Co-funded by the European Union

Documento di ePolicy
PRIMO LEVI

VIA PALAVERTA 69 - 00040 - MARINO
Roma (RM) - Lazio
Data di approvazione: 21/03/2025 - 11:00

Cap 1 - Lo scopo della ePolicy

1.1 Scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

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

Capitolo 2 - Sensibilizzazione e prevenzione

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

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

Capitolo 4 - Segnalazione e gestione dei casi

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

1.1 Scopo dell'ePolicy

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

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

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

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

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

Attraverso l'E-policy il nostro Istituto intende dotarsi di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento che assicuri un approccio consapevole, critico ed efficace alla tecnologia e che sviluppi, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi ad essa connessi.

L'E-policy fornisce delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse**.**

L'Istituto comprensivo Primo Levi, preso atto del diffuso uso delle TIC nella comunità di riferimento, e ai sensi dell'art. 5 "Educazione alla cittadinanza digitale" della Legge n. 92/2019, si è dotato di una E-policy quale strumento operativo che sia di riferimento per tutta la comunità educante. A tal scopo, attraverso azioni volte alla diffusione di regole di utilizzo e di educazione e formazione su e con le tecnologie, si intende sviluppare una maggiore consapevolezza e sensibilità, evidenziarne le potenzialità e soprattutto i rischi.

Il Documento E-Policy è stato redatto dal gruppo di lavoro composto dai docenti che hanno seguito una formazione online specifica ai fini della redazione di tale documento. Le norme adottate e sottoscritte dalla scuola in materia di sicurezza ed utilizzo delle tecnologie digitali, sono rese note tramite pubblicazione del presente documento sul sito web della scuola. In particolare, fanno parte di questo gruppo di lavoro la Referente d'Istituto per il contrasto ai fenomeni di bullismo e cyberbullismo e l'animaltore digitale.

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.

RESPONSABILITA' DEL DIRIGENTE SCOLASTICO

1. Si impegna a garantire la sicurezza, anche online, di tutti i membri della comunità scolastica.
2. Promuove la cultura della sicurezza online. 3. Ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

RESPONSABILITA' DELL'ANIMATORE DIGITALE

1. Promuove percorsi di formazione interna all'Istituto negli ambiti di sviluppo delle competenze digitali e della media education.
2. Monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola.
3. Controlla che gli utenti (studenti e docenti) usino gli account forniti dall'Istituto e accedano alla Rete della scuola solo per scopi istituzionali e consentiti. (Vedi amministratore Google Workspace)

RESPONSABILITA' DEL REFERENTE DEL BULLISMO E CYBERBULLISMO

Coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo

RESPONSABILITA' DEI DOCENTI

1. Diffondono la cultura dell'uso responsabile delle TIC e della rete.
2. Promuovono l'uso delle tecnologie digitali nella didattica con l'impiego della strumentazione in adozione alla scuola (Digital Board, notebook).

3. Hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

RESPONSABILITA' DEGLI STUDENTI

1. Si impegnano a utilizzare gli strumenti e le tecnologie digitali in coerenza con quanto richiesto dai docenti e nel rispetto delle regole condivise e della netiquette.
2. Si impegnano a condividere online esclusivamente contenuti digitali appropriati, in modo tale da non danneggiare la propria privacy e quella dei compagni.
3. Partecipano a progetti/eventi ed attività che riguardano l'uso responsabile delle TIC e della Rete.

RESPONSABILITA' DEI GENITORI

1. Partecipano alle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete e sull'uso responsabile dei device personali.
2. Comunicano con i docenti circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet.
3. Accettano e condividono quanto scritto nell'e-Policy dell'Istituto.

RESPONSABILITA' DEL TEAM

1. Intervenire (come gruppo ristretto, composto da Dirigente, animatore digitale, referente per il bullismo e il cyberbullismo, referenti degli ordini di scuola, psicologa) nelle situazioni acute di bullismo.
2. Promuovere la redazione e l'applicazione della ePolicy e monitorare le segnalazioni.

RUOLI E RESPONSABILITÀ ENTI EDUCATIVI ESTERNI E ASSOCIAZIONI

Devono conformarsi alla politica dell'e-Policy, riguardo all'uso consapevole della Rete e delle TIC.

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'ePolicy rappresenta un elemento trasversale che deve essere integrato nei principali documenti regolatori e progettuali dell'Istituto Comprensivo Primo Levi, assicurando un approccio strutturato alla cittadinanza digitale e alla sicurezza online.

- Regolamento d'Istituto: sarà aggiornato per includere norme specifiche relative all'uso consapevole e sicuro delle Tecnologie dell'Informazione e della Comunicazione (TIC), richiamando le indicazioni dell'ePolicy e delle Linee Guida Ministeriali.

- Patto di Corresponsabilità Educativa: verrà implementato con riferimenti espliciti all'ePolicy, evidenziando il ruolo della scuola nel promuovere eventi formativi per studenti e genitori, e sottolineando l'impegno delle famiglie nel supportare un uso responsabile della rete e dei dispositivi digitali.

- Piano Triennale dell'Offerta Formativa (PTOF): comprenderà le azioni media-educative connesse all'ePolicy, garantendo percorsi di sensibilizzazione e formazione sulla cittadinanza digitale, la sicurezza in rete e la prevenzione del cyberbullismo.

- Curricolo Verticale d'Istituto: sarà aggiornato per includere riferimenti trasversali all'educazione alla cittadinanza digitale in tutte le discipline, assicurando un approccio sistematico e interdisciplinare alla formazione degli studenti nell'ambito dell'uso responsabile della rete.

- Curricolo Verticale delle Competenze Digitali: strutturato secondo il framework DigComp 2.2 e le Linee Guida di Educazione Civica, dettaglierà un percorso progressivo per sviluppare competenze specifiche legate alla sicurezza informatica, alla protezione dei dati personali, alla netiquette e alla prevenzione dei rischi del web.

- Curricolo di Educazione Civica: integrerà le tematiche dell'ePolicy, inserendo moduli didattici su diritti e doveri digitali, gestione dell'identità online, uso etico delle tecnologie e prevenzione del cyberbullismo, favorendo un approccio attivo e consapevole alla cittadinanza digitale.

- Regolamento per l'uso dei laboratori e delle TIC: includerà disposizioni chiare sull'utilizzo delle risorse digitali e delle infrastrutture tecnologiche dell'istituto, regolamentando l'accesso ai dispositivi e promuovendo pratiche di utilizzo sicuro e responsabile da parte di docenti e studenti.

- Regolamento per il BYOD (Bring Your Own Device): se in futuro l'Istituto adotterà questa modalità, sarà predisposto un regolamento che disciplini l'uso dei dispositivi personali a scuola, garantendo un utilizzo sicuro, inclusivo e conforme alle normative sulla protezione dei dati e sulla sicurezza informatica.

- Regolamento DADA: l'Istituto, adottando il modello Didattica per Ambienti di Apprendimento (DADA), disciplina l'uso degli spazi e delle tecnologie digitali in funzione di un ambiente scolastico flessibile e innovativo. Il regolamento DADA sarà aggiornato per includere riferimenti specifici all'ePolicy, con indicazioni relative alla gestione delle aule

materia, all'uso dei dispositivi digitali personali e scolastici, e alle strategie per promuovere una didattica integrata con strumenti digitali nel rispetto della sicurezza informatica e della protezione dei dati personali.

L'integrazione dell'ePolicy in questi documenti permetterà di consolidare una strategia educativa coerente e condivisa, promuovendo un ambiente scolastico sicuro, inclusivo e responsabile nell'uso delle tecnologie digitali.

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.

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete. Occorre, in tal senso, valorizzare la dimensione relazionale e fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità; promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network; favorire una presa di coscienza critica e costruttiva da parte dei giovani. Inoltre, l'Istituto si potrà avvalere di consulenti/esperti esterni per organizzare incontri formativi rivolti a docenti, genitori ed alunni (Carabinieri, Polizia Postale, equipe Formazione Territoriale del MIUR, associazioni territoriali preposte allo scopo...). La scuola è aperta a tutte le inziative e progetti che intendano sollecitare riflessione e partecipazione attiva per un uso consapevole della rete. Si prodiga per una costruzione di relazioni efficaci, non violente e non prevaricatrici.

Nell'ambito del PNSD questa scuola è dotata dell'Animatore Digitale e del TEAM digitale. Ha previsto formazione dei docenti all'utilizzo delle TIC, in particolare nell'utilizzo di G-Suite. Ha effettuato e continua ad effettuare corsi di formazione e aggiornamento a tutto il personale sulla privacy e gestione di dati sensibili. Ha effettuato e continua ad effettuare una formazione e aggiornamento del personale in materia di sicurezza online. Fornisce informazioni a tutto il nuovo personale circa le indicazioni presenti sulla E-Safety Policy d'Istituto.

Il nostro istituto negli ultimi anni si è impegnato nell'attuazione del PNSD ("Piano Nazionale Scuola Digitale"), aderendo ai bandi PON, investendo in infrastrutture, sperimentando nuove metodologie didattiche e impegnandosi in un percorso continuo di formazione del personale docente ed amministrativo. Per permettere la realizzazione di una nuova didattica in grado di sfruttare le potenzialità delle ICT, viene messo a disposizione degli alunni e di tutto il personale quanto serve per accedere a internet, lavorare, comunicare e collaborare avvalendosi delle nuove tecnologie. Per garantire la sicurezza nelle ICT l'Istituto adotta le seguenti strategie: Individuazione, di norma all'interno dell'ufficio tecnico, di un responsabile della sicurezza informatica in grado di monitorare l'utilizzo della rete; uso di un firewall hardware in grado di proteggere le reti locali e monitorare gli accessi ad internet implementando funzionalità proxy; controllo del sistema informatico della scuola al fine di prevenire e/o rimediare a possibili disfunzioni dell'hardware o del software, come di difesa preventiva da attacchi informatici ed intrusioni dall'esterno e di immissione di virus nelle reti LAN (Local Area Network) della scuola; utilizzo di un software antivirus aggiornato costantemente; uso di filtri nella navigazione preimpostati attraverso il proxy/firewall; uso di VLAN per regolamentare l'accesso ad Internet per ambienti e categorie di utenti; separazione fisica della rete didattica da quella amministrativa; individuazione di un amministratore di rete per ogni rete LAN; Gestione dei dati nel rispetto delle Misure minime di sicurezza ICT per le pubbliche amministrazioni (documento depositato presso la segreteria); regolamentazione dell'utilizzo dei laboratori di informatica e dei dispositivi informatici WiFI all'interno delle classi. La formazione del curricolo digitale tiene conto di quanto disposto dall'art. 5 della legge 20 agosto 2019 n. 92 (Introduzione dell'insegnamento scolastico dell'educazione civica) dedicato alla "Cittadinanza Digitale" intesa come capacità di un individuo di avvalersi consapevolmente e responsabilmente dei mezzi di comunicazione virtuali.

Nell'ambito del PNSD questa scuola propone un programma di educazione alla sicurezza online come parte integrante del curriculum scolastico. Si impegna a sviluppare una serie di competenze e comportamenti adeguati all'età degli alunni e ad esperienza, tra cui:

•Programmare attività e far partecipare gli alunni a laboratori specifici sul digitale e la sicurezza in rete

• Sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettare l'esattezza

• Essere a conoscenza delle fonti delle notizie in rete e che l'autore di un post o un sito web/pagina può avere un particolare pregiudizio

• Sapere come restringere o affinare una ricerca

• Riconoscere un comportamento accettabile quando si utilizza un ambiente online, vale a dire, essere educato, non utilizzare comportamenti inappropriati, mantenere le informazioni personali private

• Conoscere e seguire la netiquette

• Capire come le fotografie possano essere manipolate e individuare contenuti web in grado di attrarre il tipo sbagliato di attenzione

• Comprendere l'esistenza e saper riconoscere i profili fake e le false identità degli interlocutori in chat e social network

• Capire il motivo per cui non dovrebbero inviare o condividere resoconti dettagliati delle loro vite personali e informazioni di contatto

• Capire il motivo per cui non devono pubblicare foto o video di altri senza permesso

• Comprendere la motivazione del divieto di utilizzo dei cellulari a scuola

• Comprendere l'importanza di non scaricare file, software coperti da copyright o di dubbia natura

• Conoscere e contrastare i fenomeni di bullismo e cyberbullismo in tutte le sue forme.

• Sapere come chiedere aiuto e segnalare atti di bullismo e cyberbullismo

• Utilizzare con attenzione Internet per garantire che si adatti alla loro età e supporti gli obiettivi di apprendimento per le aree curricolari specifiche

• Conoscere e saper utilizzare positivamente le potenzialità delle nuove tecnologie e del mondo digitale.

Relativamente agli strumenti di comunicazione e agli ambienti di apprendimento il nostro istituto opera su tre livelli di comunicazione online: 1. Comunicazione istituzionale - Sito web: Il nuovo sito dell'Istituto, aggiornato con l'adeguamento alle norme di accessibilità, oltre a offrire una visione d'insieme dell'Istituto, permette, utilizzando l'account personale, l'accesso a documenti e servizi riservati alle diverse categorie di utenti. Circolari. 2. Comunicazione didattica - Didattica Digitale Integrata (Google Workspace): A partire dall'anno scolastico 2019-2020, l'Istituto ha attivato la piattaforma Google Workspace for Education (ex. GSuite for Education), un insieme di applicativi i cui servizi sono stati progettati per ottimizzare la circolazione delle informazioni interne, favorire la creazione di archivi di materiale didattico e stimolare in modo specifico gli apprendimenti attraverso le nuove tecnologie all'interno di un ambiente cloud sicuro; I servizi di questa piattaforma didattica hanno un valore inclusivo per gli studenti, in quanto consentono loro di imparare a lavorare in modo collaborativo e compartecipato, tenendo conto delle capacità di ciascuno. Sempre attraverso Google Workspace viene fornito al personale, agli studenti e ai genitori, un account personale per accedere ai servizi cloud e alle applicazioni specifiche (Classroom, Meet, Gmail, Gdrive, ecc.). In relazione all'utilizzo di questa piattaforma l'Istituto si è dotato di un Piano per la Didattica Digitale Integrata che individua le modalità di attuazione della Didattica digitale integrata dell'Istituto. 3. Comunicazione all'interno della comunità scolastica - il registro elettronico (AXIOS): Strumento che apre un canale di comunicazione scuola/famiglia privilegiato per tutte quelle informazioni relative all'andamento scolastico, alla partecipazione e al rendimento didattico. Anche per questo strumento vengono fornite a docenti, studenti e genitori specifici account con funzionalità e viste sui dati differenti e si ribadisce l'importanza della riservatezza. In particolare ai genitori si raccomanda di non cedere le proprie credenziali ai figli per non pregiudicare la corretta fruizione delle informazioni scuola/famiglia.

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

Negli ultimi anni sono state svolte le seguenti attività:

Creazione del gruppo di lavoro ePolicy; presentazione del documento ePolicy al collegio dei docenti; esecuzione, tramite lo strumento di auto-valutazione europeo SELFIE, della raccolta dati sull'attuale livello di efficacia dell'utilizzo delle tecnologie digitali; somministrazione ai docenti del questionario di monitoraggio dei fenomeni di bullismo e cyberbullismo attraverso a piattaforma ELISA; partecipazione attiva alle giornate del Safer Internet Day; progetto "benessere a scuola" finanziato dalla Regione Lazio per il triennio 2023-2025 grazie al quale abbiamo potuto attivare molteplici attività sulla gestione delle emozioni, comunicazione e relazione efficace, educazione all'affettività, formazione sul bullismo e cyberbullismo, educazione e contrasto alle forme di prevaricazione nella scuola dell'infanzia. Partecipazione al progetto Bulli Stop. Incontri con esperti esterni sul codice rosso, il sexting e il revenge porn. Restituzione del lavoro svolto da parte del Team al Collegio docenti. Incontri strutturati con personale scolastico, famiglie e studenti organizzati dall'amministrazione comunale; Progetto "cappuccetto rotto" con l'associazione "La Terzina";

Per il prossimo triennio si intendono pianificare incontri con consulenti esterni rivolti agli studenti, genitori, docenti e personale ATA relativamente al contrasto bullismo e cyberbllismo; Si prevede di effettuare una disseminazione delle definizioni, strategie di intervento e attività di prevenzione con tutta la comunità educante. Si procederà a rinnovare la documentazione, i protocolli e le schede di segnalazione casi che verranno pubblicati in area apposita del sito della scuola. Si proseguirà con le azioni già avviate e consolidate.

Azioni da svolgere entro un'annualità scolastica: condividere collegialmente con i docenti le azioni svolte e le modifiche previste al documento; presentare agli studenti il documento della ePolicy e le procedure ad esso connesse; organizzare il coinvolgimento attivo dei docenti interessati attraverso attività di formazione legate alle piattaforme Generazioni Connesse e Elisa; abbiamo pianificato incontri con le forze dell'ordine in tema sicurezza. A partire dalla scuola primaria, la scuola invita i genitori ad assumersi l'incarico di accompagnare e supervisionare i figli durante la navigazione in rete, aiutandoli a riconoscere ed evitare i rischi. Inoltre la scuola

si assume i compiti di:

• Presentare ai genitori il Regolamento della Policy, al fine di garantire che i principi di comportamento sicuro online siano chiari • Mettere a disposizione dei genitori e degli alunni una mail per informazioni, segnalazioni e supporto

• Gestire e aggiornare costantemente una sezione dedicata sul sito internet della scuola

• Fornire informazioni sui siti nazionali di sostegno per i genitori, quali il sito www.generazioniconnesse.it

• Fornire uno sportello di ascolto psicologico gratuito

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete. Occorre, in tal senso, valorizzare la dimensione relazionale e fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità; promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network; favorire una presa di coscienza critica e costruttiva da parte dei giovani. Inoltre, l'Istituto si potrà avvalere di consulenti/esperti esterni per organizzare incontri formativi rivolti a docenti, genitori ed alunni (Carabinieri, Polizia Postale, equipe Formazione Territoriale del MIUR, associazioni territoriali preposte allo scopo...).La scuola è aperta a tutte le inziative e progetti che intendano sollecitare riflessione e partecipazione attiva per un uso consapevole della rete. Si prodiga per una costruzione di relazioni efficaci, non violente e non prevaricatrici.

La formazione del curricolo digitale tiene conto di quanto disposto dall'art. 5 della legge 20 agosto 2019 n. 92 (Introduzione dell'insegnamento scolastico dell'educazione civica) dedicato alla "Cittadinanza Digitale" intesa come capacità di un individuo di avvalersi consapevolmente e responsabilmente dei mezzi di comunicazione virtuali.

Nell'ambito del PNSD questa scuola è dotata dell'Animatore Digitale e del TEAM digitale. Ha previsto formazione dei docenti all'utilizzo delle TIC, in particolare nell'utilizzo di G-Suite. Ha effettuato e continua ad effettuare corsi di formazione e aggiornamento a tutto il personale sulla privacy e gestione di dati sensibili. Ha effettuato e continua ad effettuare una formazione e aggiornamento del personale in materia di sicurezza online. Fornisce informazioni a tutto il nuovo personale circa le indicazioni presenti sulla E-Safety Policy d'Istituto.

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

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

Il nostro Istituto si avvale di tutti gli strumenti messi a disposizione dalla piattaforma generazioni connesse, dalla piattaforma Elisa, si avvale della documentazione fornita dal Ministero, comprese le linee guida e aggiornamenti. Partecipa ogni anno al SIF.

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.

Nell'ambito del PNSD questa scuola si propone un programma di progressiva educazione alla sicurezza online come parte del curriculum scolastico. Si impegna a sviluppare una serie di competenze e comportamenti adeguati all'età degli alunni e ad esperienza, tra cui: • Programmare attività e far partecipare gli alunni a laboratori specifici sul digitale e la sicurezza in rete • Sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettare l'esattezza • Essere a conoscenza delle fonti delle notizie in rete e che l'autore di un post o un sito web/pagina può avere un particolare pregiudizio • Sapere come restringere o affinare una ricerca • Riconoscere un comportamento accettabile quando si utilizza un ambiente online, vale a dire, essere educato, non utilizzare comportamenti inappropriati, mantenere le informazioni personali private • Conoscere e seguire la netiquette • Capire come le fotografie possono essere manipolate e individuare contenuti web in grado di attrarre il tipo sbagliato di attenzione • Comprendere l'esistenza e saper riconoscere i profili fake e le false identità degli interlocutori in chat e social network • Capire il motivo per cui non dovrebbero inviare o condividere resoconti dettagliati delle loro vite personali e informazioni di contatto • Capire il motivo per cui non devono pubblicare foto o video di altri senza permesso • Comprendere la motivazione del divieto di utilizzo dei cellulari a scuola • Comprendere l'importanza di non scaricare file, software coperti da copyright o di dubbia natura • Conoscere e contrastare i fenomeni di bullismo e cyberbullismo in tutte le sue forme. • Sapere come chiedere aiuto e segnalare atti di bullismo e cyberbullismo • Utilizzare con attenzione Internet per garantire che si adatti alla loro età e supporti gli obiettivi di apprendimento per le aree curricolari specifiche • Conoscere e saper utilizzare positivamente le potenzialità delle nuove tecnologie e del mondo digitale. Il nostro Istituto nell'ottica di un processo di sensibilizzazione e prevenzione dei rischi connessi all'uso improprio delle tecnologie digitali, ha adottato un Regolamento specifico per la prevenzione e il contrasto del bullismo e cyberbullismo, ai sensi della Legge 71 del 29 maggio 2017. Si propongono costantemente attività che prevedono l'acquisizione di competenze perun uso consapevole delle nuove tecnologie digitali, per prevenire i rischi correlati ad un loro uso scorretto o addirittura illecito. Inoltre ha potenziato lo "Sportello di ascolto" di Istituto e promosso interventi specifici in tutti gli ordini di scuola. Nell'ultimo triennio, grazie all'aggiudicazione di un bando della Regione Lazio, abbiamo strutturato un progetto con esperti esterni "benessere a scuola" con l'obiettivo di fornire agli studenti e alle famiglie strumenti per costruire relazioni efficaci e non prevaricatrici, educazione alla sessualità e all'affettività e per la promozione del rispetto della diversità: rispetto delle differenze di genere e di orientamento e identità sessuale con particolare attenzione ai rischi connessi al digitale.

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono

quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete. Occorre, in tal senso, valorizzare la dimensione relazionale e fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità; promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network; favorire una presa di coscienza critica e costruttiva da parte dei giovani. Inoltre, l'Istituto si avvale di consulenti/esperti esterni per organizzare incontri formativi rivolti a docenti, genitori ed alunni (Carabinieri, Polizia Postale, equipe Formazione Territoriale del MIUR, associazioni territoriali preposte allo scopo...).

La nostra scuola presta particolare attenzione ai segnali comportamentali degli studenti e delle studentesse da cui si può evincere un attaccamento morboso al gioco online, l'abuso di navigazione virtuale, interazioni e relazioni aggressive e volgari, informando preventivamente i genitori e, nei casi di dipendenza più gravi, rinviando allo Sportello di Ascolto per l'adozione di un intervento personalizzato. Gli elementi che contribuiscono al benessere digitale sono: la ricerca di equilibrio nelle relazioni anche online, l'uso degli strumenti digitali per il raggiungimento di obiettivi di accrescimento personale, la capacità di interagire negli ambienti digitali in modo sicuro e responsabile, la capacità di gestire il sovraccarico informativo e le distrazioni.

È importante che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Fondamentale quindi, è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è). Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi tempestivamente, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video...).

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.

L'Istituto Comprensivo "Primo Levi" ha recentemente aggiornato il Curricolo Verticale delle Competenze Digitali, riconoscendo l'educazione digitale come un elemento imprescindibile per formare cittadini consapevoli e autonomi. Il nuovo curricolo si allinea alle indicazioni più recenti, ispirandosi al framework europeo DigComp 2.2 e recependo le Linee Guida per l'educazione civica 2024 (D.M. 183/2024). L'obiettivo è accompagnare gli studenti in un percorso di crescita progressiva nell'acquisizione di competenze digitali che vanno oltre l'uso degli strumenti informatici, investendo aspetti fondamentali della vita quotidiana e della cittadinanza attiva. Il curricolo mira a fornire agli alunni strumenti adeguati per affrontare le sfide della società dell'informazione in modo critico e responsabile.

Cittadinanza Digitale ed ePolicy

Un elemento chiave dell'aggiornamento è l'integrazione dell'ePolicy d'istituto all'interno del curricolo digitale. L'ePolicy è un documento programmatico scolastico che definisce:

- Approccio formativo alle competenze digitali e alla sicurezza online, che promuove un uso costruttivo delle tecnologie in ambito didattico.
- Norme di comportamento e procedure per l'impiego delle tecnologie dell'informazione e comunicazione a scuola.
- Misure di prevenzione rispetto a rischi e problematiche digitali.
- Procedure di rilevazione e gestione di eventuali situazioni problematiche derivanti da un uso non consapevole delle tecnologie.

Integrare l'ePolicy nel curricolo garantisce quindi un approccio strutturato alla cittadinanza digitale e alla sicurezza online. Questo documento condiviso diventa un riferimento per l'intera comunità scolastica (studenti, docenti e famiglie) e rientra nelle azioni di sensibilizzazione e prevenzione promosse dall'Istituto. In tal modo si contribuisce a sviluppare negli studenti una maggiore consapevolezza sia dei rischi sia delle opportunità del mondo digitale, favorendo comportamenti responsabili.

Percorso Didattico Verticale e Interdisciplinare

Con l'intregrazione dell'e-policy, il Curricolo Verticale delle Competenze Digitali prevedrà attività didattiche calibrate per ogni classe ed età, con momenti formativi specifici e l'impiego di kit didattici per facilitare l'apprendimento delle tematiche digitali. Il percorso di apprendimento ha carattere interdisciplinare e progressivo, coinvolgendo tutte le materie: il digitale non viene trattato come ambito separato, ma come elemento integrato nelle diverse aree del sapere. Ciò significa che ogni disciplina può concorrere allo sviluppo delle competenze digitali, evitando di relegarle a un solo corso. Man mano che gli studenti avanzano negli anni, le attività proposte aumentano in complessità e gli alunni acquisiscono una crescente autonomia nell'uso critico e consapevole della tecnologia. Questo approccio trasversale assicura che le competenze digitali si sviluppino in continuità lungo tutto il percorso scolastico, valorizzando connessioni tra saperi diversi.

Le cinque aree di competenza DigComp 2.2

Le competenze digitali sviluppate nel curricolo si articolano secondo le cinque aree chiave del framework DigComp 2.2:

1. Alfabetizzazione su informazioni e dati – Saper cercare, comprendere, valutare criticamente e gestire le informazioni online.
2. Comunicazione e collaborazione – Utilizzare piattaforme e strumenti digitali in modo sicuro e responsabile per comunicare e lavorare con gli altri.
3. Creazione di contenuti digitali – Sviluppare la capacità di produrre nuovi contenuti in formato digitale, rispettando norme di copyright e principi etici.
4. Sicurezza – Proteggere i propri dispositivi e dati personali, garantire la sicurezza informatica e gestire in modo consapevole la propria identità digitale.
5. Risolvere problemi – Affrontare problemi e sfide utilizzando gli strumenti tecnologici, sviluppando il pensiero computazionale e strategie efficaci di problem solving.

Queste aree tematiche assicurano che il curricolo copra tutte le dimensioni della competenza digitale cittadina, dal saper navigare tra le informazioni al saper interagire online, fino al padroneggiare la tecnologia come mezzo per innovare e

risolvere problemi. Ogni area viene declinata in obiettivi di conoscenza, abilità e atteggiamenti adeguati all'età degli studenti, costruendo basi solide fin dalla scuola dell'infanzia fino al termine del ciclo.

Focus sul Coding e il Pensiero Computazionale

Nel nuovo curricolo viene dedicata particolare attenzione al coding, riconosciuto come attività fondamentale per sviluppare il pensiero computazionale e le capacità di problem solving. Sin dai primi anni, agli studenti vengono proposte esperienze di programmazione (anche unplugged e attraverso giochi didattici) per stimolare un approccio logico-creativo alla risoluzione dei problemi. Il coding infatti aiuta i ragazzi a scomporre problemi complessi in parti affrontabili, a pianificare soluzioni passo-passo e a perseverare di fronte alle sfide – competenze trasferibili anche al di fuori dell'informatica. Questo focus sul coding, progressivamente approfondito nel corso degli studi, mira a formare menti creative e logiche, capaci di capire il funzionamento delle tecnologie e non solo di utilizzarle passivamente.

Privacy, Cyberbullismo e Disinformazione

Un altro aspetto centrale è l'educazione alla cittadinanza digitale responsabile. Il curricolo include momenti di riflessione e attività specifiche su temi quali la privacy dei dati, il cyberbullismo e la disinformazione online, in piena coerenza con le azioni di prevenzione promosse dall'Istituto. L'obiettivo è formare gli studenti a un uso critico e sicuro delle tecnologie digitali, fornendo strategie per riconoscere i pericoli della rete e comportamenti corretti per evitarli. Ciò risponde alla necessità di prevenire fenomeni negativi del web (fake news, bullismo digitale, violazioni della riservatezza), ma anche di far comprendere agli alunni l'importanza di tutelare i propri dati personali e la propria reputazione online. Attraverso discussioni guidate, casi di studio e simulazioni, i ragazzi imparano a valutare l'attendibilità delle fonti, a gestire in modo sicuro le interazioni sui social network e a sviluppare empatia e rispetto nelle comunicazioni digitali. Questo segmento formativo contribuisce a creare un ambiente scolastico digitale più sicuro e inclusivo, dove gli studenti si sentono informati e protetti.

Conclusioni

In sintesi, l'integrazione dell'ePolicy nel Curricolo Verticale delle Competenze Digitali dell'I.C. Primo Levi fa sì che le regole e i principi per l'uso consapevole della tecnologia diventino parte integrante del percorso educativo quotidiano. Grazie a questo approccio, gli studenti acquisiscono competenze sempre più avanzate nell'uso responsabile degli strumenti digitali, rafforzando al contempo la propria autonomia digitale. Il curricolo aggiornato intende guidare i ragazzi a diventare protagonisti attivi del loro apprendimento e cittadini digitali maturi, consapevoli delle opportunità e delle sfide offerte dal mondo connesso. Questa preparazione permetterà loro di affrontare il futuro con maggiore consapevolezza, spirito critico e sicurezza, pronti a utilizzare le tecnologie non solo con competenza tecnica ma anche con senso etico e civico.

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.

È importante riconoscere alcuni dei rischi on-line, saperli distinguere in modo da poter adottare le strategie migliori per arginarli e contenerli.

CYBERBULLISMO: CHE COS'È?

Qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo. [legge 71/2017 e legge 70/2024 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo].

CYBERBULLISMO: COME PREVENIRLO? Nomina del Referente per le iniziative di prevenzione e contrasto che:

• ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo;

• può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio; • supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, Rav...).

HATE SPEECH: CHE COS'È E COME PREVENIRLO

Indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, genere o di orientamento sessuale, di disabilita, eccetera) ai danni di una persona o di un gruppo. Azioni che il nostro Istituto intende intraprendere in relazione a questa problematica: 1. fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, legati alla razza, al genere, all'orientamento sessuale, alla disabilita; 2. promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network; 3. favorire una presa di parola consapevole e costruttiva da parte dei giovani.

DIPENDENZA DA INTERNET E GIOCO ONLINE

Fa riferimento all'utilizzo eccessivo e incontrollato di Internet che può causare isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete. Azioni che il nostro Istituto intende intraprendere in relazione a questa problematica: • fornire al personale della scuola, agli studenti e alle loro famiglie strumenti finalizzati al riconoscimento e alla prevenzione del fenomeno.

SEXTING Indica un fenomeno, molto frequente fra i giovanissimi, che consiste nello scambio di contenuti mediali sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video. Azioni che il nostro Istituto intende intraprendere in relazione a questa problematica: 1. fornire al personale della scuola, agli studenti e alle loro famiglie strumenti finalizzati al riconoscimento e alla prevenzione del fenomeno; 2. formazione degli studenti sui rischi del sexting, legati al revenge porn, che possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione.

ADESCAMENTO ONLINE Rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro. I luoghi virtuali in cui si sviluppano maggiormente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (WhatsApp, Telegram etc.), i siti e le app di teen dating (siti di incontri per adolescenti). Azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata

problematica dell'adescamento: 1. fornire al personale della scuola, agli studenti e alle loro famiglie strumenti finalizzati al riconoscimento e alla prevenzione del fenomeno; 2. predisposizione per gli studenti di percorsi guidati su educazione all'affettività e alla sessualità, anche attraverso il ricorso a medici e psicoterapeuti specializzati.

PEDOPORNOGRAFIA La pedopornografia online è un reato che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, concrete o simulate o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali. Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse. Qualora navigando in Rete si incontri materiale pedopornografico e opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione "Segnala contenuti illegali" (Hotline).

Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children.

https://www.commissariatodips.it/

https://azzurro.it/

https://www.generazioniconnesse.it/site/it/home-page/

https://www.amnesty.it/appelli/stop-alla-violenza-online-su-toxictwitter/

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

3.1 - Protezione dei dati personali e GDPR

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

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

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

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

La protezione dei dati personali costituisce un diritto fondamentale, sancito dall'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione Europea e dall'art. 16, par. 1, del Trattato sul funzionamento dell'Unione Europea (TFUE). Le principali normative di riferimento per il trattamento dei dati personali nel settore scolastico sono il Regolamento Generale sulla Protezione dei Dati 2016/679 (GDPR) e il D.Lgs. 196/2003, noto come Codice Privacy.

L'Istituto Comprensivo Primo Levi è fortemente orientato all'innovazione didattica e da tempo utilizza metodologie che prevedono l'integrazione delle nuove tecnologie nel processo di insegnamento e apprendimento. A seguito della pandemia, l'Istituto ha adottato la piattaforma Google Workspace for Education, un ambiente di apprendimento digitale conforme al GDPR, come indicato nei Termini di Servizio e nella Google Cloud Data Processing Addendum (DPA), che garantiscono il rispetto degli standard europei in materia di protezione dei dati personali.

Google Workspace for Education è stato scelto perché il suo utilizzo da parte delle scuole non comporta il trattamento su larga scala di dati personali né l'impiego di tecnologie invasive, come chiarito dal Considerando 91 del GDPR. Inoltre, i dati degli utenti vengono trattati con elevati standard di sicurezza e nel rispetto dei principi di minimizzazione e protezione dei dati personali.

Gestione degli account e trattamento dei dati personali

- Per ogni alunno dell'Istituto, all'inizio dell'anno scolastico, viene creato un account personale all'interno di Google Workspace for Education.
- Per ragioni di sicurezza e tutela della privacy, gli account degli alunni utilizzano un dominio dedicato, separato da quello ufficiale dell'Istituto, evitando così l'associazione diretta con eventuali dati personali.
- L'account consente l'accesso ai servizi base di Google Workspace, tra cui Classroom, Gmail, Documenti, Drive, Moduli e Meet.

- I servizi aggiuntivi di Google (es. YouTube, Google Earth, ecc.) non sono attivati di default, ma vengono abilitati solo previa autorizzazione scritta dei genitori o di chi esercita la responsabilità genitoriale.
- I servizi di terze parti per gli studenti non vengono attivati, garantendo così un maggiore controllo sulla gestione dei dati personali.
- All'inizio del percorso scolastico, le famiglie firmano una liberatoria per l'uso dei servizi Google Workspace for Education; solo dopo la firma vengono comunicate le credenziali di accesso dell'alunno.
- L'account rimane attivo per tutta la durata della carriera scolastica dell'alunno nell'Istituto (dalla scuola dell'infanzia alla scuola secondaria di primo grado).
- Alla fine del percorso scolastico o in caso di trasferimento dell'alunno, l'account viene eliminato, e i materiali didattici prodotti vengono archiviati nel drive dell'amministratore di sistema, secondo le procedure previste per la conservazione dei dati.

Ruoli e responsabilità

- Il Responsabile della Protezione dei Dati (RPD o DPO), designato dall'Istituto in conformità con l'art. 37 del GDPR, monitora il rispetto della normativa sulla protezione dei dati personali e fornisce consulenza sulle misure di sicurezza da adottare.
- La gestione della piattaforma Google Workspace for Education è affidata all'Animatore Digitale, che garantisce il corretto funzionamento degli strumenti digitali e il rispetto delle procedure di sicurezza.

Questa organizzazione garantisce che l'Istituto Comprensivo Primo Levi adotti un approccio responsabile alla protezione dei dati, in conformità con il GDPR, tutelando la privacy di studenti e docenti nell'ambiente scolastico digitale.

3.2 - Strumenti di comunicazione online (PUA)

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

Politica di Uso Accettabile e Responsabile della Rete (P.U.A.)

L'Istituto Comprensivo Primo Levi riconosce l'importanza della Politica di Uso Accettabile e Responsabile della Rete (P.U.A.) nella costruzione di una cittadinanza digitale consapevole e responsabile. Per questo motivo, si impegna a dotarsi di un documento strutturato che regolamenti l'uso delle tecnologie digitali e della rete all'interno dell'ambiente scolastico.

Alcuni principi e regolamenti che saranno formalizzati nel P.U.A. sono già stati integrati nel Curricolo Verticale delle Competenze Digitali, con particolare attenzione alla tutela della privacy, al diritto d'autore e alla sicurezza in rete.

Obiettivi e finalità della P.U.A.

La P.U.A. dell'Istituto si propone di:

- Promuovere un uso sicuro e consapevole di Internet da parte di studenti, docenti e personale scolastico.
- Sensibilizzare gli utenti sui rischi connessi alla navigazione online, come il cyberbullismo, le violazioni della privacy e il furto di dati personali.
- Definire norme e comportamenti responsabili nell'uso della rete, nel rispetto del regolamento scolastico e delle normative vigenti.
- Garantire la protezione dei dati personali e il rispetto della normativa GDPR.

Regole di impiego della rete e delle tecnologie digitali che verranno integrate nella PUA

L'impiego della rete scolastica e delle TIC (Tecnologie dell'Informazione e della Comunicazione) da parte di studenti e personale dell'Istituto è regolato da principi di sicurezza, responsabilità e rispetto delle normative vigenti.

1. Accesso alla rete e ai dispositivi scolastici

- L'accesso a Internet è consentito esclusivamente per scopi didattici e istituzionali.
- È vietato accedere a siti web non idonei all'ambiente educativo o che promuovano contenuti inappropriati.
- L'uso delle TIC è subordinato al rispetto delle regole stabilite nel regolamento scolastico e nel Regolamento per l'uso dei laboratori e delle TIC.
- L'utilizzo della rete e dei dispositivi scolastici è monitorato e tracciato per garantire la sicurezza degli utenti.

2. Uso degli account e delle piattaforme digitali

- Ogni studente e membro del personale docente ha un account istituzionale su Google Workspace for Education, che segue le linee guida GDPR per la protezione dei dati personali.
- L'uso dei servizi Google è regolato da un sistema di autorizzazione preventiva da parte delle famiglie per gli studenti minorenni.
- I servizi di terze parti non vengono attivati per gli studenti, salvo autorizzazione specifica.

3. Netiquette e comportamento online

- Gli utenti devono rispettare le regole di Netiquette, adottando un comportamento corretto, responsabile e rispettoso nelle interazioni online.
- È vietato:
  - Diffondere informazioni personali proprie o altrui senza autorizzazione.
  - Accedere senza permesso a risorse informatiche riservate.
  - Utilizzare la rete per diffondere contenuti offensivi, discriminatori o illegali.
  - Condividere o scaricare materiali protetti da diritto d'autore senza autorizzazione.
- In caso di violazioni, si applicano le sanzioni previste dal regolamento scolastico.

4. Sicurezza e protezione dei dati personali

- Tutti gli utenti devono seguire le disposizioni del GDPR e del Codice Privacy (D.Lgs. 196/2003) per la tutela dei dati personali.
- I docenti sono responsabili nel guidare gli studenti verso un utilizzo sicuro della rete, spiegando come proteggere la propria identità digitale e riconoscere le minacce online.
- La scuola utilizza filtri di navigazione per limitare l'accesso a contenuti inappropriati e garantire un ambiente digitale sicuro.

5. Uso dei dispositivi personali (BYOD - Bring Your Own Device)

- Al momento, per ragioni infrastrutturali, l'Istituto non ha attivato la modalità BYOD (Bring Your Own Device).
- Qualora in futuro l'uso dei dispositivi personali venisse consentito, sarà predisposto un Regolamento specifico per disciplinarne l'uso nel rispetto della sicurezza e della privacy.

Responsabilità e sanzioni

L'utilizzo della rete e delle TIC all'interno dell'Istituto deve avvenire nel rispetto delle regole stabilite. In caso di violazioni:

- L'accesso alla rete o ai servizi digitali dell'Istituto potrà essere sospeso temporaneamente o revocato.
- In caso di comportamenti gravi, il Consiglio di Classe e il Dirigente Scolastico potranno adottare provvedimenti disciplinari in linea con il regolamento d'Istituto.
- Eventuali violazioni delle normative potranno essere segnalate alle autorità competenti in caso di reati informatici o cyberbullismo.

Conclusioni

L'adozione della Politica di Uso Accettabile e Responsabile della Rete (P.U.A.) rappresenta un passo fondamentale per la tutela della sicurezza digitale della comunità scolastica. La scuola si impegna a promuovere la cittadinanza digitale attraverso percorsi formativi specifici, in continuità con le azioni previste nel Curricolo Verticale delle Competenze Digitali e nelle linee guida per l'Educazione Civica Digitale.

L'integrazione della P.U.A. nelle attività didattiche e nei regolamenti scolastici permetterà di garantire un ambiente digitale sicuro, inclusivo e consapevole.

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.

BYOD (Bring Your Own Device) nell'IC Primo Levi e il Modello DADA

L'Istituto Comprensivo Primo Levi adotta il modello DADA (Didattica per Ambienti di Apprendimento), in cui gli studenti si spostano tra le diverse aule materia per seguire le lezioni. In questo contesto, ogni alunno dispone già di un dispositivo personale, che contiene le versioni digitali dei libri di testo in adozione, rendendo l'ambiente di apprendimento più dinamico e flessibile. Tuttavia, i dispositivi personali degli alunni non possono essere connessi a Internet, né tramite Wi-Fi né con dati mobili, per ragioni di controllo della navigazione.

Tuttavia, allo stato attuale, l'Istituto non adotta la modalità BYOD (Bring Your Own Device) per ragioni legate all'infrastruttura di rete.

Nonostante questa limitazione, la presenza diffusa di dispositivi personali tra gli studenti rappresenta un'opportunità futura, che potrebbe essere sviluppata in un quadro normativo e infrastrutturale adeguato. Qualora l'Istituto decidesse di attivare

questa modalità, sarà necessario aggiornare l'ePolicy con un Regolamento per l'uso dei dispositivi personali, che garantisca un utilizzo controllato e conforme alle normative sulla sicurezza digitale.

Linee guida per un futuro Regolamento BYOD

Se il BYOD venisse implementato nell'Istituto, il regolamento dovrà prevedere le seguenti disposizioni:

1. Finalità dell'uso dei dispositivi personali

- I dispositivi personali potranno essere utilizzati esclusivamente per scopi didattici, in coerenza con il modello DADA e le esigenze di apprendimento.
- Il loro utilizzo dovrà favorire la personalizzazione dell'apprendimento, la collaborazione tra pari e l'accesso a risorse digitali funzionali alla didattica.

2. Accesso alla rete e requisiti tecnici

- L'accesso alla rete scolastica sarà regolamentato e consentito solo se il dispositivo rispetta i requisiti di sicurezza previsti.
- Qualora venisse attivata la connettività, l'accesso a Internet sarà monitorato e filtrato per garantire un uso sicuro e conforme all'ePolicy.
- Gli alunni dovranno mantenere aggiornati i propri dispositivi, dotandoli di software adeguati e strumenti di protezione (es. antivirus).

3. Uso in classe e gestione didattica

- L'uso del dispositivo sarà consentito solo su indicazione del docente, per attività didattiche specifiche.
- Il dispositivo dovrà essere utilizzato in modalità silenziosa e non potrà essere impiegato per scopi personali, come social network o giochi.
- Gli insegnanti definiranno in autonomia modalità e limiti di utilizzo, a seconda delle esigenze disciplinari e delle metodologie adottate.

4. Privacy e sicurezza

- Gli studenti dovranno rispettare le normative GDPR e le regole sulla privacy, evitando di registrare, fotografare o condividere dati senza autorizzazione.
- Sarà vietato l'uso del dispositivo per attività di cyberbullismo, diffusione di contenuti offensivi o violazione della privacy.
- La scuola non sarà responsabile per eventuali smarrimenti, furti o danni ai dispositivi personali.

5. Corresponsabilità scuola-famiglia

- Le famiglie saranno coinvolte nella definizione del regolamento e chiamate a sottoscrivere un documento di accettazione, impegnandosi a educare i propri figli a un uso consapevole della tecnologia.
- La scuola promuoverà momenti di formazione e sensibilizzazione su cittadinanza digitale, sicurezza informatica e uso responsabile dei dispositivi.

6. Sanzioni in caso di violazioni

- In caso di uso improprio, l'accesso ai dispositivi potrà essere limitato o sospeso per un periodo stabilito.
- Comportamenti gravi, come la violazione della privacy o la diffusione di contenuti inappropriati, saranno gestiti in base al Regolamento d'Istituto e potranno comportare sanzioni disciplinari.
- Il regolamento sarà soggetto a revisioni periodiche per adeguarlo alle evoluzioni tecnologiche e normative.

Conclusioni

Attualmente, per motivi legati all'infrastruttura di rete, l'Istituto Comprensivo Primo Levi non adotta il BYOD e i dispositivi personali degli studenti non possono connettersi a Internet. Tuttavia, la presenza diffusa di tali strumenti e il modello DADA rappresentano una potenziale opportunità futura.

Qualora le condizioni tecniche lo permettessero, il BYOD potrebbe essere introdotto con un regolamento chiaro e sicuro, che garantisca un uso controllato, etico e funzionale dei dispositivi personali nella didattica, nel rispetto della sicurezza informatica e della protezione dei dati. In tale eventualità, l'ePolicy dell'Istituto sarà aggiornata per includere linee guida specifiche e riferimenti normativi.

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.

Il rischio online si configura come la possibilità per il minore di commettere azioni online che possano danneggiare sé stessi o altri; essere una vittima di queste azioni; osservare altri commettere queste azioni. È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e contenerli, ma è altrettanto importante praticare strategie efficaci di prevenzione e conoscere le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. Ciò è possibile lavorando su aspetti di ampio raggio che possano permettere una riduzione dei fattori di rischio e di conseguenza una minore probabilità che i ragazzi si trovino in situazioni non piacevoli. È importante che abbiano gli strumenti idonei per riconoscere possibili situazioni di rischio e segnalarle ad un adulto di riferimento. Gli strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio si configurano come interventi di sensibilizzazione e prevenzione. Nel caso della sensibilizzazione si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare. Nel caso della prevenzione si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i. Nell'Istituto viene promosso l'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con l'obiettivo di ridurre le situazioni di rischio attraverso tre campi di intervento:

AREA PERSONALE SCOLASTICO la formazione dei docenti e del personale ATA attraverso specifici corsi di aggiornamento adesione a progetti dedicati utilizzo del materiale a disposizione nella piattaforma Generazioni Connesse diffusione capillare di tutte le iniziative e i corsi sul tema

AREA ALUNNI tutte le UDA d'Istituto hanno come obiettivo le competenze digitali, la sensibilizzazione al rispetto reciproco, delle regole di convivenza civile e all'empatia. Vengono regolarmente organizzati incontri formativi e attività con figure esperte, adesione a progetti dedicati.

AREA GENITORI adesione a progetti specifici con consulenza da parte di esperti; visione, condivisione e conoscenza dei Regolamenti d'Istituto.

La diffusione di materiale in rete è soggetta a normative stringenti che tutelano la privicy e impediscono che ne venga fatto un uso improprio. Tuttavia queste azioni non sono facilmente controllabili. Un contenuto offensivo o denigratorio online può diventare virale e ledere in modo importante la reputazione e la serenità della vittima. Una delle ragioni per la quale questo fenomeno può diffondersi in modo incontrollato è la convinzione dell'anonimato: spesso, chi offende utilizzando Internet, è convinto di potersi nascondere dietro profili falsi in modo da non essere riconoscibile; questa sicurezza di anonimato consente di compiere impunemente atti denigratori. Contrariamente a quanto si pensi, qualsiasi azione online lascia tracce e, con strumenti adeguati e/o con l'intervento di esperti (Polizia Postale), l'anonimato può essere smascherato. L'atto offensivo può avvenire ad ogni ora del giorno e della notte. Quando le interazioni avvengono online viene a mancare la relazione che invece si crea con contatto visivo e fisico diretto; quindi, non essendo fisicamente presente l'altro/a, si accentua la mancanza di empatia che, poi, degenera in comportamenti noti messi in atto dai cyberbulli. Il cyberbullo non vede in modo diretto le reazioni della vittima e, questo riduce ulteriormente l'empatia e la capacità di rendersi conto dei danni provocati. Gli atti di cyberbullismo possono essere raccolti in due grandi gruppi:

cyberbullismo diretto: si verifica quando il bullo utilizza strumenti di messaggistica istantanea che hanno effetto immediato

sulla vittima (flaming---- ->litigi online con linguaggio violento e volgare; harassment ---- >molestie con invio ripetuto di linguaggio offensivo; cyberstalking----->invio ripetuto di messaggi con minacce fisiche)

cyberbullismo indiretto: si verifica quando il bullo fa uso di spazi pubblici in Rete per diffondere contenuti dannosi e diffamatori per la vittima (denigrazione, outing estorto, impersonificazione) I ragazzi/e che fanno azioni di cyberbullismo possono commettere reati: percosse (art.581 C.P.); lesione personale (art.582); ingiuria (art. 594); diffamazione (art 595); violenza privata (art. 610); minaccia (art. 612); danneggiamento (art. 635)

L'Istituto rende noto che, negli atti di bullismo/cyberbullismo vanno distinte diverse responsabilità: 1. culpa del minore: necessario distinguere tra il minore di 14 anni e quello con età compresa tra i 14 e i 18 anni. il primo non è mai imputabile penalmente; se viene riconosciuto come "socialmente pericoloso" possono essere previste misure di sicurezza. Il secondo è imputabile se viene riconosciuta la sua capacità di intendere e volere. 2. culpa in vigilando ed educando dei genitori: si applica l'art 2048 del cod. civile. Il non esercitare vigilanza adeguata è alla base della responsabilità civile dei genitori per gli atti illeciti commessi dal minore, a meno che i genitori non dimostrino di non aver potuto impedire il fatto. 3. culpa in vigilando e in organizzando della scuola: si fa riferimento all'art. 28 della Costituzione Italiana e, all'applicazione di quanto previsto dall'art 2048 del codice civile (secondo comma).

Si specifica:

1. responsabilità genitori: se il minore non ha compiuto i 14 anni, non risponde penalmente per l'evento, ma i genitori saranno tenuti al risarcimento del danno (presunta culpa in educando); non c'è responsabilità penale dei genitori, perchè la responsabilità penale è personale; se i genitori riescono a fornire la prova di aver fatto il possibile per impedire il fatto, sono esonerati dall'obbligo di risarcire il danno. Tale prova deve dimostrare di aver educato e istruito adeguatamente il/la proprio/a figlio/a (valutazione che viene dal giudice commisurata alle circostanze); di aver vigilato attentamente e costantemente sulla sua condotta; di non aver in nessun modo potuto impedire il fatto.
2. responsabilità docenti: nel caso in cui i comportamenti penalmente rilevanti o i danni procurati avvenissero a scuola o durante un viaggio di istruzione, sarà applicato l'art. 2048 del Codice Civile e, l'art. 61 della Legge 312/1980 n.312.Gli insegnanti sono quindi responsabili dei danni causati a terzi "dal fatto illecito dei loro allievi...nel tempo in cui sono sotto la loro vigilanza". Perciò la responsabilità non si limita alle sole ore di didattica ma, anche a tutti quei momenti di vita scolastica (ricreazione, pausa pranzo, palestra, uscite didattiche e viaggi di istruzione) La presunzione di colpa si può superare solo nel caso in cui si dimostri di aver adeguatamente vigilato

Al fine di prevenire atti di bullismo/cyberbullismo, l'Istituto ha individuato una referente per le iniziative di prevenzione e contrasto al cyberbullismo; stimolato un ruolo attivo degli studenti/esse in attività di Peer education; integrato il Regolamento di Istituto e il Patto di Corresponsabilità; stabilito procedure di interventi in caso di segnalazione di atti di bullismo/cyberbullismo, previsto misure di sostegno e rieducazione dei minori coinvolti (integrazione alle attività didattiche di percorsi mirati alla sensibilizzazione e prevenzioni di casi di bullismo/cyberbullismo, anche con l'ausilio di materiale disponibile in Piattaforma Generazioni Connesse) attivazione dello sportello di ascolto; attivazione del progetto "benessere a scuola"; qualora fosse necessario, interventi di tipo educativo e preventivo: -prevenzione universale, rivolta a tutti gli alunni;

- selettiva, rivolta a sottogruppi a rischio;

-indicata, indirizzata a studentesse/i che presentano problematiche specifiche

L'intervento invece di tipo educativo-preventivo deve prevedere:

1. diffusione e condivisione con alunne/i e le loro famiglie delle iniziative che l'Istituto intende intraprendere
2. attuazione di progetti che mirano all'inclusione della diversità e al rispetto con la creazione di un ambiente che favorisca la relazione tra pari.

Come riconoscerlo e prevenirlo:

-ampia diffusione delle caratteristiche dell'hate speech, con la diffusione nello specifico del documento No Hate Speech

Affinchè questo fenomeno possa essere contrastato è necessario progettare strategie di intervento. Quindi, lo sviluppo delle competenze digitali e l'educazione ad uso etico e consapevole delle tecnologie, assume un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete.

Si propongono azioni educative volte al raggiungimento degli obiettivi che contribuiscano al benessere digitale come: ricerca di equilibrio nelle relazioni anche online uso degli strumenti digitali per il raggiungimento di obiettivi personali capacità di interagire negli ambienti in modo sicuro e responsabile capacità di gestire il sovraccarico informativo e le distrazioni.

E' necessario proporre metodologie didattiche valide che abbiano come strumento giochi virtuali d'aula ed è importante non demonizzare la tecnologia o il gioco ma, stabilire semplici e chiare regole.

Il nostro Istituto aderisce anche alle iniziative della ASL regionale (Lazio) che ha costituito uno specifico progetto "Scuole che promuovono la salute", promosso dall'Organizzazione Mondiale della Sanità, riconosciuto a livello europeo e nazionale per la promozione della salute e del benessere a scuola. In particolare, tra le varie proposte, nella scuola secondaria è attivo da qualche anno il progetto UNPLUGGED.

L'Istituto attiva, anche con personale qualificato interno alla scuola, formazione per i docenti al fine di riconoscere segnali di rischio.

Attiva, inoltre, percorsi di educazione all'affettività e alla sessualità rivolti alle studentesse e agli studenti al fine di renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi.

Promuove percorsi di educazione digitale e sui rischi dell'adescamento online, anche in un'ottica di adeguata formazione sui problemi derivanti dalla poca attenzione nei confronti della protezione della propria privacy e gestione dell'immagine e dell'identità online. Se si sospetta o si ha la certezza di un caso di adescamento online, gli adulti di riferimento non devono sostituirsi al minore nel rispondere, ad esempio, all'adescatore. È importante che il computer o altri dispositivi elettronici del minorevittima non vengano usati per non compromettere eventuali prove. In caso di adescamento online è necessario l'intervento delle Forze dell'Ordine.

L'Istituto garantisce che le alunne e gli alunni acquisiscano le competenze necessarie che le/li guidino nelle scelte online sicure. La pedopornografia è un fenomeno che va affrontato e discusso per sapere bene di cosa si tratta ed essere a conoscenza anche delle conseguenze legali a cui vanno incontro. Ecco che tali temi dovranno rientrare in attività di sensibilizzazione rivolta anche ai genitori e al personale scolastico.

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

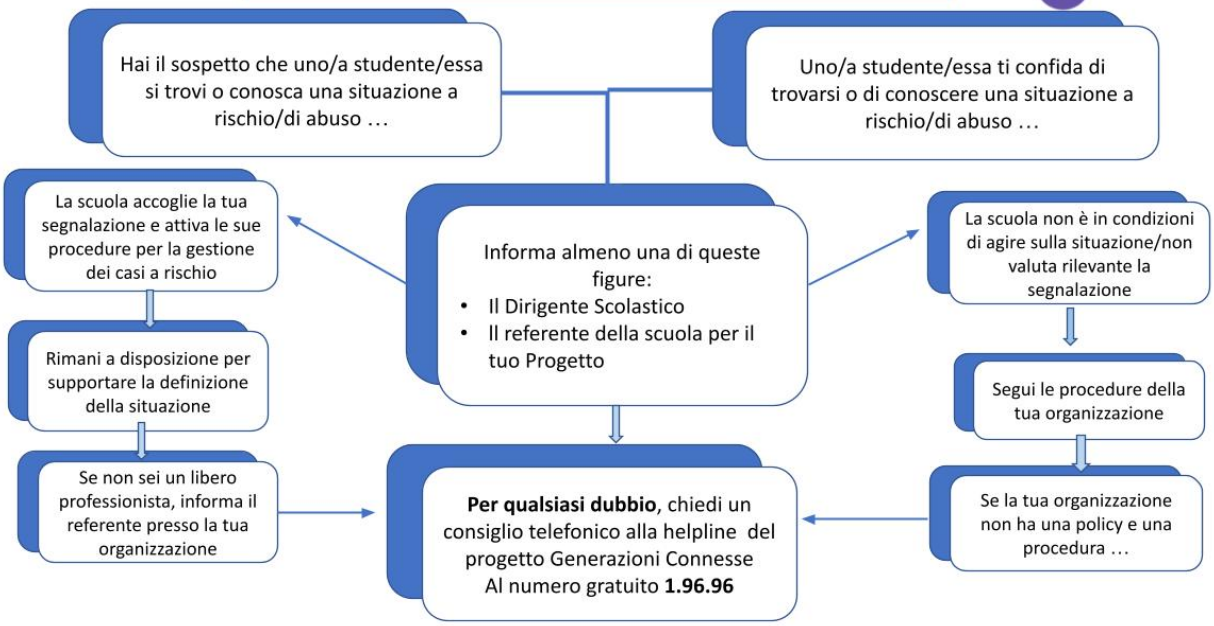
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

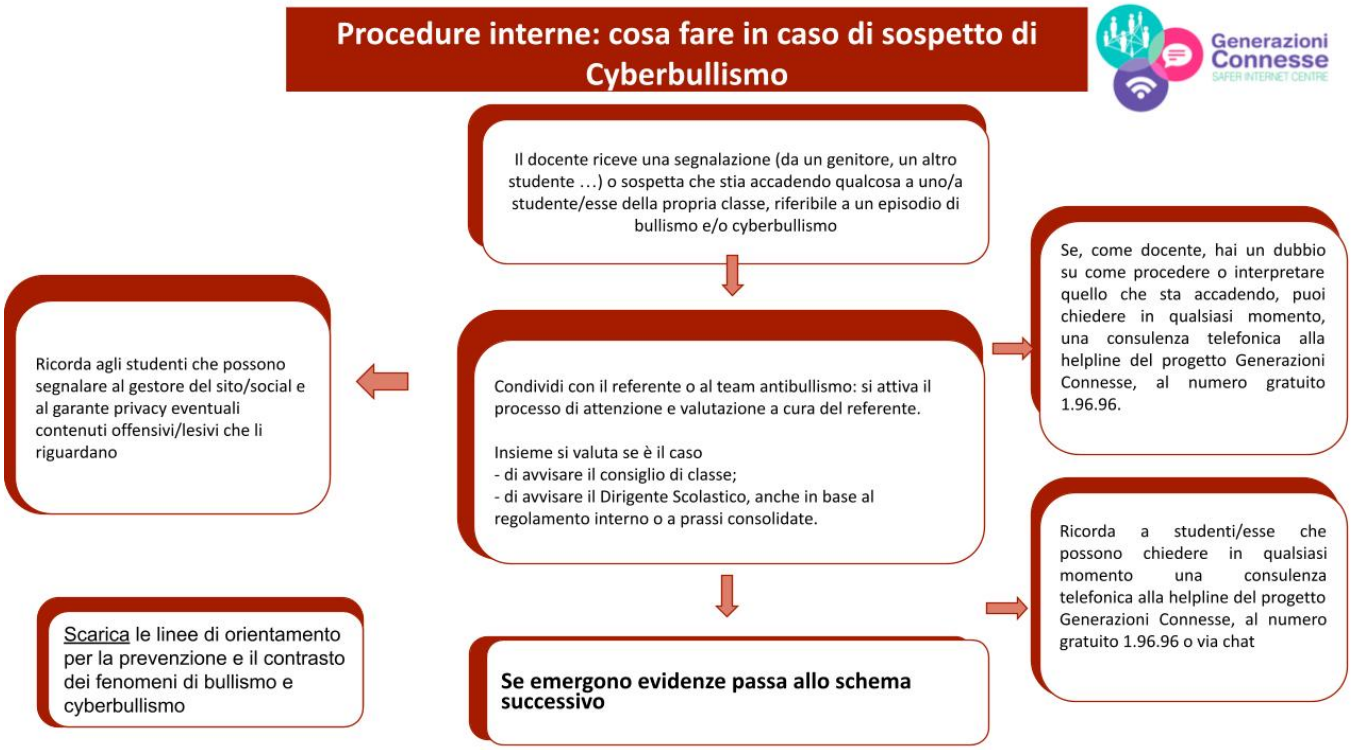
Il docente ha evidenza che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

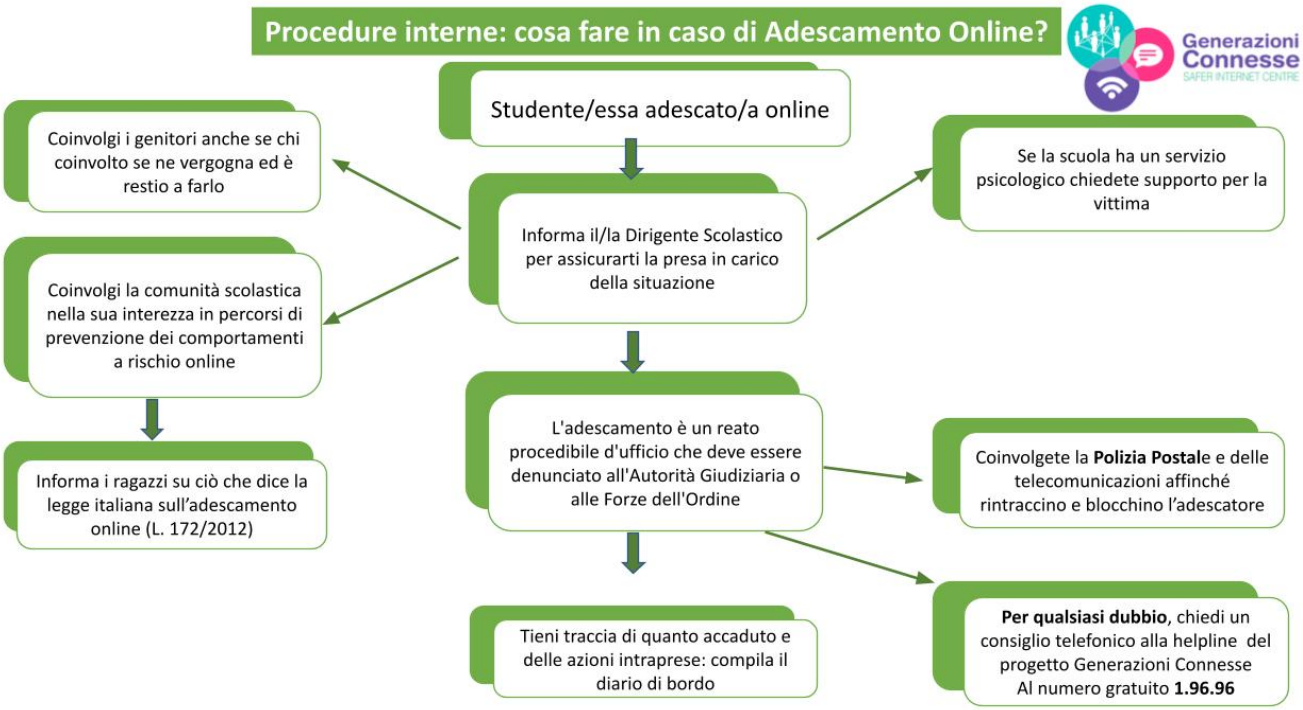
Se non è già stato fatto, avvisa il referente per il cyberbullismo (e/o il team antibullismo) che attiva le procedure ("Corso 4" della piattaforma ELISA) e il Dirigente Scolastico.
Ricordare sempre che in base alla legge 71-2017:
A) Se c'è fattispecie di reato va fatta la segnalazione alle forze dell'ordine
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.

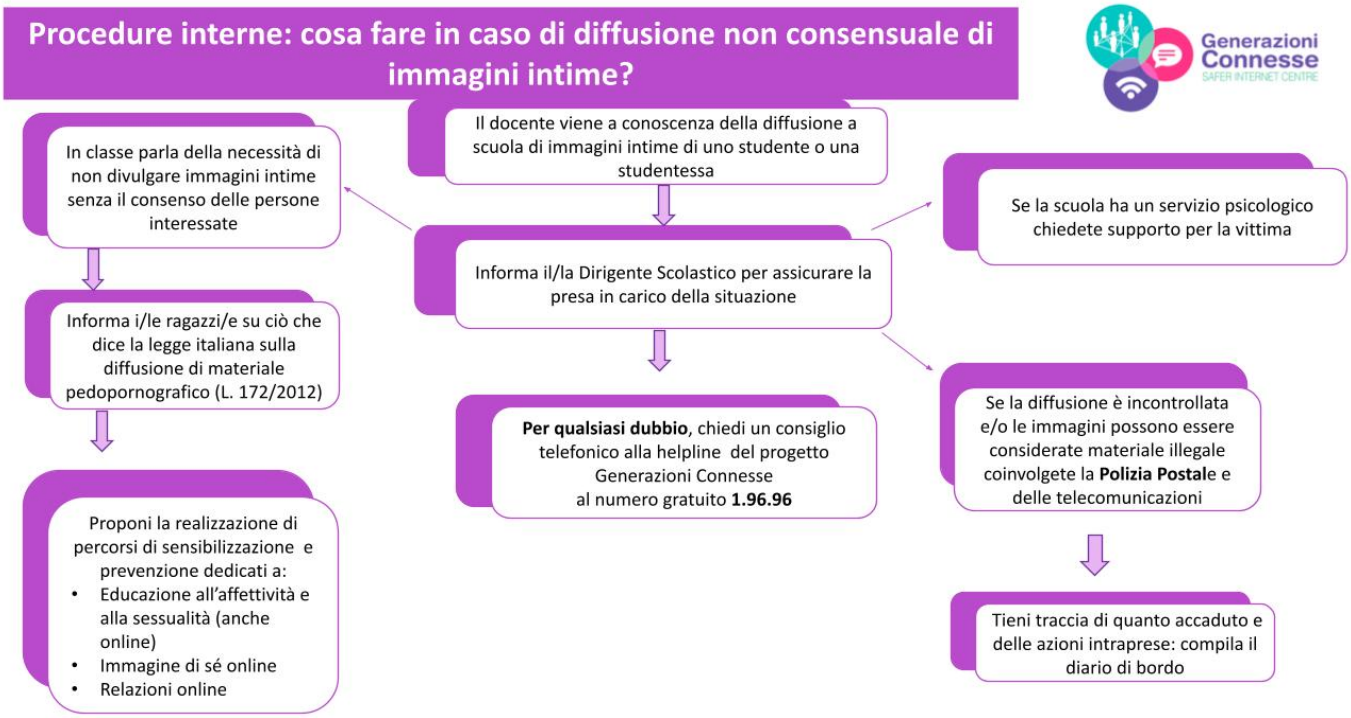
A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla Polizia Postale:
a) contenuto; b) modalità di diffusione.
Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita 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
Generazioni Connesse
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, 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 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 emergono evidenze passa allo schema successivo
Ricorda a studenti/esse che possono chiedere in qualsiasi momento una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 o via chat


Procedure interne: cosa fare in caso di Adescamento Online?
Generazioni Connesse
Studente/essa adescato/a online
Informa il/la Dirigente Scolastico per assicurarti la presa in carico della situazione
Coinvolgi i genitori anche se chi coinvolto se ne vergogna ed è restio a farlo
Coinvolgi la comunità scolastica nella sua interezza in percorsi di prevenzione dei comportamenti a rischio online
Informa i ragazzi su ciò che dice la legge italiana sull'adescamento online (L. 172/2012)
Se la scuola ha un servizio psicologico chiedete supporto per la vittima
L'adescamento è un reato procedibile d'ufficio che deve essere denunciato all'Autorità Giudiziaria o alle Forze dell'Ordine
Coinvolgete la Polizia Postale e delle telecomunicazioni affinché rintraccino e blocchino l'adescatore
Tieni traccia di quanto accaduto e delle azioni intraprese: compila il diario di bordo
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse Al numero gratuito 1.96.96



All'interno dell'Istituto, opera il Team bullismo/cyberbullismo. Tutta la comunità scolastica (alunni/e, docenti, personale ATA, genitori) possono segnalare casi di sospetto bullismo cyberbullismo, sexting, adescamento online tramite apposito modulo di segnalazione presente nell'area dedicata del sito scolastico.

L'Istituto mette a disposizione del personale, delle famiglie e di studentesse e studenti i seguenti strumenti di segnalazione:

1. Area dedicata sul sito ufficiale della scuola;
2. scheda di segnalazione di presunti casi di bullismo e cyberbullismo, compresi adescamento online e sexting;
3. contenitore per la raccolta delle segnalazioni anonime da posizionare in uno spazio accessibile e ben visibile della scuola;
4. accesso allo Sportello Ascolto con figure professionali specializzate

STRUMENTI A DISPOSIZIONE SPECIFICI **indirizzo mail di istituto dedicato: segnalazioni.bullismo@plevimarino.it**

diario di bordo

scheda segnalazione

elenco reati procedibili

slide informative

per le segnalazioni utilizzo del servizio Helpline, progetto Generazioni Connesse, al numero gratuito 1.96.96

https://www.commissariatodips.it/

https://azzurro.it/

https://www.generazioniconnesse.it/site/it/home-page/

Il dirigente scolastico
Francesca Toscano
Documento Firmato digitalmente ai sensi del
Codice Amministrazione Digitale e norme ad esso connesse
21/03/2025 11:06:37