Documento di ePolicy

IC MARTIRANO DON LORENZO MILANI

VIA POGGIO - 88040 - MARTIRANO
Catanzaro (CZ) - Calabria
Data di approvazione: 23/06/2025 - 15:23

Cap 1 - Lo scopo della ePolicy

1.1 Scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

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

Capitolo 2 - Sensibilizzazione e prevenzione

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

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

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

Capitolo 4 - Segnalazione e gestione dei casi

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

1.1 Scopo dell'ePolicy

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

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

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

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

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

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

Le Tecnologie dell'Informazione e della Comunicazione (TIC) costituiscono un supporto essenziale per l'insegnamento e l'apprendimento, contribuendo in modo significativo al percorso educativo di studenti e studentesse. In un contesto scolastico sempre più articolato e interconnesso, è fondamentale che ogni istituto scolastico si doti di un'e-policy: un documento strategico pensato per favorire lo sviluppo delle competenze digitali e promuovere un uso delle tecnologie che sia consapevole, critico e responsabile, sia per i giovani che per gli adulti coinvolti nel processo educativo.

L'e-policy ha anche lo scopo di prevenire comportamenti inappropriati legati all'utilizzo degli strumenti digitali, offrendo indicazioni su come riconoscere, affrontare, segnalare e monitorare eventuali situazioni problematiche. Questo documento si propone quindi non solo come guida all'uso corretto delle tecnologie, ma anche come strumento di tutela e promozione del benessere digitale all'interno della comunità scolastica.

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

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

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

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

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

IL DIRIGENTE SCOLASTICO

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

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

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

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

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

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

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

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

Il Team ha il compito di:

- coadiuvare il Dirigente scolastico, coordinatore del Team, nella definizione degli interventi di prevenzione del bullismo (per questa funzione partecipano anche il presidente del Consiglio d'Istituto e i Rappresentanti degli studenti).
- Intervenire (come gruppo ristretto, composto da Dirigente e referente o referenti per il bullismo e il cyberbullismo, psicologo o 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.

COLLEGIO DEI DOCENTI

Il Collegio dei Docenti sostiene e promuove scelte educative e didattiche orientate alla prevenzione di comportamenti a rischio, anche attraverso la collaborazione con altre scuole in rete. Tali scelte mirano a creare un ambiente scolastico positivo e inclusivo.

CONSIGLIO DI CLASSE

Il Consiglio di Classe elabora e propone attività didattiche, anche integrative, che coinvolgano attivamente gli studenti e le studentesse. Tali attività hanno l'obiettivo di stimolare la riflessione e accrescere la consapevolezza sull'importanza dei valori della convivenza civile. Inoltre, si impegna a promuovere un clima sereno e collaborativo in aula e a instaurare un dialogo costruttivo con le famiglie, anche attraverso progetti di educazione alla legalità e alla cittadinanza attiva.

DSGA (Direttore dei Servizi Generali e Amministrativi)

Il DSGA è responsabile anche dei seguenti aspetti legati alla ePolicy:

- supervisionare il rispetto delle indicazioni contenute nella ePolicy da parte del personale ATA;
- proporre eventuali aggiornamenti o integrazioni utili al miglioramento del documento.

Indicazioni per i COLLABORATORI ESTERNI che Svolgono Attività Educative nell'Istituto

Tutti coloro che, a vario titolo, entrano in relazione educativa con gli alunni e le alunne dell'Istituto sono tenuti a mantenere un comportamento esemplare sotto il profilo professionale e personale. Devono evitare atteggiamenti inappropriati e agire

sempre nel rispetto del principio del superiore interesse del minore.

È fondamentale prestare attenzione ai segnali, ascoltare con empatia e dare valore alle opinioni e alle preoccupazioni degli studenti e delle studentesse, soprattutto in situazioni delicate o allarmanti.

Sono espressamente vietati comportamenti che possano risultare irrispettosi, offensivi o invasivi della sfera privata degli studenti, così come la partecipazione o la tolleranza verso condotte illecite, pericolose o potenzialmente abusive da parte dei minori.

Chiunque svolga attività con gli studenti deve conoscere e attenersi al regolamento dell'Istituto, in particolare per quanto riguarda l'uso dei dispositivi personali (come smartphone, tablet e computer) e di quelli messi a disposizione dalla scuola. È necessario evitare qualsiasi utilizzo improprio o non eticamente corretto durante le attività educative.

Infine, è obbligatorio rispettare la normativa sulla privacy, soprattutto in relazione ai minorenni: è vietato scattare fotografie, registrare video, diffondere immagini o scambiare contatti personali (numeri di telefono, indirizzi e-mail, chat o profili social) con gli studenti e le studentesse.

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.

La ePolicy si inserisce in modo armonico e coerente all'interno del quadro normativo e regolamentare dell'Istituto Comprensivo. A tal fine, il Regolamento d'Istituto e il Patto Educativo di Corresponsabilità vengono aggiornati per includere riferimenti espliciti alla ePolicy, in linea con le Linee Guida del MIM e con le normative vigenti in materia di educazione

digitale, sicurezza e benessere degli studenti.

Il documento rispetta quanto previsto dalle principali disposizioni legislative, tra cui:

- **DPR 24 giugno 1998, n. 249**, recante lo *Statuto delle studentesse e degli studenti della scuola secondaria*, modificato dal **DPR 21 novembre 2007, n. 235**;
- **Legge 29 maggio 2017, n. 71**, riguardante la prevenzione e il contrasto del cyberbullismo, integrata successivamente dalla **Legge 17 maggio 2024, n. 70**, in vigore dal 14 giugno 2024, che amplia l'azione di tutela anche al bullismo;
- **Legge 31 dicembre 1996, n. 675**, relativa alla protezione dei dati personali.

La ePolicy si coordina inoltre con i regolamenti interni già esistenti, costituendo parte integrante della visione educativa dell'Istituto in materia di cittadinanza digitale. Essa si sviluppa in coerenza con i seguenti documenti istituzionali:

- **PTOF**, comprensivo delle azioni previste dal *Piano Nazionale Scuola Digitale (PNSD)*;
- **Regolamento di Istituto**, con tutte le disposizioni relative alla vita scolastica;
- **Regolamento per la Didattica Digitale Integrata (DDI)**;
- **Curricolo Digitale di Istituto**, che delinea il percorso formativo degli studenti nell'ambito delle competenze digitali.

L'integrazione tra questi strumenti garantisce un approccio educativo unitario e sistemico, volto a promuovere un uso consapevole, sicuro e responsabile delle tecnologie digitali all'interno della scuola.

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.

La ePolicy viene promossa come strumento condiviso da tutta la comunità educante, mettendo al centro il benessere e la crescita consapevole degli studenti e delle studentesse. Il documento evidenzia in modo chiaro ruoli, responsabilità e azioni reciproche tra tutti i soggetti coinvolti nel percorso formativo. È fondamentale che ogni componente della scuola – docenti, personale, alunni e alunne – si faccia portavoce dei principi e dei contenuti della ePolicy, contribuendo attivamente alla sua diffusione e applicazione.

Per garantire un'adeguata comunicazione e accessibilità, la ePolicy viene resa pubblica attraverso:

- la pubblicazione sul sito ufficiale dell'Istituto, sia nella versione completa che in una forma sintetica e facilmente consultabile;
- l'inserimento nel Registro Elettronico, all'interno delle sezioni dedicate ai Docenti e alle Famiglie.

Gli studenti e le studentesse, durante l'utilizzo delle tecnologie digitali negli spazi scolastici, sono accompagnati, guidati e monitorati, al fine di favorire un uso sicuro e responsabile della rete. Vengono inoltre informati in merito alle regole di comportamento da adottare online.

L'Istituto Comprensivo "Don Lorenzo Milani" di Martirano si impegna concretamente a realizzare azioni mirate alla condivisione della ePolicy con tutti i membri della comunità scolastica, valorizzando il dialogo e la collaborazione tra scuola e famiglia.

Infine, all'inizio di ogni ciclo scolastico, la ePolicy viene presentata ai genitori e agli alunni e alle alunne insieme al Patto Educativo di Corresponsabilità, così da favorire una conoscenza chiara e condivisa delle regole e dei valori che guidano l'Istituto.

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

Revisione, Aggiornamento e Monitoraggio della ePolicy

La ePolicy viene sottoposta a revisioni periodiche, specialmente in occasione di cambiamenti rilevanti riguardanti l'impiego delle tecnologie digitali all'interno dell'Istituto. Ogni aggiornamento del documento sarà discusso collegialmente con il personale docente, in un'ottica di condivisione e partecipazione.

Il monitoraggio dell'efficacia della ePolicy si baserà sull'analisi del raggiungimento degli obiettivi prefissati, nonché sulla valutazione di eventuali criticità emerse durante la sua applicazione. L'aggiornamento e la successiva implementazione della ePolicy verranno effettuati in concomitanza con la redazione del *Rapporto di Autovalutazione d'Istituto*, prendendo in considerazione sia i casi problematici riscontrati che la modalità con cui sono stati gestiti.

Eventuali revisioni straordinarie saranno predisposte qualora emergano nuove esigenze educative, cambiamenti normativi o innovazioni nell'uso delle tecnologie digitali da parte della scuola. Il compito di monitorare, rivedere e aggiornare il documento resta affidato al gruppo di lavoro originariamente incaricato della sua stesura.

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

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

Cap 2 - Sensibilizzazione e prevenzione

2.1 - Sensibilizzazione e prevenzione

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

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

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

I giovani utilizzano Internet e gli strumenti digitali ogni giorno, spesso con una naturalezza e rapidità che può sembrare superiore rispetto a quella degli adulti. Tuttavia, questa abilità pratica non corrisponde necessariamente a un livello più alto di **competenza digitale**.

Secondo la *Raccomandazione del Consiglio dell'Unione Europea sulle competenze chiave per l'apprendimento permanente* (C189/9, p. 9), la competenza digitale non si limita alla semplice capacità di usare la tecnologia, ma include una serie articolata di abilità e conoscenze. Essa implica interesse per il mondo digitale e un utilizzo consapevole, critico e responsabile degli strumenti tecnologici in diversi contesti: educazione, lavoro e partecipazione attiva alla vita sociale.

Questa competenza comprende:

- alfabetizzazione digitale e informatica;
- capacità di comunicare e collaborare online;
- comprensione dei media digitali;
- creazione di contenuti, anche tramite programmazione;
- sicurezza digitale e cybersicurezza;
- rispetto della proprietà intellettuale;
- abilità nel risolvere problemi e nel pensare in modo critico.

In quest'ottica, la scuola ha il compito di guidare gli studenti e le studentesse verso un uso consapevole e sicuro delle tecnologie digitali. Per raggiungere questo obiettivo, l'Istituto si impegna a progettare e attuare un **curricolo digitale**, attraverso percorsi formativi specifici che favoriscano lo sviluppo di queste competenze chiave, indispensabili per affrontare con responsabilità le sfide della società contemporanea.

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.

In coerenza con le più recenti indicazioni europee e nazionali – tra cui la *Raccomandazione del Consiglio dell'Unione Europea del 22 maggio 2018 relativa alle competenze chiave per l'apprendimento permanente*, il *DigComp 2.2* (aggiornamento 2022 del Quadro Europeo delle Competenze Digitali), il *Sillabo per l'Educazione Civica Digitale* e le indicazioni del *Piano Scuola 4.0* e del *PNSD – Piano Nazionale Scuola Digitale*, l'Istituto Comprensivo "Don Lorenzo Milani" di Martirano ha sviluppato e adottato un **curricolo digitale verticale** che coinvolge tutti gli alunni e le alunne della Scuola dell'Infanzia, della Primaria e della Secondaria di primo grado.

Attraverso l'accesso guidato alle TIC e alla rete, la scuola si pone l'obiettivo di formare cittadini digitali consapevoli, in grado di utilizzare in modo critico, sicuro e creativo le tecnologie, promuovendo così una cultura dell'innovazione e della responsabilità.

Le tre dimensioni delle competenze digitali

Le competenze digitali non si limitano all'uso tecnico degli strumenti, ma abbracciano una visione più ampia che integra aspetti tecnologici, cognitivi ed etici/sociali. In particolare, il curricolo digitale dell'Istituto si sviluppa attraverso tre dimensioni fondamentali:

- **Tecnologica**: riconosciuta come una delle otto competenze chiave europee, questa dimensione non riguarda solo le abilità operative legate all'uso degli strumenti, ma anche la capacità di riflettere sul loro impatto e potenziale. Gli alunni e le alunne vengono accompagnati a comprendere il funzionamento delle tecnologie e a utilizzarle per affrontare problemi reali, evitando approcci automatici o passivi.
- **Cognitiva**: comprende le competenze necessarie per cercare, analizzare, valutare e creare informazioni in modo critico. Gli studenti imparano a distinguere fonti affidabili da quelle non attendibili, a costruire conoscenze e a rielaborare contenuti in maniera consapevole e autonoma.
- **Etico-sociale**: si articola nella gestione sicura dei dati personali, nel rispetto della privacy, nella prevenzione di comportamenti dannosi come il cyberbullismo e nell'uso delle tecnologie per scopi leciti e costruttivi. Questa dimensione promuove anche lo sviluppo di abilità socio-relazionali e comunicative, fondamentali per partecipare in modo attivo e responsabile alla vita online e alle comunità virtuali.

Una visione integrata della competenza digitale

L'unione di queste tre dimensioni dà origine a una concezione integrata e trasversale della **competenza digitale**, intesa non solo come abilità tecnica, ma come capacità di *costruire conoscenza, partecipare attivamente alla vita sociale e culturale, favorire l'inclusione e la cittadinanza attiva* attraverso l'uso consapevole delle tecnologie.

Tale competenza si declina concretamente secondo le **cinque aree del quadro DigComp 2.2**, che costituiscono il riferimento europeo per l'educazione digitale:

1. **Alfabetizzazione all'informazione e ai dati**: saper individuare, selezionare, archiviare, organizzare e valutare criticamente le informazioni digitali, comprendendone pertinenza, affidabilità e obiettivi.
2. **Comunicazione e collaborazione online**: utilizzare ambienti digitali per comunicare, condividere risorse, partecipare a reti e comunità virtuali, collaborare in modo efficace e responsabile.
3. **Creazione di contenuti digitali**: produrre, modificare e rielaborare contenuti digitali (testi, immagini, video, multimedia), programmare semplici applicazioni, conoscere e rispettare le norme relative ai diritti d'autore e alle licenze d'uso.
4. **Sicurezza**: proteggere la propria identità digitale, i dati personali e quelli degli altri, gestire i rischi legati all'uso del web, utilizzare le tecnologie in modo sostenibile e sicuro.
5. **Problem solving**: riconoscere bisogni e problemi legati all'ambiente digitale, scegliere gli strumenti adeguati per risolverli, usare le tecnologie in modo creativo, aggiornare costantemente le proprie competenze.

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.

Formazione Docenti e Collaborazione Educativa sull'Uso Consapevole delle Tecnologie Digitali

Per garantire una didattica realmente inclusiva, innovativa ed efficace, è essenziale che tutti i docenti dell'Istituto siano adeguatamente formati e costantemente aggiornati sull'utilizzo consapevole, critico e funzionale delle Tecnologie dell'Informazione e della Comunicazione (TIC). L'integrazione delle tecnologie nella pratica didattica quotidiana consente infatti di diversificare le strategie educative, valorizzare i diversi stili di apprendimento e fornire agli studenti esempi concreti di utilizzo positivo e responsabile degli strumenti digitali.

La figura del docente oggi richiede competenze complesse e trasversali, tra cui quelle digitali rivestono un ruolo sempre più centrale. Le TIC non devono essere intese solo come strumenti di supporto, ma come vere e proprie risorse per progettare, attuare, gestire e valutare i percorsi di apprendimento, promuovendo esperienze didattiche più coinvolgenti e significative per tutti gli alunni e le alunne.

Promozione della Formazione Continua e Rete Educativa

L'Istituto riconosce l'importanza strategica della formazione continua e favorisce la partecipazione attiva del personale a iniziative organizzate internamente, da reti di scuole, dall'amministrazione scolastica, o anche a percorsi scelti autonomamente dai docenti, comprese le offerte online.

Periodicamente, il personale scolastico sarà coinvolto in attività di aggiornamento riguardanti l'uso consapevole e sicuro delle tecnologie e la prevenzione dei pericoli connessi alla rete. Tali momenti formativi mirano non solo all'acquisizione di competenze digitali, ma anche allo sviluppo della sensibilità educativa rispetto agli aspetti emotivi, relazionali e identitari connessi all'utilizzo dei dispositivi digitali da parte degli alunni.

Formazione Docenti e Ricadute Didattiche

La formazione non deve limitarsi a un'alfabetizzazione tecnica, ma deve tenere conto del ruolo che le tecnologie hanno nella costruzione dell'identità e nella gestione delle emozioni dei più giovani. I dispositivi digitali sono oggi spazi di comunicazione e auto-espressione, e per questo è fondamentale che i docenti acquisiscano strumenti per educare gli studenti anche alla cittadinanza emotiva e digitale.

L'adesione al progetto *Generazioni Connesse* rappresenta una preziosa opportunità per strutturare in modo coerente e organico la formazione digitale di tutto il personale scolastico

Rafforzare l'Alleanza Educativa con le Famiglie

Per prevenire i rischi derivanti da un uso inappropriato delle tecnologie e promuovere comportamenti positivi e consapevoli, è fondamentale che la scuola collabori strettamente con le famiglie. Questa alleanza educativa ha un ruolo chiave nell'accompagnare bambini e ragazzi verso una relazione sana con il mondo digitale, anche in un'ottica di preparazione al futuro professionale.

L'Istituto si impegna a garantire una comunicazione costante e trasparente con le famiglie, informandole puntualmente su tutte le attività previste dal Piano d'Azione dell'ePolicy d'Istituto.

Ruoli e Responsabilità nella Comunità Educante

Il rispetto delle regole da parte degli studenti è parte integrante della convivenza scolastica, così come la vigilanza attiva da parte delle famiglie, che sono invitate a supervisionare l'utilizzo domestico della rete.

Il Dirigente Scolastico, insieme al Referente per il bullismo/cyberbullismo, all'Animatore Digitale e al Team Digitale, promuove nei Consigli di Classe e negli organi collegiali momenti di confronto e scambio, affinché le competenze acquisite dai docenti nei percorsi formativi possano essere condivise e diventare patrimonio comune dell'Istituto.

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.

Le istituzioni scolastiche sono ogni giorno chiamate a svolgere un ruolo educativo di primaria importanza, non solo nella trasmissione di conoscenze e competenze, ma soprattutto nella formazione di cittadini consapevoli e rispettosi dei valori fondamentali della convivenza civile. In un contesto sempre più permeato dalle tecnologie digitali e dalle nuove modalità di comunicazione, questo compito assume un significato ancora più profondo.

Diventa quindi essenziale ribadire costantemente, anche a scuola, principi imprescindibili come il rispetto della dignità umana, della riservatezza e dell'identità personale, che devono essere alla base di ogni percorso formativo.

All'interno della scuola vengono quotidianamente gestite numerose informazioni personali riguardanti studenti e famiglie. Spesso si tratta di dati particolarmente delicati, come condizioni di salute, situazioni familiari complesse o disagi sociali. È quindi fondamentale che queste informazioni vengano trattate con la massima attenzione e responsabilità, in modo da garantire la protezione della privacy di ogni individuo, soprattutto se minorenne.

Il corretto trattamento dei dati personali rappresenta una condizione indispensabile per assicurare il rispetto dei diritti e della dignità delle persone coinvolte nei processi educativi.

La protezione dei dati è riconosciuta come un diritto fondamentale dell'individuo, come sancito dall'articolo 8 della Carta dei diritti fondamentali dell'Unione Europea. A livello normativo, essa è disciplinata dal Regolamento Europeo 2016/679 (GDPR), entrato in vigore il 27 aprile 2016, e, in Italia, dal Decreto Legislativo 10 agosto 2018, n. 101, applicato a partire dal 19 settembre dello stesso anno.

Anche le istituzioni scolastiche, dunque, sono tenute ad adeguarsi pienamente a queste disposizioni, adottando misure idonee a garantire la riservatezza, la sicurezza e il corretto utilizzo dei dati personali trattati nell'ambito della propria attività. Si tratta di un impegno essenziale per assicurare la tutela dei diritti degli studenti e delle loro famiglie, in un'ottica di

trasparenza, legalità e rispetto.

La SEZIONE PRIVACY del sito dell'Istituto Comprensivo "Don Lorenzo Milani" raccoglie e rende accessibile la documentazione ufficiale relativa all'applicazione del Regolamento (UE) 2016/679 (GDPR) e delle normative nazionali in materia di protezione dei dati personali.

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.

Accesso a Internet

L'accesso a Internet è oggi riconosciuto come un diritto fondamentale dell'individuo, indispensabile per il pieno sviluppo personale e per una partecipazione attiva alla vita sociale. Ogni cittadino ha diritto ad accedere alla rete in condizioni di equità, utilizzando tecnologie moderne e aggiornate che eliminino le barriere economiche e sociali. Questo diritto deve essere garantito non solo come mera possibilità tecnica di connessione, ma anche attraverso infrastrutture e condizioni che lo rendano effettivo.

La Dichiarazione dei diritti in Internet, redatta dalla Commissione per i diritti e i doveri in Internet (istituita il 27 ottobre 2014 presso la Camera dei Deputati e presieduta da Stefano Rodotà), afferma nel suo articolo 2 che l'accesso alla rete deve avvenire in modo libero e paritario, includendo la libertà di scelta di dispositivi, sistemi operativi e applicazioni. Inoltre, le istituzioni pubbliche devono impegnarsi ad abbattere ogni forma di divario digitale, anche legato a genere, condizioni economiche, disabilità o situazioni di vulnerabilità.

A livello normativo europeo, il Regolamento UE del 25 novembre 2015 (in vigore dal 30 aprile 2016) ha introdotto misure specifiche per garantire un accesso equo a un'Internet aperta. Parallelamente, il Piano Nazionale Scuola Digitale (PNSD) prevede che tutte le scuole siano messe nelle condizioni di offrire un accesso pieno alla società dell'informazione, rendendo concreto il diritto a Internet a partire dall'ambiente scolastico.

Infrastruttura digitale dell'Istituto Comprensivo Don Lorenzo Milani

Il nostro Istituto è dotato di un sito web costantemente aggiornato, che funge da punto di riferimento informativo per il personale scolastico e per le famiglie. Tutti i plessi scolastici dispongono di una connessione Internet protetta tramite rete Wi-Fi con accesso riservato mediante password. Gli studenti possono accedere alla rete solo in presenza degli insegnanti e per finalità didattiche, utilizzando dispositivi scolastici configurati con filtri che impediscono l'accesso a siti inappropriati,

garantendo così la sicurezza della navigazione.

Il personale docente e ATA può connettersi anche con i propri dispositivi personali, previa richiesta della password al Referente di plesso. Le classi, i laboratori, i corridoi e le aree comuni sono tutti coperti da rete Wi-Fi, progettata per sostenere un numero elevato di utenti e consentire l'utilizzo di strumenti didattici basati su cloud e contenuti multimediali.

L'adeguamento infrastrutturale è stato possibile grazie a un costante monitoraggio, alla partecipazione a bandi PON ed europei. Per la Didattica Digitale Integrata (DDI) e la Didattica a Distanza (DAD), vengono utilizzati il Registro Elettronico e la piattaforma Google Workspace for Education, accessibili tramite credenziali personali fornite dall'Istituto. Questi strumenti permettono la condivisione di materiale didattico e la comunicazione tra docenti, alunni e famiglie, nel rispetto della sicurezza e della privacy.

Sicurezza online e tutela degli utenti

Il nostro Istituto pone particolare attenzione alla sicurezza dell'ambiente digitale, trattandola con la stessa cura riservata all'ambiente fisico. In ambito anglosassone, la sicurezza online si distingue in "safety" (prevenzione dei rischi tramite educazione e consapevolezza) e "security" (protezione tecnica attraverso strumenti informatici).

L'Istituto garantisce la sicurezza informatica tramite antivirus, firewall, protocolli di comunicazione sicuri (HTTPS) e aggiornamenti periodici dei software. La gestione degli account è differenziata per alunni, docenti e personale amministrativo. L'accesso alla rete è regolato da un firewall, e i log di navigazione vengono conservati e, se necessario, forniti alle autorità competenti.

Sono state implementate reti distinte per la didattica e per la segreteria, evitando così interconnessioni che potrebbero compromettere la riservatezza dei dati amministrativi.

Manutenzione e supporto tecnico

L'Istituto programma interventi di manutenzione periodici per garantire il corretto funzionamento delle dotazioni tecnologiche. Le eventuali problematiche vengono segnalate ai Referenti di plesso che si interfacciano con il Team Digitale. Il Team interviene a seconda della situazione, fornendo anche supporto formativo ai docenti per risolvere autonomamente eventuali criticità ricorrenti. Per interventi di natura puramente tecnica verrà contattato l'assistente tecnico dell'istituto.

Le attività di configurazione, gestione, backup e ripristino dei sistemi sono affidate a figure interne competenti, supportate da tecnici esterni quando necessario, per assicurare un ambiente digitale efficiente, sicuro e funzionale alla didattica.

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.

Tuttavia, la normativa scolastica è recentemente cambiata in modo significativo:

- Con la **Circolare Ministeriale n. 5274 del 11 luglio 2024**, il Ministero dell'Istruzione e del Merito ha disposto il **divieto assoluto** di utilizzare il telefono cellulare nella scuola dell'Infanzia, nella scuola Primaria e nella scuola secondaria di primo grado, **anche per scopi didattici**, eccetto nei casi volti allo scopo di favorire l'inclusione di alunni con BES e in ogni caso espressamente previsto dai PEI o PDP.

Di conseguenza, la nostra ePolicy viene aggiornata per riflettere questi nuovi obblighi.

L'Istituto si impegna a:

· - Rivedere i propri regolamenti interni e il Patto di Corresponsabilità Educativa

· - Mappare modalità operative per garantire il divieto – ad esempio, attraverso contenitori sicuri per raccogliere i device all'inizio della giornata, in stretto raccordo con i Consigli di Istituto e i Documenti di Istituto.

· - Salvaguardare le eccezioni previste per tutelare studenti con necessità specifiche (PEI/PDP), o per attività didattiche specialistiche in ambiti tecnici.

· - Mantenere lo spazio per usare strumenti digitali comuni, come tablet, computer e LIM, esclusivamente sotto la guida dei docenti e sempre per scopi educativi.

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.

Prevenzione e gestione di bullismo e cyberbullismo

Nel nostro Istituto è stato nominato un docente con il ruolo di Referente per il contrasto al bullismo e al cyberbullismo. Tale figura, in collaborazione con il Dirigente Scolastico e i membri del Team Antibullismo ed Emergenza, supporta l'intero corpo docente nelle attività di prevenzione, sensibilizzazione e monitoraggio di episodi problematici. Il Team ha seguito percorsi formativi specialistici su piattaforme accreditate come *Generazioni Connesse* e *Piattaforma Elisa*.

Segnalazione di situazioni a rischio

Ogni docente, in presenza di indizi o certezze che un alunno/a sia coinvolto – come vittima o responsabile – in episodi di bullismo, cyberbullismo, sexting o adescamento online, ha il dovere di segnalare immediatamente quanto osservato. In particolare, vanno attenzionati casi che rientrano nelle seguenti tipologie:

- **Violenza fisica o psicologica reiterata**, intimidazioni o esclusione intenzionale dal gruppo;
- **Flaming**: discussioni online con linguaggio offensivo o aggressivo;
- **Harassment**: invio sistematico di messaggi ingiuriosi o molesti;
- **Cyberstalking**: minacce ripetute online che generano timore per la propria sicurezza;
- **Denigrazione**: diffusione in rete di contenuti lesivi della reputazione altrui;
- **Outing o Trickery**: diffusione di confidenze o informazioni riservate ottenute con l'inganno;
- **Impersonificazione**: uso fraudolento dell'identità digitale di un altro per ledere la reputazione della vittima;
- **Esclusione intenzionale** da ambienti digitali condivisi;
- **Happy slapping**: registrazione e diffusione di episodi di violenza;
- **Exposure**: pubblicazione di contenuti privati o imbarazzanti;
- **Sexting**: invio di immagini o testi a contenuto sessuale attraverso dispositivi digitali.

Riconoscere i segnali

I minori coinvolti possono manifestare segni di disagio come tristezza, ansia, rabbia o tensioni nei confronti dei pari. A volte raccontano spontaneamente le esperienze vissute, altre volte rispondono a stimoli offerti dai docenti, anche durante momenti di educazione alla cittadinanza digitale. Gli episodi segnalati possono verificarsi anche al di fuori dell'ambiente scolastico, ma restano di rilevanza educativa e disciplinare.

Le prove a supporto delle segnalazioni possono derivare da:

- contenuti salvati sui dispositivi digitali personali o scolastici;
- confessioni spontanee dell'alunno/a;
- reclami o comunicazioni da parte dei genitori;
- osservazioni dirette da parte degli insegnanti.

I docenti sono autorizzati a controllare le attrezzature scolastiche. In caso di necessità di verificare dispositivi personali degli alunni, è obbligatorio coinvolgere le famiglie.

Contenuti digitali a rischio da segnalare

Particolare attenzione va riservata alla circolazione di contenuti pericolosi, come:

- **Violazioni della privacy**: condivisione non autorizzata di foto, dati personali, contatti, eventi privati;
- **Contenuti violenti o offensivi**: insulti, calunnie, minacce, incitazioni all'odio, contenuti razzisti, videogiochi inappropriati;
- **Contenuti a sfondo sessuale**: messaggi molesti, conversazioni intime o sessualizzate, immagini pornografiche, nudità, materiale pedopornografico.

Modalità di intervento

I casi vengono gestiti in base alla loro gravità:

- **Eventi di bassa entità**, come silenziare un compagno durante una videolezione, possono essere affrontati con un confronto diretto in classe, per favorire consapevolezza e responsabilità.
- **Situazioni di media entità**, come insulti in chat o invio di immagini inappropriate, richiedono una segnalazione formale al Referente bullismo/cyberbullismo e successivamente al Dirigente Scolastico. In questi casi possono essere convocati alunni/e famiglie, per riflettere congiuntamente sull'accaduto e concordare strategie correttive.
- **Nei casi più gravi**, come sexting o grooming, o in presenza di sospetti di reato, il Dirigente Scolastico deve essere immediatamente informato. È prevista la convocazione urgente delle famiglie e, se necessario, l'attivazione delle autorità competenti.

Tutte le segnalazioni da parte dei docenti devono essere **formalizzate**, in conformità al "Protocollo d'intervento per la gestione delle emergenze relative a bullismo e cyberbullismo".

Sensibilizzazione e Prevenzione nell'ambiente digitale

L'ambiente online può esporre i minori a diversi tipi di rischi, che si concretizzano in tre principali situazioni:

- il minore può essere autore di azioni che danneggiano sé stesso o altri;
- può diventare vittima di tali azioni;
- può assistere passivamente ad episodi dannosi compiuti da altri.

Comprendere e distinguere chiaramente questi scenari è fondamentale per individuare le strategie più efficaci atte a prevenirli e gestirli. Una corretta educazione al digitale, infatti, non si limita alla conoscenza dei pericoli, ma punta anche alla riduzione dei fattori che possono aumentare la vulnerabilità dei giovani. È essenziale fornire loro strumenti adeguati per riconoscere le situazioni a rischio e sapere a chi rivolgersi, privilegiando sempre il dialogo con un adulto di riferimento.

Strumenti di prevenzione e azioni di sensibilizzazione

Per limitare l'esposizione ai pericoli online, è necessario attuare due tipi di interventi complementari:

- **Sensibilizzazione**: si tratta di iniziative volte a favorire un cambiamento culturale e comportamentale. Oltre a fornire informazioni dettagliate sui fenomeni digitali, queste attività mirano a far comprendere i comportamenti corretti da adottare e le possibili soluzioni per affrontare situazioni problematiche.
- **Prevenzione**: comprende una serie di azioni e programmi formativi finalizzati a sviluppare competenze digitali responsabili e a prevenire l'insorgenza di situazioni a rischio, migliorando la sicurezza online di bambini e adolescenti.

L'ampia diffusione delle tecnologie digitali fin dai primi anni di vita ha modificato profondamente il modo in cui i giovani comunicano, si relazionano e costruiscono la propria identità. Le Tecnologie dell'Informazione e della Comunicazione (TIC), infatti, sono oggi parte integrante della quotidianità giovanile: vengono usate per studiare, informarsi, esprimere sé stessi e partecipare alla vita sociale. Tuttavia, accanto alle potenzialità, emergono anche nuove sfide legate alla sicurezza, al rispetto

delle regole e alla responsabilità individuale.

È fondamentale evitare l'errore di considerare i giovani come "nativi digitali" completamente autosufficienti, demandando agli strumenti la funzione educativa che invece spetta agli adulti. Il mondo digitale è stato pensato per un'utenza adulta e può contenere contenuti e comportamenti inadeguati o dannosi per i più giovani.

Rischi online: riconoscerli per prevenirli

Tra i principali pericoli associati all'uso improprio delle tecnologie digitali si annoverano:

- cyberbullismo e adescamento online;
- sexting e violazione della privacy;
- esposizione a contenuti pornografici o pedopornografici;
- gioco d'azzardo digitale e dipendenza da internet;
- uso improprio di videogiochi;
- contenuti pericolosi o inappropriati (ad esempio, che promuovono odio, autolesionismo, disordini alimentari, razzismo).

Educare i giovani alla cittadinanza digitale significa offrire loro gli strumenti per riconoscere questi rischi e adottare un comportamento consapevole, in grado di cogliere le opportunità del digitale ma anche di gestirne le criticità.

Il ruolo della scuola, delle famiglie e degli studenti

I docenti del nostro Istituto partecipano a percorsi di formazione continua per promuovere, nelle classi, l'uso sicuro e consapevole della rete e dei dispositivi digitali. Gli insegnanti guidano gli alunni nella comprensione dei pericoli legati a comportamenti scorretti, sia online sia nella vita reale.

Alle famiglie è richiesto un impegno attivo: leggere attentamente l'e-Safety Policy della scuola e partecipare alle iniziative proposte per promuovere una cultura digitale condivisa.
Agli studenti, invece, è richiesto di rispettare i Regolamenti e partecipare con responsabilità ai momenti di confronto organizzati dall'Istituto.

Laddove disponibili, i fondi scolastici saranno utilizzati per attivare interventi formativi mirati, in collaborazione con figure esperte come rappresentanti della Polizia di Stato, della Polizia Postale e professionisti qualificati.

Interventi di sensibilizzazione: come promuovere il cambiamento

Perché una campagna di sensibilizzazione sia realmente efficace, occorre che:

- venga riconosciuto lo **stato attuale** del problema;
- sia rafforzata la **motivazione al cambiamento**.

È necessario che chi partecipa a questi percorsi abbia una comprensione chiara del fenomeno affrontato e delle ragioni per cui è importante modificarne le dinamiche. Solo così sarà possibile generare un autentico cambiamento.

Ogni intervento deve quindi:

- stimolare il desiderio di migliorare le situazioni esistenti;
- evidenziare come sia possibile trasformare il contesto in modo positivo;
- indicare azioni concrete da intraprendere.

In sintesi, la sensibilizzazione non si limita a fornire informazioni: offre esempi di comportamento virtuoso e suggerisce soluzioni praticabili, favorendo la nascita di una cultura digitale più sicura, rispettosa e consapevole.

Interventi di Prevenzione dei Rischi Online

Il concetto di **prevenzione**, nato in ambito medico ed epidemiologico, è inteso – secondo quanto definito dal Ministero della Salute – come l'insieme di azioni e strategie volte a promuovere il benessere, preservare lo stato di salute e prevenire l'insorgenza di problemi o malattie.

Nel contesto della sicurezza online, non basta limitarsi alla semplice individuazione dei rischi presenti. È fondamentale adottare un approccio preventivo, mirato ad anticipare i comportamenti dannosi e a rafforzare le capacità individuali dei ragazzi/e nell'affrontare le sfide del digitale.

I tre livelli della prevenzione

Secondo la classificazione dell'**Institute of Medicine**, la prevenzione si articola in tre livelli, ognuno con obiettivi e destinatari differenti:

1. **Prevenzione Universale**
   Questo tipo di intervento è rivolto all'intera popolazione scolastica, indipendentemente dalla presenza di fattori di rischio specifici. Si parte dall'ipotesi che ogni studente possa trovarsi in situazioni di potenziale pericolo, pertanto si promuovono attività educative estese, come percorsi sulla cittadinanza digitale o sullo sviluppo delle competenze emotive. Sebbene l'impatto su ogni singolo individuo possa essere limitato, l'efficacia complessiva si misura nei cambiamenti positivi a livello di gruppo.
2. **Prevenzione Selettiva**
   Si concentra su gruppi specifici di studenti per i quali sono stati identificati segnali o fattori di rischio concreti. Questi programmi nascono dall'osservazione diretta, da segnalazioni interne alla scuola o da analisi del contesto territoriale. Gli interventi selettivi prevedono percorsi strutturati per rafforzare le competenze digitali e le capacità di gestione dei problemi.
3. **Prevenzione Indicata**
   Si tratta di azioni mirate su singoli casi, con l'obiettivo di affrontare situazioni già problematiche, ridurre comportamenti a rischio o sostenere eventuali vittime. Questo tipo di intervento richiede il coinvolgimento di più figure professionali – educatori, psicologi, esperti digitali – e spesso anche della famiglia dello studente, specie nei casi che coinvolgono aspetti legati al benessere psico-emotivo del minore.

Questo modello a tre livelli costituisce una guida preziosa per affrontare con metodo ogni possibile situazione di disagio legata all'uso delle tecnologie.

Ruolo della scuola nella prevenzione

Gli interventi più comuni e facilmente realizzabili rientrano nel primo livello (Prevenzione Universale) e sono fondamentali per sviluppare nei giovani quelle competenze di base necessarie per affrontare le dinamiche relazionali e digitali della quotidianità.

Le situazioni problematiche, infatti, spesso non nascono da un uso tecnico scorretto della tecnologia, ma da difficoltà legate allo sviluppo personale. È essenziale che la scuola educhi anche alla:

- gestione della relazione con persone diverse da sé;
- comprensione dell'affettività e della sessualità;
- riconoscimento dei limiti, inclusi quelli legali;
- consapevolezza e responsabilità nell'utilizzo degli strumenti digitali.

Per rispondere in modo efficace a tali esigenze, l'Istituto mette in campo strumenti e azioni mirate. Quando si verificano episodi critici legati ai rischi digitali all'interno del contesto scolastico, è indispensabile adottare un approccio integrato, supportato da protocolli ben definiti. Questi devono prevedere il coinvolgimento diretto di enti territoriali competenti o la **Polizia Postale**, tramite specifici accordi di collaborazione.

Un'azione educativa condivisa

La prevenzione non è responsabilità esclusiva della scuola, ma un compito condiviso tra più soggetti: famiglie, istituzioni, associazioni, mondo civile. Solo attraverso un impegno collettivo è possibile costruire un progetto educativo solido e coerente.

I comportamenti a rischio cambiano con l'età e sono spesso legati a fasi transitorie dello sviluppo, oppure a difficoltà nella gestione delle emozioni, delle relazioni o del senso del limite. Alcuni esempi includono:

- difficoltà nel relazionarsi con gli altri;
- gestione della sfera emotiva e affettiva;
- riconoscimento delle regole e del concetto di legalità;
- uso improprio delle tecnologie digitali.

Azioni pratiche per contenere i rischi online

In caso di comportamenti inappropriati da parte degli studenti, è necessario attivare rapidamente misure correttive. Di seguito alcune azioni concrete:

- **Diffusione di immagini imbarazzanti o intime**: contattare il fornitore del servizio online e richiederne la rimozione, segnalando la violazione dei termini d'uso.
- **Offese o molestie digitali**: suggerire agli studenti di modificare le impostazioni del profilo rendendolo privato, bloccare gli utenti molesti, rimuoverli dalla lista contatti e segnalarli come indesiderati.
- **Spam o messaggi offensivi**: consigliare il cambio dell'indirizzo email o del numero di telefono; se necessario, utilizzare app per bloccare numeri sconosciuti o contattare l'operatore telefonico per assistenza.
- **Presenza di materiale offensivo su dispositivi mobili**: coinvolgere i genitori per la rimozione dei contenuti, raccogliere informazioni su dove e a chi è stato inviato, e conservarne una copia in caso di indagini.
- **Materiale illegale o pedopornografico**: contattare immediatamente le forze dell'ordine. È vietato scaricare, duplicare o diffondere tale materiale: la sola detenzione o condivisione rappresenta un reato.

Cyberbullismo: definizione e strategie di prevenzione

La legge n. 71 del 2017, intitolata "*Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo*", all'articolo 1, comma 2, definisce il cyberbullismo come qualsiasi forma di violenza o prevaricazione realizzata attraverso strumenti digitali. Rientrano in questa categoria atti come: pressioni psicologiche, aggressioni verbali, molestie, minacce, insulti, diffamazione, furto d'identità, diffusione illecita o manipolazione di dati personali, anche quando coinvolgono familiari del minore, con lo scopo di isolarlo, danneggiarlo o ridicolizzarlo.

Successivamente, la legge n. 70 del 17 maggio 2024, entrata in vigore il 14 giugno, ha ampliato e aggiornato queste disposizioni, rafforzando gli strumenti di prevenzione e contrasto, anche alla luce delle *Linee di orientamento per la prevenzione e il contrasto del bullismo e cyberbullismo* (D.M. 18/2021). Le nuove direttive riconoscono alla scuola un ruolo centrale e identificano una serie di azioni da intraprendere:

- Formazione specifica del personale scolastico, con la nomina di un referente per ogni istituto;
- Inserimento delle competenze digitali tra gli obiettivi formativi prioritari (in linea con la Legge 107/2015);
- Promozione dell'educazione tra pari (peer education) attraverso il coinvolgimento attivo degli studenti ed ex studenti;
- Adozione di percorsi di sostegno e rieducazione per i minori coinvolti;
- Aggiornamento dei regolamenti d'istituto e del patto educativo di corresponsabilità con riferimenti espliciti al cyberbullismo e alle relative sanzioni;
- Affermazione di una visione educativa che privilegi l'azione preventiva rispetto a quella esclusivamente punitiva.

Come intervenire: riconoscere e affrontare il cyberbullismo

Per agire in modo efficace, è importante innanzitutto distinguere il cyberbullismo da altri comportamenti disfunzionali o violenti. Oltre al contesto e alle modalità di attuazione, va considerata l'età dei soggetti coinvolti e l'eventuale stato di disagio emotivo o psicologico. In presenza di un malessere evidente, può rendersi necessario il coinvolgimento dei servizi socio-sanitari territoriali, che offrono supporto psicologico e mediazione.

Nel caso in cui un minore di 14 anni sia vittima di cyberbullismo, i genitori o chi ne esercita la responsabilità possono richiedere la rimozione, l'oscuramento o il blocco dei contenuti online rivolgendosi al gestore della piattaforma. Se entro 24 ore non si ottiene risposta, la richiesta può essere inoltrata al Garante per la Protezione dei Dati Personali, che ha l'obbligo di intervenire entro 48 ore. Un apposito modulo per la segnalazione è disponibile sul sito del Garante, all'indirizzo email: **cyberbullismo@gpdp.it**.

Quando si sospetta che i comportamenti subiti rientrino nel perimetro del reato – come nel caso di furto d'identità o persecuzioni che compromettano seriamente il benessere psico-fisico della vittima – si deve procedere con una denuncia alle Forze dell'Ordine. I referenti competenti sono:

- la **Polizia Postale e delle Comunicazioni**,
- la **Questura** o il **Commissariato di Polizia** del territorio,
- l'**Arma dei Carabinieri**,
- oppure il **Commissariato online** tramite il sito: https://www.commissariatodips.it.

Per assistenza e orientamento, è inoltre attiva la **Helpline di Telefono Azzurro per Generazioni Connesse**, che fornisce supporto a studenti, famiglie, docenti e dirigenti scolastici, offrendo un punto di riferimento qualificato per affrontare situazioni problematiche legate all'uso dei media digitali.

Le azioni del nostro Istituto: prevenzione e contrasto su tre livelli

L'Istituto Comprensivo "Don Lorenzo Milani" si impegna nella promozione della consapevolezza e nella prevenzione del cyberbullismo attraverso un approccio articolato su tre livelli:

1. Intervento a livello individuale

- Sviluppo della consapevolezza sul fenomeno;
- Rafforzamento delle competenze digitali personali;
- Promozione dell'autostima e del benessere individuale.

2. Intervento a livello di classe

- Educazione alla conoscenza del cyberbullismo;
- Incentivazione di un clima di rispetto e collaborazione, tramite attività come circle time e apprendimento cooperativo;
- Gestione positiva dei conflitti e valorizzazione delle diversità.

3. Intervento a livello d'Istituto

- Nomina del referente per il bullismo e il cyberbullismo, con compiti di coordinamento;
- Realizzazione di incontri informativi e attività di sensibilizzazione rivolte anche alle famiglie;
- Celebrazione della Giornata Nazionale contro il Bullismo e Cyberbullismo (7 febbraio);
- Diffusione di buone pratiche educative e disciplinari.

Azioni specifiche di contrasto

L'Istituto ha previsto anche una serie di azioni per affrontare concretamente i casi rilevati:

A livello individuale

- Somministrazione di questionari o strumenti di rilevazione per valutare il clima scolastico percepito dagli studenti.

A livello di classe

- Analisi e condivisione dei dati raccolti all'interno dei Consigli di Classe e Interclasse, al fine di individuare strategie educative mirate.

A livello d'Istituto

- Adozione di un regolamento che disciplini anche l'uso corretto dei dispositivi digitali;
- Rafforzamento della sorveglianza durante momenti più a rischio (intervallo, cambio dell'ora, spogliatoi, ingressi/uscite).

Una cultura del rispetto: la cornice educativa

Le attività di prevenzione e contrasto al bullismo e al cyberbullismo si inseriscono nel più ampio progetto educativo promosso dalla scuola. In particolare, la Legge n. 92 del 2019 sull'insegnamento dell'educazione civica offre il quadro normativo per promuovere valori come la responsabilità, la legalità e il rispetto degli altri.

In questo contesto si colloca anche la **Giornata del Rispetto**, istituita dalla Legge 70/2024 e celebrata ogni anno il **20 gennaio**: una giornata dedicata all'approfondimento delle tematiche legate alla non violenza, alla lotta contro le discriminazioni e alla promozione del rispetto reciproco.

Hate Speech: di cosa si tratta e come contrastarlo

L'hate speech, o "discorso d'odio", si manifesta attraverso espressioni verbali, visive o simboliche – come post, immagini, commenti – che comunicano disprezzo e intolleranza verso una persona o un gruppo, spesso identificabili per razza, religione, genere, orientamento sessuale, disabilità o origine etnica. Tali espressioni, che possono essere veicolate online ma anche nella vita reale, alimentano discriminazione e possono scatenare reazioni aggressive e violente.

Poiché questo fenomeno è in costante crescita, diventa fondamentale affrontarlo anche in ambito scolastico ed educativo. L'obiettivo è:

- aiutare gli studenti a riconoscere e smontare gli stereotipi alla base del linguaggio d'odio;
- promuovere l'impegno civile e la partecipazione attiva, anche attraverso l'uso consapevole dei social media;
- incentivare una comunicazione responsabile, consapevole e rispettosa da parte dei giovani.

Cosa si intende per Hate Speech

Secondo il Consiglio d'Europa, l'incitamento all'odio comprende tutte le espressioni che promuovono, giustificano o diffondono l'odio razziale, la xenofobia, l'antisemitismo o altre forme di intolleranza. Questo include l'odio derivante da ideologie nazionalistiche aggressive, etnocentrismo, ostilità verso migranti, minoranze e persone con background differenti.

Le iniziative dell'Istituto

Il nostro Istituto si impegna ad affrontare questo tema con una serie di azioni rivolte a tutta la comunità scolastica:

- **Attività informative** rivolte a docenti, studenti, famiglie e personale ATA;
- **Formazione specifica** tenuta da esperti del settore;
- **Laboratori e attività didattiche** in classe, incentrate sul rispetto delle differenze culturali, di genere, di identità sessuale e di provenienza;
- **Educazione alla diversità**, attraverso:
  - progetti mirati alla valorizzazione della pluralità;
  - visione e discussione di materiali audiovisivi, come i "Supererrori" del sito Generazioni Connesse;
  - adesione al Manifesto della comunicazione non ostile;
- **Partecipazione ad eventi territoriali** e giornate tematiche contro razzismo e bullismo.

Come riconoscere e prevenire l'Hate Speech

Il documento "No Hate Ita" individua alcuni tratti distintivi dell'hate speech:

- **Parole che fanno male**: anche online, il linguaggio d'odio ha conseguenze reali e può violare i diritti umani;
- **Dal pensiero all'azione**: certi atteggiamenti possono trasformarsi in atti concreti di violenza o esclusione;
- **Molteplici forme di espressione**: l'odio può manifestarsi con testi, immagini, video, e spesso è amplificato dall'anonimato online;
- **Obiettivi vulnerabili**: individui o gruppi già marginalizzati sono spesso i bersagli più colpiti;
- **Contesto culturale e storico**: il significato del messaggio d'odio cambia a seconda dell'ambiente sociale in cui si diffonde;
- **Impatto sociale**: le conseguenze possono essere devastanti, sia a livello individuale che collettivo;
- **Anonimato e impunità**: la rete favorisce la percezione di impunità, ma ogni azione lascia traccia ed è potenzialmente rintracciabile.

Indicatori del discorso d'odio

Per valutare la gravità di un messaggio offensivo è utile considerare:

- **Il tono e il linguaggio utilizzato**: più è violento o offensivo, maggiore è il rischio di incitamento;
- **L'intenzionalità**: è possibile offendere anche involontariamente, ma la consapevolezza gioca un ruolo importante;
- **I destinatari**: alcune categorie sociali risultano più vulnerabili;
- **Il contesto**: i significati cambiano in base alla situazione, all'autore e al mezzo utilizzato;
- **Le conseguenze**: l'impatto emotivo e sociale sulle vittime deve essere sempre valutato attentamente.

Come agire per contrastarlo

Promuovere un uso consapevole delle tecnologie digitali è essenziale per formare cittadini responsabili anche in rete. L'Istituto si propone di:

- sviluppare nei ragazzi capacità relazionali e senso critico per gestire situazioni di conflitto e comunicazione;
- proporre percorsi di **educazione interculturale** che aiutino a decostruire pregiudizi e discriminazioni;
- promuovere l'impegno civico e una comunicazione positiva attraverso i nuovi media;
- aiutare gli studenti a **prendere la parola** in modo costruttivo, per prevenire comportamenti offensivi e umilianti.

Un approccio educativo integrato

Tutte le discipline contribuiscono a sviluppare competenze di cittadinanza e a costruire una cultura del rispetto e della legalità. Gli insegnanti intervengono in presenza di linguaggio volgare o comportamenti irrispettosi, favorendo nei ragazzi:

- la consapevolezza del proprio corpo e dei propri limiti;
- la capacità di riconoscere contatti sgraditi e opporvisi;
- la fiducia nelle proprie percezioni e la determinazione nel rifiutare comunicazioni moleste, anche digitali;
- la comprensione che le interazioni online devono seguire regole di rispetto, come nella vita reale.

In caso di situazioni problematiche, la scuola coinvolge le famiglie per valutare insieme il ricorso a risorse del territorio.

Infine, gli studenti sono coinvolti in progetti di solidarietà e legalità, per aumentare la loro sensibilità verso i temi sociali e promuovere una cittadinanza attiva e consapevole.

Dipendenza da Internet e gioco online: un fenomeno da conoscere e prevenire

L'uso eccessivo e non controllato di Internet può trasformarsi in una vera e propria dipendenza, al pari di altre forme patologiche, e avere conseguenze rilevanti sulla vita quotidiana, scolastica e sociale di bambini e adolescenti. Questo comportamento, noto come dipendenza da Internet, si manifesta spesso attraverso un bisogno compulsivo di connettersi, trascorrere molte ore online o dedicarsi in modo ossessivo a videogiochi.

La scuola riconosce la rilevanza di questa problematica e intende attivarsi con percorsi educativi sul benessere digitale, per fornire agli studenti strumenti utili a riconoscere e gestire i rischi legati alla sovraesposizione alla Rete.

Internet Addiction Disorder (I.A.D.)

Il termine *Internet Addiction Disorder* è stato coniato nel 1996 dallo psichiatra Ivan Goldberg per descrivere una condizione che presenta sintomi analoghi a quelli di altre dipendenze: aumento progressivo del tempo trascorso online (tolleranza), disagio psicofisico in caso di disconnessione (astinenza), difficoltà a interrompere l'uso nonostante le conseguenze negative. Tutto ciò può portare all'isolamento sociale, a un peggioramento del rendimento scolastico, a un'alterazione dell'umore e a una percezione distorta del tempo.

Una forma particolare di disagio è la *nomofobia* (da "no-mobile-phobia"), che descrive l'ansia o il malessere provato quando non si ha accesso allo smartphone o a Internet.

Dipendenza da gioco online

Tra le manifestazioni della dipendenza digitale rientra anche quella da videogiochi, chiamata *Internet Gaming Disorder*, riconosciuta dal Manuale Diagnostico e Statistico dei Disturbi Mentali (DSM-5). Si parla di dipendenza quando il gioco online viene praticato in modo continuativo e sistematico, a scapito delle attività quotidiane e delle relazioni reali.

I principali segnali da monitorare, se persistenti per almeno 12 mesi, sono:

1. Pensiero costante rivolto al gioco;
2. Necessità impellente di giocare;
3. Utilizzo del gioco per evadere dalla realtà;
4. Ricerca continua di esperienze emozionanti attraverso il gioco;
5. Aumento del tempo dedicato ai giochi;
6. Stati di agitazione, ansia o depressione in assenza di gioco;
7. Tendenza al ritiro sociale;
8. Incapacità di smettere di giocare nonostante la consapevolezza del problema;
9. Bugie sull'effettivo utilizzo dei giochi;
10. Perdita di interesse per le attività quotidiane e relazionali a causa del gioco online.

Le caratteristiche della dipendenza secondo la S.I.I.Pa.C.

La Società Italiana Intervento Patologie Compulsive definisce la dipendenza da Internet come un progressivo coinvolgimento totale nella Rete. Tra le sue caratteristiche principali troviamo:

- **Dominanza**: l'attività online diventa centrale nella vita dell'individuo, condizionando pensieri e comportamenti.
- **Variazione dell'umore**: l'utilizzo di Internet induce cambiamenti emotivi significativi, come eccitazione o rilassamento.
- **Conflitti**: si manifestano contrasti con familiari o amici e conflitti interiori legati alla consapevolezza della dipendenza.
- **Ricadute**: dopo tentativi di interruzione, il soggetto tende a riprendere l'attività con le stesse modalità disfunzionali.

Il ruolo dell'Istituto scolastico

L'obiettivo è promuovere una cultura digitale consapevole, aiutare gli alunni a distinguere un sano utilizzo della rete da un comportamento compulsivo, e incoraggiarli a gestire il tempo online evitando il sovraccarico informativo.

Attraverso attività educative e laboratori mirati, si intende rafforzare nei giovani la capacità di autocontrollo e di discernimento, fornendo strumenti per vivere la dimensione digitale in modo equilibrato e responsabile.

Sexting: un rischio concreto nell'uso inconsapevole della rete

Tra i pericoli più comuni legati a un utilizzo non responsabile di Internet da parte dei più giovani vi è il fenomeno del *sexting*. Questo termine si riferisce allo scambio di immagini, video o messaggi a contenuto sessuale esplicito, spesso generati e inviati direttamente dagli stessi adolescenti. Ciò avviene, nella maggior parte dei casi, senza piena consapevolezza delle implicazioni legali ed emotive che tale comportamento può comportare.

Molti ragazzi e ragazze, infatti, non si rendono conto che la condivisione di materiale intimo, soprattutto se ritrae minorenni, può configurare il reato di diffusione di contenuti pedopornografici, anche se le immagini sono inviate in un contesto di fiducia, ad esempio all'interno di una relazione sentimentale. Una volta che questi contenuti vengono diffusi, è quasi impossibile controllarne la circolazione, e ciò può generare conseguenze gravi per chi ne è protagonista.

Diffusione incontrollata e revenge porn

Le immagini o i video sessualmente espliciti, una volta condivisi tramite smartphone (attraverso messaggi, bluetooth, e-mail o piattaforme social), possono circolare in modo incontrollato, anche se inizialmente destinati a una cerchia ristretta. Questo rende il fenomeno particolarmente pericoloso.

Quando questi contenuti vengono utilizzati per vendetta o ricatto, si parla di *revenge porn* (vendetta porno), ossia della diffusione non autorizzata di materiale intimo con l'intento di ferire o umiliare l'altro. In Italia, questo reato è stato formalmente riconosciuto con la Legge n. 69 del 19 luglio 2019, che ha introdotto l'art. 612-ter del Codice Penale, punendo la "diffusione illecita di immagini o video sessualmente espliciti".

Caratteristiche del fenomeno

Il sexting e le sue conseguenze presentano tre elementi principali:

- **Tradimento della fiducia**: chi invia contenuti intimi lo fa spesso in un contesto di fiducia, talvolta per rispondere a richieste presentate come prove d'amore.
- **Capacità virale della rete**: bastano pochi clic perché immagini o video si diffondano a un pubblico vastissimo, su numerose piattaforme. Il contenuto, una volta circolato, può essere scaricato, modificato e redistribuito, rendendo impossibile eliminarlo del tutto.
- **Persistenza del materiale online**: una volta pubblicato o condiviso, il contenuto può restare disponibile sulla rete per un tempo indefinito, riaffiorare anche a distanza di anni, e continuare a causare danni nel tempo.

Conseguenze emotive e psicologiche

Le conseguenze del sexting, in particolare quando sfociano nel revenge porn, possono essere molto gravi. I soggetti coinvolti possono sperimentare forme di disagio psicologico come:

- senso di umiliazione;
- perdita di fiducia nelle relazioni;
- ansia, depressione, isolamento sociale;
- molestie e cyberbullismo;
- danni alla sfera affettiva e sessuale;
- difficoltà a vivere serenamente il proprio corpo e la propria identità.

L'impegno dell'Istituto

Per contrastare questi fenomeni, l'Istituto scolastico ritiene fondamentale attivare percorsi educativi mirati alla prevenzione del disagio giovanile. Tali percorsi mirano alla promozione del benessere individuale e relazionale, affinché i ragazzi possano imparare a rispettare sé stessi e gli altri anche nel contesto digitale.

Tra i temi affrontati:

- educazione all'affettività e alla sessualità;
- sviluppo dell'autostima e della consapevolezza di sé;
- alfabetizzazione emotiva;
- dinamiche relazionali e capacità di cooperazione;
- uso consapevole della rete e prevenzione dei comportamenti a rischio.

Attraverso queste attività, l'Istituto si propone di creare un ambiente educativo sicuro e informato, in cui le nuove generazioni possano acquisire gli strumenti necessari per affrontare responsabilmente la vita digitale e costruire relazioni sane e rispettose.

Adescamento Online: una minaccia da conoscere e prevenire

Il **grooming**, termine inglese che significa "prendersi cura", è una forma subdola di **manipolazione psicologica** messa in atto da adulti con intenti sessuali nei confronti di minori. Questi soggetti, approfittando della vulnerabilità emotiva di bambini e adolescenti, instaurano un legame affettivo apparentemente rassicurante con l'obiettivo di superare le loro difese e spingerli in relazioni intime o sessualizzate. Internet rappresenta un mezzo privilegiato per questi tentativi, grazie alla facilità con cui si possono contattare i giovani attraverso chat, social network, app di messaggistica istantanea e piattaforme di giochi online.

Il fenomeno dell'**adescamento online** – noto anche come **grooming** – è oggi riconosciuto come **reato** nel nostro ordinamento giuridico, a partire dal 2012 con l'introduzione dell'art. 609-undecies del Codice Penale, dopo la ratifica della **Convenzione di Lanzarote** (Legge 172/2012). Anche un semplice tentativo, senza che avvenga un incontro fisico, è sufficiente per configurare l'illecito.

Le dinamiche del grooming

Il processo manipolativo si articola in diverse fasi, che si susseguono in modo graduale:

1. **Contatto iniziale e socializzazione**: l'adulto adescatore cerca di entrare in confidenza con il minore, ponendo domande personali e mostrando interesse verso i suoi gusti e problemi.
2. **Valutazione del rischio**: cerca di capire quanto il minore sia controllato dagli adulti e quanto sia isolato, tentando di spostare la comunicazione su canali più privati.
3. **Costruzione della fiducia**: il rapporto diventa più intimo. L'adulto può inviare piccoli regali o farsi inviare foto,

anche se inizialmente non a sfondo sessuale.

4. **Esclusività**: il contatto viene reso segreto, isolando progressivamente la vittima da familiari e amici. In questa fase possono comparire i primi ricatti emotivi.
5. **Sessualizzazione del rapporto**: l'adulto chiede contenuti espliciti o propone incontri fisici. Può arrivare a minacciare la vittima con la diffusione di immagini precedentemente ricevute, cercando di normalizzare il comportamento.

Le ragioni della vulnerabilità adolescenziale

Durante l'adolescenza, i ragazzi sono in una fase delicata di **costruzione della propria identità**. Il bisogno di sentirsi accettati e apprezzati, anche dal punto di vista estetico, li rende più esposti a lusinghe e attenzioni apparentemente innocue. Quando si rendono conto di essere stati ingannati, provano spesso vergogna, senso di colpa e perdita di autostima.

Come riconoscere l'adescamento

Un campanello d'allarme importante è rappresentato da **cambiamenti improvvisi nel comportamento** del minore, come chiusura, nervosismo o disagio nell'uso del dispositivo elettronico. È quindi fondamentale mantenere un dialogo aperto e non giudicante con bambini e adolescenti, così che possano confidarsi senza timore.

Come intervenire in caso di sospetto

In presenza di un sospetto o di un caso certo di adescamento:

- **Non rispondere** direttamente all'adescatore al posto del minore.
- **Non utilizzare** il dispositivo coinvolto per non compromettere le prove.
- **Conservare ogni traccia** utile (screenshot, video, chat, immagini).
- **Contattare subito la Polizia Postale**.
- **Valutare un supporto psicologico** per il minore, attraverso consultori, neuropsichiatria infantile o altri servizi territoriali.

In casi gravi, in cui l'adescamento sfoci in abusi sessuali, è indispensabile **l'intervento tempestivo di professionisti** qualificati per la tutela psicologica e legale della vittima.

Educazione e prevenzione

Il ruolo della scuola è fondamentale non solo nella **segnalazione** degli episodi, ma soprattutto nella **prevenzione**. L'Istituto ha attivato da tempo uno **sportello d'ascolto** e favorisce occasioni di confronto diretto tra studenti, insegnanti e famiglie.

Per contrastare l'adescamento è necessario accompagnare i giovani in un **percorso educativo strutturato**, che li aiuti a sviluppare:

- Alfabetizzazione emotiva
- Autostima e consapevolezza di sé
- Competenze relazionali e sociali
- Capacità di cooperazione
- Educazione all'affettività e alla sessualità

Particolare attenzione va posta all'**educazione digitale**, che deve comprendere anche l'uso consapevole dei social media, la protezione della propria **privacy online**, la **gestione dell'identità virtuale** e la comprensione del valore delle proprie immagini.

Una cultura dell'affetto e del rispetto

Il web trasmette spesso immagini distorte della sessualità, fondate su **stereotipi di genere** e su una visione priva di

empatia o rispetto. Educare gli adolescenti al rispetto di sé e degli altri significa anche offrir loro strumenti per **distinguere relazioni autentiche da quelle tossiche o manipolative**.

Collaborazione tra scuola, famiglie e istituzioni

Il contrasto all'adescamento richiede una **sinergia tra scuola, famiglie, servizi del territorio, Forze dell'Ordine** e figure professionali. Insieme, possiamo costruire un ambiente sicuro e protettivo, in cui i giovani possano crescere serenamente, sviluppare fiducia in se stessi e sentirsi ascoltati.

Per supporto e orientamento, è attivo il servizio **Helpline di Generazioni Connesse** (numero 19696), rivolto a studenti, genitori, insegnanti e operatori scolastici.

Pedopornografia online: un reato grave e un fenomeno da contrastare

La pedopornografia su Internet rappresenta un grave reato disciplinato dall'art. 600-ter, comma 3, del Codice Penale. Essa consiste nella produzione, diffusione, promozione e condivisione – anche tramite strumenti telematici – di immagini o video che ritraggono minori coinvolti in attività sessualmente esplicite, reali o simulate, o che mostrano i loro organi genitali con finalità di natura sessuale.

Un passo decisivo nella lotta contro questo fenomeno è stato compiuto con la Legge n. 269 del 3 agosto 1998, che ha introdotto nuove fattispecie di reato legate allo sfruttamento sessuale dei minori, tra cui il cosiddetto turismo sessuale. Successivamente, la Legge n. 38 del 6 febbraio 2006 ha rafforzato le misure di contrasto, includendo tra le altre il reato di **pornografia minorile virtuale**: si tratta di rappresentazioni digitali di bambini e adolescenti create graficamente, non tratte da situazioni reali, ma con un livello di realismo tale da sembrare autentiche.

Con l'adesione alla **Convenzione di Lanzarote** tramite la Legge 172/2012, l'Italia ha ulteriormente ampliato la definizione di pornografia minorile, includendo ogni rappresentazione, attraverso qualsiasi mezzo, di un minore di 18 anni in attività sessuali esplicite (vere o simulate) o immagini dei loro organi sessuali a scopi sessuali.

Sebbene la pedopornografia sia un fenomeno esistente da tempo, l'avvento e la diffusione di Internet ne hanno facilitato la produzione e la distribuzione, moltiplicando i canali di accesso e rendendo il materiale più facilmente reperibile.

La prevenzione: un compito educativo e sociale

Affrontare questo argomento richiede grande delicatezza, tenendo conto dell'età e del livello di maturità degli interlocutori, così da scegliere con cura le informazioni da trasmettere. È importante parlarne, soprattutto per chiarire i rischi collegati a comportamenti come il sexting e per promuovere una maggiore consapevolezza tra adulti e ragazzi.

È fondamentale sensibilizzare anche genitori, insegnanti ed educatori attraverso progetti formativi e informativi. In questo senso, l'Istituto propone percorsi specifici volti alla prevenzione del disagio giovanile e alla promozione del benessere psicologico e relazionale degli studenti. Le tematiche trattate includono:

- alfabetizzazione emotiva;
- sviluppo dell'autostima;
- dinamiche relazionali e socializzazione;
- collaborazione e cooperazione;
- educazione all'affettività e alla sessualità.

Strumenti e servizi per la segnalazione

Chiunque si imbatta in contenuti pedopornografici online è invitato a segnalarli tempestivamente, anche in forma anonima, attraverso la sezione "Segnala contenuti illegali" presente sul sito www.generazioniconnesse.it. I servizi del *Safer Internet*

Centre, come “Clicca e Segnala” di **Telefono Azzurro** e “STOP-IT” di **Save the Children**, sono attivi per ricevere queste segnalazioni.

Le informazioni raccolte vengono trasmesse alle autorità competenti, con l’obiettivo di rimuovere rapidamente il materiale illegale dalla rete, avviare le necessarie indagini e, cosa più importante, identificare le vittime di abuso per interrompere eventuali violenze in corso e offrire loro il supporto necessario.

Supporto psicologico e interventi istituzionali

Nel caso in cui un minore venga esposto a contenuti di questo tipo, è essenziale considerare anche il suo benessere psicofisico. Può essere utile rivolgersi al medico di base, al pediatra o ai servizi sanitari territoriali, come i Consultori Familiari, i Servizi di Neuropsichiatria Infantile o i centri specializzati nella tutela dell’infanzia.

Chi è a conoscenza di casi riconducibili a reati di pedopornografia può rivolgersi a:

- Polizia di Stato – Compartimenti di Polizia Postale e delle Comunicazioni
- Questura o Commissariato di Polizia
- Arma dei Carabinieri – Comandi o Stazioni territoriali
- Commissariato Online della Polizia di Stato

4.2 - Quali strumenti e a chi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

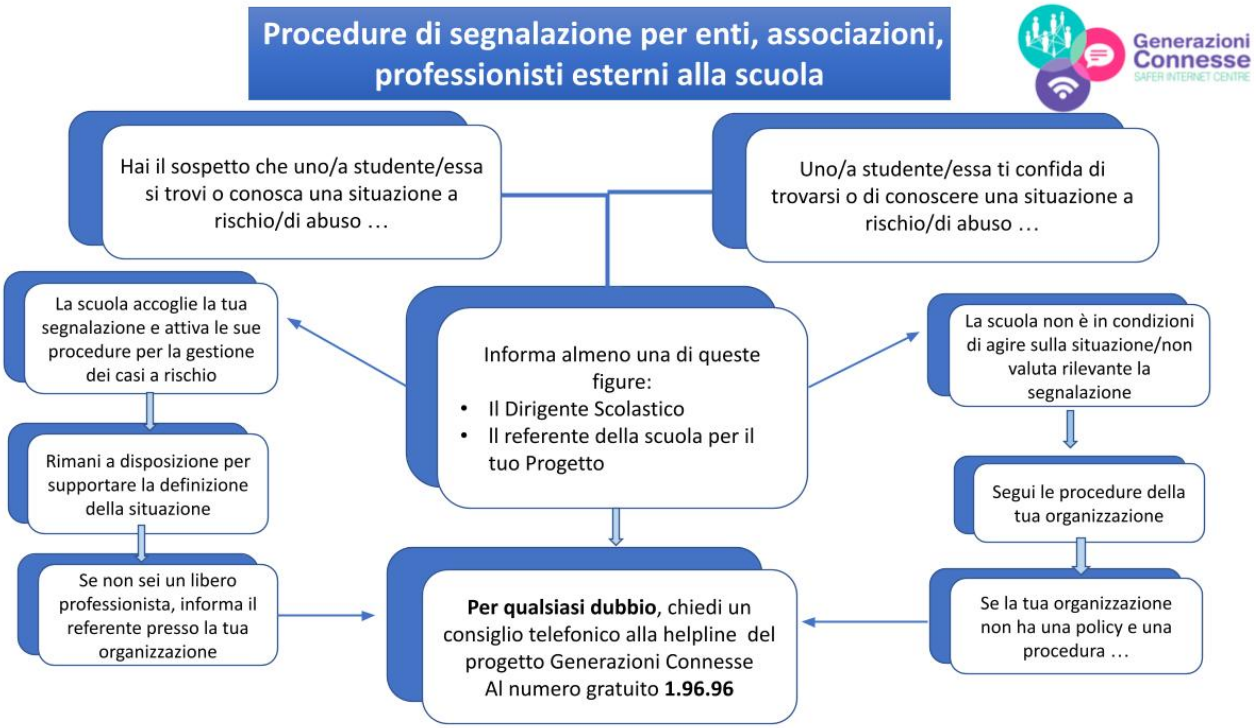
Strumenti a disposizione di studenti/esse

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

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

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

Procedure



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

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

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

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

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

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

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo

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

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

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

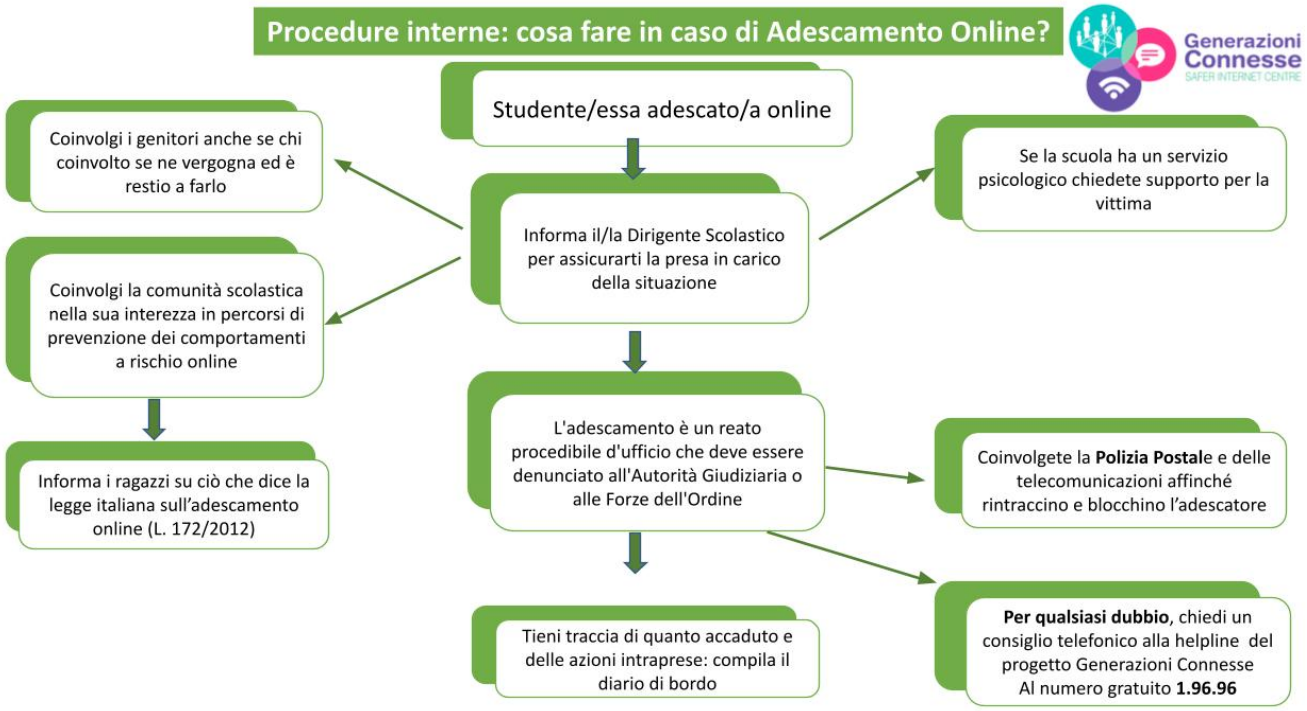
Se emergono evidenze passa allo schema successivo

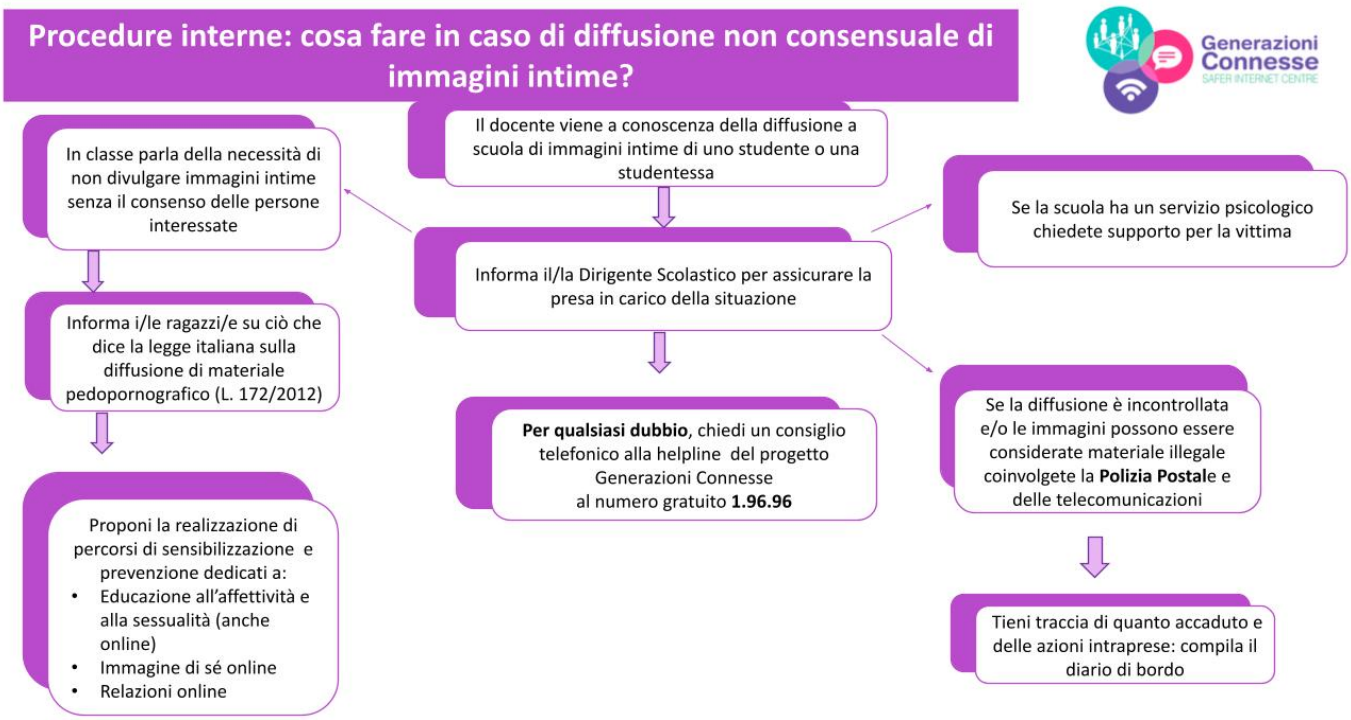
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

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

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

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


Procedure interne: cosa fare in caso di Adescamento Online?
Generazioni Connesse
SAFER INTERNET CENTRE
Studente/essa adescato/a online
Coinvolgi i genitori anche se chi coinvolto se ne vergogna ed è restio a farlo
Informa il/la Dirigente Scolastico per assicurarti la presa in carico della situazione
Se la scuola ha un servizio psicologico chiedete supporto per la vittima
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)
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


Procedure interne: cosa fare in caso di diffusione non consensuale di immagini intime?
Generazioni Connesse
SAFER INTERNET CENTRE
In classe parla della necessità di non divulgare immagini intime senza il consenso delle persone interessate
Il docente viene a conoscenza della diffusione a scuola di immagini intime di uno studente o una studentessa
Se la scuola ha un servizio psicologico chiedete supporto per la vittima
Informa il/la Dirigente Scolastico per assicurare la presa in carico della situazione
Informa i/le ragazzi/e su ciò che dice la legge italiana sulla diffusione di materiale pedopornografico (L. 172/2012)
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse al numero gratuito 1.96.96
Se la diffusione è incontrollata e/o le immagini possono essere considerate materiale illegale coinvolgete la Polizia Postale e delle telecomunicazioni
Proponi la realizzazione di percorsi di sensibilizzazione e prevenzione dedicati a:
• Educazione all'affettività e alla sessualità (anche online)
• Immagine di sé online
• Relazioni online
Tieni traccia di quanto accaduto e delle azioni intraprese: compila il diario di bordo