dispositivi elettronici per giochi didattici (es. Coding, etc.) durante le ore scolastiche, come parte integrante di una lezione.

Agli studenti non è consentito:

- usare i propri dispositivi al di fuori dell'orario di lezione. Durante la ricreazione i dispositivi vanno spenti;

- utilizzare la Rete e i social network per deridere, offendere, denigrare compagni,

docenti, personale scolastico, parenti/amici dei compagni.

- utilizzare la Rete e i social network per scaricare o caricare qualsiasi tipo di materiale che non abbia carattere didattico e non sia stato espressamente autorizzato dal docente.

ART. 5 - DIRITTI DI PROPRIETÀ INTELLETTUALE

Gli studenti devono rispettare e proteggere la proprietà intellettuale, pertanto non è ammessa la copia o il plagio di qualsiasi materiale e/o la violazione dei copyrights (es. fare copie illegali di software, musica, giochi o film). Di conseguenza si deve attribuire, citare e richiedere il consenso degli autori o creatori delle informazioni o dei media originali. La scuola favorisce e incentiva l'uso e lo sviluppo dell'open source.

ART. 6 - DIRITTO DI ISPEZIONE DEGLI INSEGNANTI

La scuola si riserva il diritto di monitorare le attività online degli utenti e accedere, controllare, copiare, raccogliere o cancellare ogni comunicazione elettronica o file, rivelando il contenuto alle forze dell'ordine qualora lo ritenga necessario.

La scuola può ispezionare la memoria del dispositivo dello studente se ritiene che le regole scolastiche non siano state rispettate; ciò si riferisce anche, ma non solo, a registrazioni audio e video, fotografie scattate nelle aree di pertinenza della scuola e che violano la privacy altrui o che siano configurabili come atti di bullismo/cyberbullismo.

ART. 7 - COMPITI DEL DOCENTE

Il docente che intende far ricorso alla metodologia BYOD ha il compito di sorvegliare costantemente l'attività degli alunni, di istruirli all'uso "in sicurezza" dei dispositivi, vigilando sull'osservanza e sul rispetto delle norme e delle indicazioni contenute nel presente Regolamento;

Il docente che intende avvalersi del BYOD è tenuto a:

- comunicare il periodo e le caratteristiche dell'attività da svolgere, agli allievi e alle famiglie attraverso il registro elettronico. Il ricorso al BYOD va riportato anche nel piano di lavoro disciplinare.

- Mettere a conoscenza sia gli alunni che i genitori del presente regolamento e verificarne l'autorizzazione tramite il portale Argo.

ART. 8 - COMPORTAMENTI SANZIONABILI PER IL MANCATO RISPETTO DEL REGOLAMENTO

L'uso della tecnologia comporta responsabilità personali. Gli studenti sono tenuti a rispettare le regole dell'Istituto e quelle del presente Regolamento, pena l'attivazione di azioni disciplinari. Saranno sanzionati i seguenti comportamenti:

- Scaricare o caricare video, musica e applicazioni senza il consenso del docente.

- Scaricare o caricare audio/video dal contenuto scabroso o gravemente irridente o per fini non didattici.
- Scattare foto e registrare audio/video a scuola senza autorizzazione del docente.
- Pubblicare tali materiali su pagine o account personali e esportarli su altre piattaforme.
- Utilizzare applicazioni, strumenti di comunicazione e social network durante le lezioni senza esplicita autorizzazione.
- Installare programmi (anche giochi) e/o applicazioni senza l'esplicita autorizzazione del docente.

ART. 9 - NORME DI SALVAGUARDIA

Per quanto non previsto nel presente Regolamento si fa riferimento al Regolamento di Istituto.

Si rammenta, infine, che l'uso dei dispositivi mobili personali (come cellulari e smartphone) è vietato durante tutto l'orario scolastico (tranne per deroghe specifiche come i PEI o PDP) in linea con quanto disposto dalla Nota Ministeriale n. 5274 dell'11 luglio 2024 e dalla Direttiva Ministeriale del 15 marzo 2007.

Cap 4 - Segnalazione e gestione dei casi

4.1 - Cosa Segnalare

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

La tutela della sicurezza in rete dei nostri alunni è per la nostra scuola una priorità. Al fine di individuare strategie di prevenzione e di contrasto al cyberbullismo e favorire opportune azioni educative e pedagogiche, il nostro Istituto promuove la conoscenza e la diffusione delle regole basilari della comunicazione e del comportamento sul web, come:
 netiquette, un insieme di regole informali che disciplinano il buon comportamento di un utente sul web di Internet, specie nel rapportarsi agli altri utenti attraverso risorse come newsgroup, mailing list, forum, blog, reti sociali o email.
 norme di uso corretto dei servizi in rete (ad es. navigare evitando siti web rischiosi; non compromettere il funzionamento della rete e degli apparecchi che la costituiscono con programmi virus, malware, etc. – costruiti appositamente);
 sensibilizzazione alla lettura attenta delle privacy policy, il documento che descrive nella maniera più dettagliata e chiara possibile le modalità di gestione e il trattamento dei dati personali degli utenti e dei visitatori dei siti internet e dei social networks da parte delle aziende stesse;
 costruzione di una propria web-reputation positiva;
 sensibilizzazione sugli effetti psico-fisici del fenomeno dilagante del "vamping" (il restare svegli la notte navigando in rete);
 regolamentazione dell'utilizzo dei telefoni cellulari e di altri dispositivi elettronici a scuola.
 vademecum uso della chat di gruppo da parte dei genitori, per le notevoli ricadute educative e relazionali sui propri figli e sul clima di classe.
 creare degli spazi in cui gli alunni si possono confrontare su questo tema, utilizzando come spunti di riflessione: libri, articoli, spezzoni di film, canzoni, etc.;
 rivolgersi alla "helpline" (1.96.96) di Generazioni connesse- Telefono Azzurro;
 sistemare delle "bully-boxes" in punti strategici dei plessi in cui gli studenti possano segnalare le preoccupazioni e/o il loro disagi.

In un'ottica di prevenzione, nel corso del mese di ottobre- novembre la Referente d'Istituto coordina annualmente il Progetto educativo curriculare di prevenzione al bullismo e cyberbullismo , destinato agli alunni delle classi prime della scuola secondaria di primo grado. Il progetto ha l'obiettivo di promuovere un contesto educativo sicuro ed inclusivo e di fornire agli alunni in ingresso alla scuola secondaria di primo grado strumenti di consapevolezza, riflessione, gestione delle relazioni, ccondivisione di strategie di prevenzione e azioni di contrasto, favorendo al tempo stesso la loro partecipazione attiva e dando voce alle loro esperienze.

La referente d'Istituto promuove e coordina eventi formativi e informativi dedicati agli alunni, ai genitori e al personale scolastico, realizzati in collaborazione con associazioni, enti locali e Forze dell'Ordine (Polizia Postale, Carabinieri, Servizi sociali, Sportelli psicologici, ecc.).
Tali eventi hanno l'obiettivo di:

- favorire la conoscenza delle norme e dei comportamenti corretti nell'uso delle tecnologie digitali;

- rafforzare le competenze relazionali ed emotive degli studenti per la gestione dei conflitti;
- sensibilizzare le famiglie al ruolo educativo e di vigilanza nella vita online dei figli;
- creare una rete di supporto territoriale stabile per la prevenzione e la gestione dei casi di bullismo e cyberbullismo.

La referente promuove la partecipazione dei docenti ai percorsi di formazione proposti dalla Piattaforma ELISA (E-Learning degli Insegnanti sulle Strategie Antibullismo), iniziativa del Ministero dell'Istruzione e del Merito in collaborazione con l'Università di Firenze e coordina le attività di monitoraggio annuale promosse dalla stessa, volte a rilevare la percezione del fenomeno del bullismo e del cyberbullismo all'interno della scuola.

In occasione del Safer Internet Day, vengono organizzate iniziative di sensibilizzazione rivolte a tutte le componenti scolastiche, in coerenza con le linee guida ministeriali e con i progetti promossi dal Safer Internet Centre – Generazioni Connesse. Le attività includono laboratori e attività didattiche per gli alunni sulla cittadinanza digitale, l'uso consapevole dei social e la prevenzione del cyberbullismo; momenti di riflessione condivisa in aula o in plenaria con visione di materiali multimediali; partecipazione a webinar nazionali o regionali e diffusione di materiali informativi a famiglie e docenti.

Procedure scolastiche in caso di bullismo/cyberbullismo

Quando si viene a conoscenza di un atto che potrebbe configurarsi come bullismo o cyberbullismo, è obbligatorio informare immediatamente il Dirigente Scolastico (D.S.), poiché tali comportamenti possono configurare veri e propri reati, la cui denuncia all'autorità giudiziaria non può essere omessa.

1. Raccolta della segnalazione e analisi del caso
Responsabile: Coordinatore di classe / Insegnante del Consiglio di Classe
Coinvolti: Referente bullismo e cyberbullismo, Referente Dispersione, Psicologo

- Raccolta informazioni, testimonianze e diverse versioni dei fatti;
- Interviste a vittima, presunto autore e gruppo classe;
- Raccolta di prove documentali (luogo, data, modalità);
- Creazione di un clima neutro, empatico e di confronto; astensione da giudizi prematuri.

2. Valutazione dei fatti

- Fatti confermati: si apre un protocollo con modulistica specifica e si definiscono le azioni da intraprendere;
- Fatti non confermati: prosegue il compito educativo ordinario senza interventi specifici.

3. Azioni e provvedimenti
Se i fatti sono confermati:

- Supporto e protezione della vittima, evitando colpevolizzazioni;

- Convocazione delle famiglie e coinvolgimento del Consiglio di Classe per definire strategie e risorse interne/esterne;
- Comunicazione formale al bullo/cyberbullo e scelta dell'ammonimento o provvedimento disciplinare appropriato;
- Eventuali interventi educativi: contratti di collaborazione, attività di riparazione, lettere di scuse, sospensioni o percorsi rieducativi esterni;
- Eventuale attivazione della procedura giudiziaria tramite denuncia alle autorità competenti;
- In caso di mancata collaborazione della famiglia o comportamenti recidivi, segnalazione ai Servizi Sociali.

4. Monitoraggio e consolidamento educativo

- Rafforzamento del percorso educativo all'interno della classe o del gruppo;
- Coinvolgimento dei rappresentanti di classe nella sorveglianza dei comportamenti;
- Monitoraggio dell'efficacia degli interventi sia verso la vittima sia verso il bullo/cyberbullo.

4.2 - Quali strumenti e a chi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

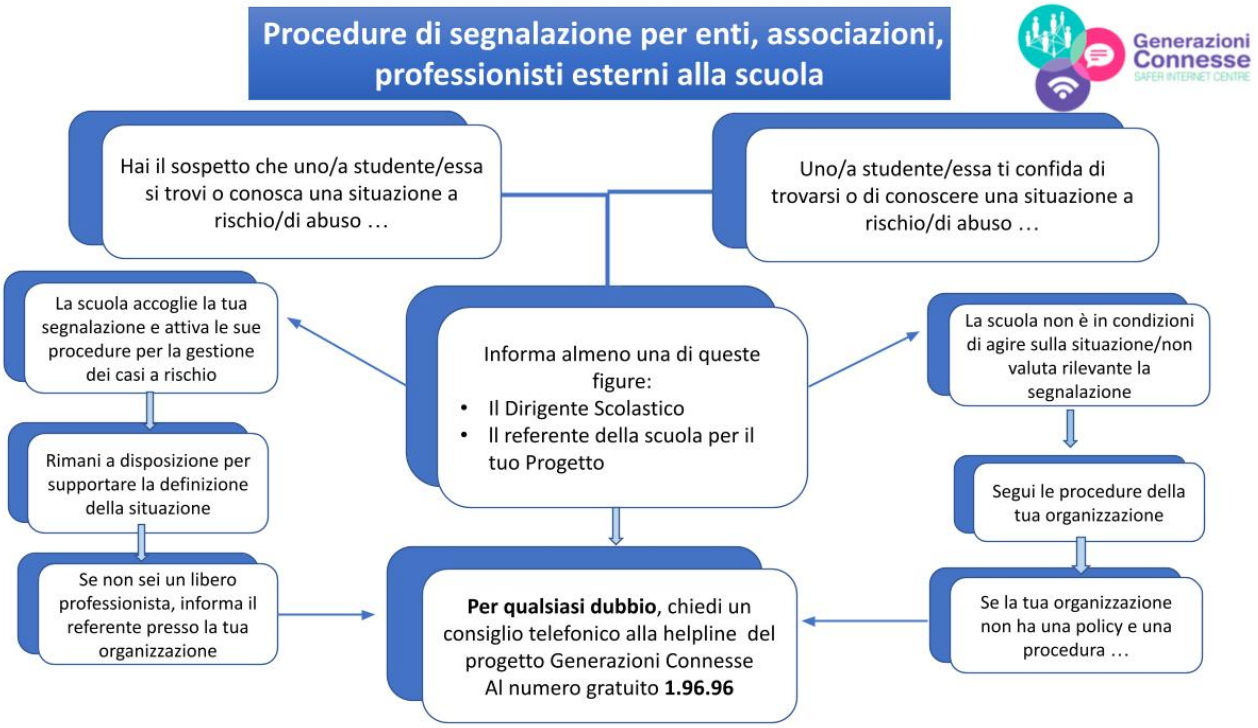
Strumenti a disposizione di studenti/esse

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

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

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

Procedure



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

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

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

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

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

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

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo

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

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

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

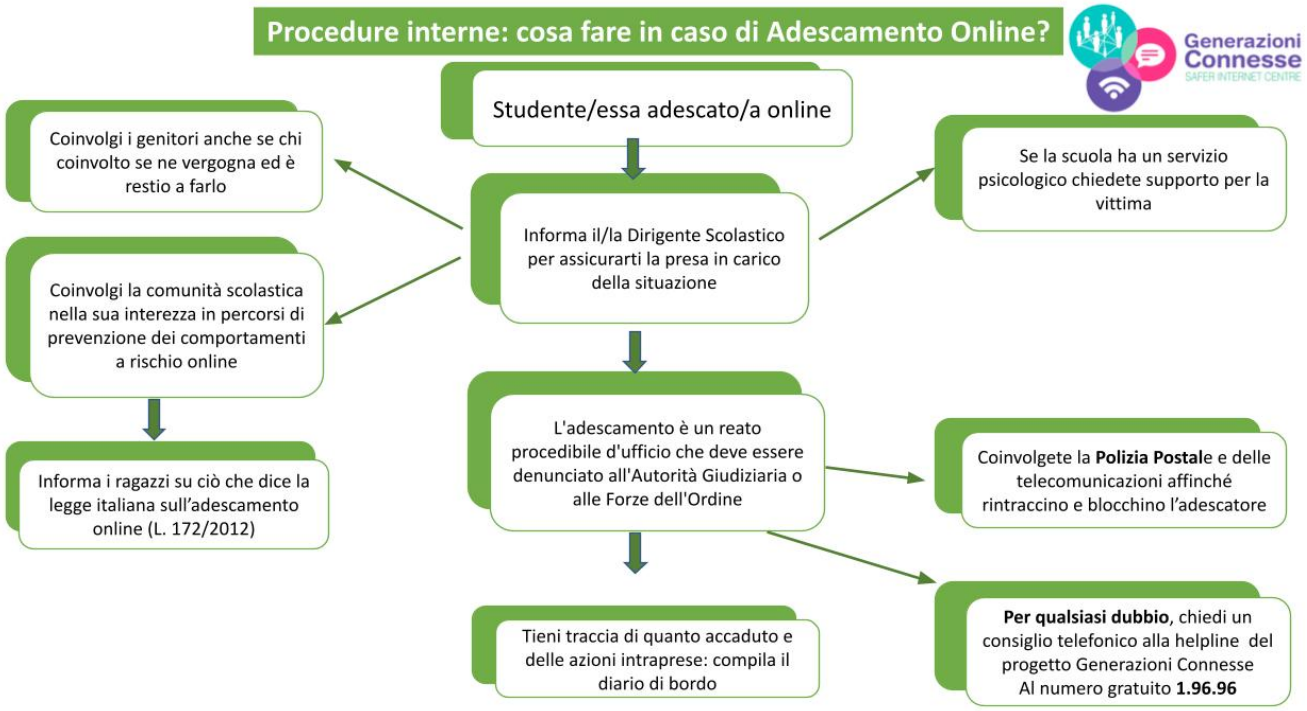
Se emergono evidenze passa allo schema successivo

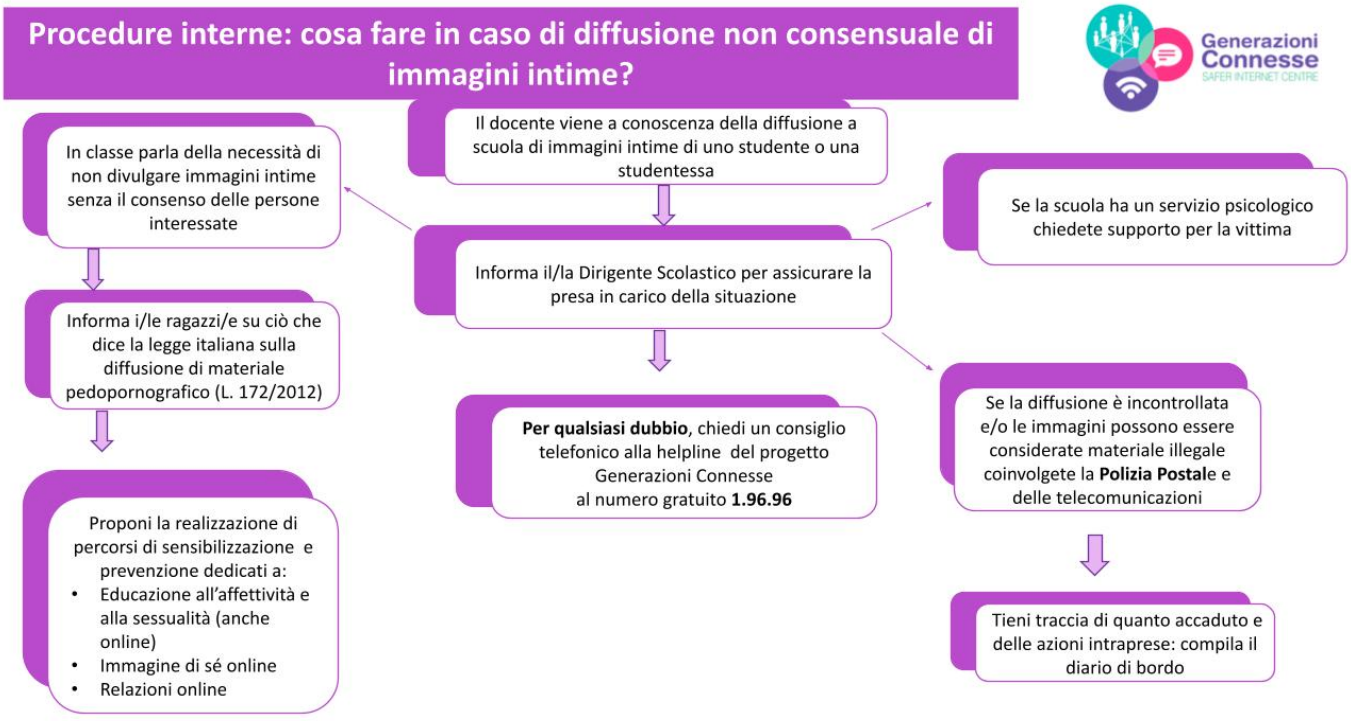
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

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

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

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





L'Istituto Comprensivo "Giuseppe Verdi" dichiara, in maniera chiara e ferma, l'inaccettabilità di qualsiasi forma di prepotenza, di violenza, di sopruso, di bullismo e di cyberbullismo. Attraverso i propri regolamenti, il Patto di corresponsabilità educativa e le strategie educative mirate a costruire relazioni sociali positive l'Istituto coinvolge l'intera comunità educante nel lavoro di prevenzione dei comportamenti problematici, di miglioramento del clima della scuola e di

supporto agli studenti in difficoltà.

IL DIRIGENTE SCOLASTICO:
 individua attraverso il Collegio dei Docenti un referente per il bullismo e il cyberbullismo;
 elabora, in collaborazione con il referente per il bullismo e cyberbullismo, nell'ambito dell'autonomia del proprio istituto, un Regolamento condiviso per il contrasto dei fenomeni di bullismo e cyber bullismo, che preveda sanzioni in un'ottica di giustizia riparativa e forme di supporto alle vittime;
 provvede alla costituzione di un Team Antibullismo e di un Team per l'Emergenza, ovvero di un gruppo di lavoro integrato, costituito da docenti referenti, animatori digitali, dal Dirigente scolastico e da altro personale qualificato e ne coordina le attività;
 adotta, nell'ambito della propria autonomia e in conformità alle Linee di orientamento, un codice interno per la prevenzione e il contrasto dei fenomeni del bullismo e del cyber bullismo;
 si impegna ad istituire un tavolo permanente di monitoraggio del quale fanno parte rappresentanti degli studenti, degli insegnanti , delle famiglie ed esperti di settore;
 promuove interventi di prevenzione primaria e il coinvolgimento degli studenti anche attraverso modalità di peer education;
 coinvolge, nella prevenzione e contrasto al fenomeno del bullismo, tutte le componenti della comunità scolastica, particolarmente quelle che operano nell'area dell'informatica, partendo dall'utilizzo sicuro di Internet a scuola;
 prevede all'interno del PTOF corsi di aggiornamento e formazione in materia di prevenzione dei fenomeni del bullismo e cyberbullismo rivolti al personale docente e Ata;
 promuove sistematicamente azioni di sensibilizzazione dei fenomeni del bullismo e cyberbullismo nel territorio in rete con enti, associazioni, istituzioni locali ed altre scuole, coinvolgendo alunni, docenti, genitori ed esperti;
 favorisce la discussione all'interno della scuola, attraverso i vari organi collegiali, creando i presupposti di regole condivise di comportamento per il contrasto e la prevenzione dei fenomeni di bullismo e cyberbullismo;
 prevede azioni culturali ed educative rivolte agli studenti, per acquisire le competenze necessarie all'esercizio di una cittadinanza digitale consapevole;
 predispone sul sito internet della scuola uno spazio riservato al tema del cyberbullismo in cui raccogliere il materiale informativo e di restituzione dell'attività svolta dalla scuola nell'ambito della prevenzione;
 si attiva nella predisposizione di uno sportello di ascolto "face to face", anche con la collaborazione di personale qualificato esterno;
 avvia, in sede di valutazione, l'istruttoria per accertare se trattasi di caso ascrivibile a bullismo o a "Sindrome di Calimero".

IL REFERENTE DEL BULLISMO E DEL CYBERBULLISMO:
 promuove la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale;
 collabora con gli insegnanti della scuola e propone corsi di formazione al collegio dei docenti;
 coordina i Team Antibullismo e per l'emergenza;
 interviene nelle classi con percorsi specifici di informazione/formazione;

coordina le attività di prevenzione ed informazione sulle sanzioni previste e sulle responsabilità di natura civile e penale, anche con eventuale affiancamento di genitori e studenti;
 si rivolge a partner esterni alla scuola, quali le Forze di polizia, i servizi sociali e sanitari, aziende del privato sociale nonché alle associazioni e ai centri di aggregazione giovanile presenti sul territorio, per realizzare iniziative di prevenzione e contrasto al bullismo e al cyber bullismo;
 cura rapporti di rete fra scuole per eventuali convegni/seminari/corsi e per la giornata mondiale sulla Sicurezza in Internet, la "Safer Internet Day" (SID);
 si attiva per la somministrazione di questionari agli studenti e ai genitori (anche attraverso

piattaforme on line e con la collaborazione di enti esterni) finalizzati al monitoraggio che possano fornire una fotografia della situazione e consentire una valutazione oggettiva dell'efficacia degli interventi attuati;
 promuove la dotazione del proprio istituto di una E - Policy, con il supporto di "Generazioni Connesse".

IL CONSIGLIO D'ISTITUTO
 approva il Regolamento d'istituto e facilita la promozione del Patto di corresponsabilità tra scuola e famiglia.

IL COLLEGIO DEI DOCENTI:
 predispone azioni e attività per la prevenzione dei fenomeni di bullismo e cyberbullismo, comprensive delle azioni di prevenzione primaria/universale e delle azioni indicate rivolte a prendere in carico le situazioni di emergenza nella scuola;
 predispone gli obiettivi nell'area educativa attraverso attività di curricolo di educazione civica e promuove scelte didattiche ed educative, anche in collaborazione con altre scuole in rete, in un'ottica di prevenzione del fenomeno riferendosi a quanto previsto con la L.92/2019 "Introduzione dell'insegnamento dell'Educazione civica", in particolare all'art.3 "Sviluppo delle competenze e obiettivi di apprendimento " e all'art.5 "Educazione alla cittadinanza digitale".

IL CONSIGLIO DI CLASSE o di INTERCLASSE:
 pianifica attività didattiche e/o integrative finalizzate al coinvolgimento attivo e collaborativo degli studenti e all'approfondimento di tematiche che favoriscano la riflessione e la presa di coscienza della necessità dei valori di convivenza civile;
 favorisce un clima collaborativo all'interno della classe e nelle relazioni con le famiglie e propone progetti di educazione alla legalità e alla cittadinanza attiva.

IL PERSONALE DOCENTE:
 interpella e si coordina col Referente per ogni iniziativa o azione di prevenzione e contrasto che preveda la contestualizzazione dei concetti collegati a bullismo e cyberbullismo;