Generazioni Connesse
SAFER INTERNET CENTRE
MIM Ministero dell'Istruzione e del Merito
Co-funded by the European Union

Documento di ePolicy

ISTITUTO COMPRENSIVO BOVA MARINA - CONDOFURI - BRANCALEONE - BRUZZANO

Via Montesanto, 26 – 89035
BOVA MARINA

Cap 1 - Lo scopo della ePolicy

1.1 Scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

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

Capitolo 2 - Sensibilizzazione e prevenzione

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

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

Capitolo 4 - Segnalazione e gestione dei casi

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

1.1 Scopo dell'ePolicy

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

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

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

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

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

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

Le principali aree di rischio per la nostra comunità scolastica riguardano i seguenti ambiti:

- **contenuto**: esposizione a contenuti e siti web non adeguati e non in linea con le finalità educative di Istituto, problemi legati all'autenticità e all'esattezza dei contenuti online;
- **contatto**: grooming (adescamento), cyberbullismo in tutte le sue forme, furto di identità;
- **condotta**: violazione della privacy (ad es. divulgazione di informazioni personali), reputazione online, diritti e doveri degli internauti (elementi fondamentali di Cittadinanza Digitale), netiquette, salute e benessere (quantità di tempo speso online su Internet o giochi), sexting (invio e ricezione di immagini personali intime), il rispetto del Copyright.

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.

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.

Si ricorda che per normativa vigente, s**ono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali o abusivi, o che mettano a rischio la loro sicurezza.**

Pertanto tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

In coerenza con il percorso intrapreso dal nostro Istituto viene predisposta un'informativa sintetica sull'ePolicy comprensiva delle "procedure di segnalazione" in caso di illecito e di episodi che mettano in pericolo studenti e studentesse.

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.

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'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

Come da regolamento d'istituto è vietato l'uso di qualsiasi dispositivo digitale personale durante l'orario scolastico, tranne nel caso in cui venga proposta un'attività didattica da parte dell'insegnante, in sua presenza e sotto la sua supervisione. Diversamente, è fatto divieto assoluto agli alunni di utilizzare qualsiasi dispositivo digitale in classe, nei corridoi, nei bagni e in qualsiasi altro locale della scuola, compreso il cortile, durante la ricreazione. Il cellulare dovrà essere tenuto spento e riposto dentro lo zaino dal momento dell'ingresso fino alla fine delle lezioni.

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

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.

Il nostro Istituto, per l'anno scolastico 2024-2025 ha creato, in collaborazione con tutti gli studenti del plesso della scuola secondaria, un decalogo per la prevenzione al cyberbullismo, a partire dalla lettura di un fumetto sul tema.

Quello che segue è il risultato del lavoro prodotto dagli studenti della scuola secondaria di I grado.

DECALOGO PER LA PREVENZIONE AL CYBERBULLISMO

1 Pensa sempre alle conseguenze delle tue azioni e non sottovalutare i rischi della rete.
2 Ricordati che lo schermo "aumenta le distanze": scrivi solo ciò che diresti anche a voce.
3 Non fare agli altri quello che non vorresti fosse fatto a te.
4 Aiuta le persone prese di mira, perché "da soli si va veloci, insieme si va lontano"
5 Non condividere dati sensibili e materiale privato: è un rischio.
6 Parla con un amico, se ti senti in pericolo.
7 Chiedi aiuto ad un adulto di cui ti fidi o alla polizia postale, se sei una vittima di cyberbullismo o se è stata violata la tua privacy.
8 Se vedi una situazione sospetta, non ignorarla.
9 Rispetta gli altri, rispetta te stesso.
10 Rendi il web e i social un posto migliore: con il tuo comportamento puoi fare la differenza!

Cosa prevedeva la legge 71/2017 e come è stata integrata dalla nuova legge 70/2024 sul bullismo e cyberbullismo

La legge 71/17 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" è nata

per tutelare il diritto delle nuove generazioni di navigare in rete in modo sicuro, positivo e libero. Ma non solo: prevede linee di orientamento per contrastare il cyberbullismo all'interno delle scuole. È una legge pensata sia per i colpevoli, che per le vittime.

Oggi però, le linee guida delineate da quella legge del 2017 risultavano insufficienti. Per questo, il governo ha deciso di integrare la legge introducendo innovazioni attraverso la nuova legge 70/24. Pubblicata sulla Gazzetta Ufficiale il 30 maggio 2024, descritta come "Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e del cyberbullismo", questa legge estende le disposizioni della 71/17 anche ai fenomeni del bullismo, con la finalità di prevenire e contrastare entrambe le azioni considerate oggetto del reato. All'uopo si precisa che se l'autore del reato ha un'età inferiore ai 14 anni, a risponderne saranno i genitori. Diversamente, chi adotta questi comportamenti supera i 14 anni di età, è bene sapere che con l'avvento della nuova legge bullismo e cyberbullismo diventano veri e propri reati a sé stanti, punibili penalmente con pena detentiva (da 1 a 7 anni) per chiunque minaccia o molesta un'altra persona di qualunque sesso e razza, con condotte reiterate e mediante violenza, atti ingiuriosi, denigratori e diffamatori nei suoi confronti. Ma non finisce qui: se questi atti avvengono per mezzo di una o più persone con testimoni al seguito, la legge punisce con la reclusione anche chi è testimone di tali atti e non interviene o denuncia (con detenzione dai 6 mesi ai 3 anni).

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.

Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società". Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico" ("Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente" C189/9, p.9).

La legge n. 92/2019 così come integrata dalla legge n. 21/2025 in ordine all'introduzione delle conoscenze di base in materia di sicurezza nei luoghi di lavoro e al Decreto Ministeriale n. 183/2024, ha introdotto l'insegnamento trasversale dell'educazione civica, i cui nuclei fondanti: Costituzione, Sviluppo economico e sostenibilità, Cittadinanza digitale sono parte

integrante del nostro curricolo verticale di ed. civica (prot. 9724 - 18/12/2024 - IV.1 – I).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale.

Avere competenza digitale significa padroneggiare le nuove tecnologie, ma soprattutto usarle con “autonomia e responsabilità” nel rispetto degli altri.

Le raccomandazioni Europee ci ricordano la dimensione integrata degli aspetti tecnologici, cognitivi ed etici che coesistono nelle competenze digitali:

- dimensione tecnologica: le tecnologie digitali sono indubbiamente strumenti per la risoluzione di molteplici problemi della vita quotidiana, ma possiedono una "grammatica" che occorre gradualmente imparare a conoscere;
- dimensione cognitiva: essa fa riferimento alla capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità;
- dimensione etica e sociale: fa riferimento sia alla capacità di gestire in modo sicuro i dati personali e altrui che alle abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online.

In ottemperanza delle indicazioni del PNSD del 2015 (paragrafo 4.2. sulle "Competenze e contenuti") l’Istituto si propone un programma di progressiva educazione alla sicurezza online come parte del curriculum scolastico. Si impegna a sviluppare una serie di competenze e comportamenti, tra cui:

- progettare attività e laboratori di Coding;
- sviluppare strategie per insegnare a valutare e verificare le informazioni per accettarne l'esattezza;
- capire la necessità di mettere in atto un comportamento corretto anche quando si utilizza un ambiente online;
- sapere che le identità online possono essere false e ingannevoli;
- comprendere che le informazioni personali pubblicate online sono vulnerabili; conoscere le principali regole che tutelano la privacy delle persone; con particolare attenzione al web, conoscere le principali regole del copyright;
- comprendere l'impatto di bullismo online, sexting, grooming e sapere come cercare aiuto in caso di pericolo;
- sapere come segnalare eventuali abusi on-line e come chiedere aiuto agli adulti.

Analogamente, si allinea ai contenuti del DigComp 2.1 del 2017, documento che contiene l'evoluzione del quadro di riferimento per le competenze digitali dei cittadini, elencando otto livelli di padronanza per ciascuna delle cinque aree della cittadinanza digitale:

1. Alfabetizzazione e dati: ovvero la capacità di cercare, selezionare e valutare le informazioni in Rete;

2. Comunicazione e collaborazione: saper riconoscere le giuste e appropriate modalità per comunicare e relazionarsi online;

3. Creazione di contenut i digitali: valutare le modalità più appropriate per modificare, migliorare e integrare contenuti e informazioni, creandone di nuovi e originali;

4. Sicurezza: imparare a proteggere i dati personali e i contenuti digitali, comprendendo i rischi e le minacce presenti negli ambienti digitali.

5. Risoluzione dei problemi: riconoscere e fronteggiare eventuali problemi tecnici, utilizzare in modo creativo le risorse digitali, individuare e colmare eventuali divari digitali.

Il DigComp 2.2 del 2022, oltre a incoraggiare la costruzione di legami tra la competenza digitale e le altre competenze, contiene un aggiornamento specifico per la Dimensione 4 (Conoscenze, abilità e attitudini applicabili a ciascuna competenza) delle Competenze Digitali. Il documento, infatti, è finalizzato ad incentivare "l'utilizzo delle tecnologie digitali con fiducia, in modo critico e sicuro". Il nostro Istituto quindi si sta impegnando per:

- affrontare i temi della malainformazione e della disinformazione nei social media e nei siti di notizie (fact-checking delle informazioni e delle loro fonti, fake news, deep fakes);
- insegnare a proteggere i propri dati personali e la privacy, introducendo anche alcune considerazioni etiche;
- proteggere la propria salute e il benessere;
- insegnare ad utilizzare correttamente (netiquette) i diversi strumenti tecnologici, sia in ambito personale che educativo;
- stimolare ad esercitare costruttivamente la propria cittadinanza digitale, agendo anche in rete come cittadini responsabili e partecipi della vita civile e sociale.

2.3 - Il Kit Didattico

L'e-Policy prevede, a livello macro, un lavoro di lettura e d'intenti condivisi dall'intera comunità scolastica, a livello micro,

invece, immagina che la singola classe lavori anche su tematiche direttamente collegate alla sicurezza in rete, ma complesse e di non immediata ricaduta nelle programmazioni scolastiche (etica e digitale, algoritmi, datafication). A tal fine si è progettato e predisposto del materiale che possa funzionare sia da attivatore, sia d'accompagnamento ai docenti e agli studenti nella fase più delicata ed incisiva del processo di prevenzione: la lezione in classe.

Pertanto, il progetto Generazioni Connesse, a supporto del lavoro dell'e-Policy ha previsto per i docenti e studenti di ogni segmento scolare un nuovo Kit Didattico che contiene materiali per le lezioni e per il proprio aggiornamento, a partire dalla scuola d'infanzia fino alla secondaria di secondo grado. Il Kit può essere usato nella sua interezza oppure può essere oggetto di selezione e scelta, sulla base di quanto fatto dal docente.

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

3.1 - Protezione dei dati personali e GDPR

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

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

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

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

Nell'Istituto sono presenti i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali. Sono "dati personali" le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona e che possono fornire molteplici informazioni sul suo conto (dai dati anagrafici a quelli "sensibili", di natura religiosa, etnica... fino a quelli giudiziari). Il "trattamento" di questi dati sono l'insieme di operazioni, digitalizzate e non, applicate ad essi e l'istituzione scolastica può trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali o quelli previsti dalla norma di settore. Un esempio di violazione della protezione dei dati personali è il trattamento di questi senza aver fornito all'interessato un'adeguata informativa in merito, o senza aver ricevuti uno specifico consenso.

Il nostro Istituto possiede tre modelli:

- due modelli per il trattamento dei dati personali di studenti/genitori (modello A) e del personale;
- una liberatoria per l'autorizzazione all'uso della piattaforma di Microsoft 365 da parte degli studenti.

1. MODELLO DI LIBERATORIA per la protezione dei dati personali degli alunni e dei loro genitori o tutori

INFORMATIVA PRIVACY AI SENSI DEL REGOLAMENTO UE 2016/679 PER IL TRATTAMENTO DEI DATI DEGLI ALUNNI E DEI LORO GENITORI O TUTORI

Titolare del trattamento: il Titolare del trattamento dei dati è ISTITUTO COMPRENSIVO BOVA MARINA - CONDOFURI - BRANCALEONE - BRUZZANO, (telefono 0965.923605 – email rcic85200d@istruzione.it) nella persona del Dirigente Scolastico, legale rappresentante dell'Istituto, Dott. Fortunato Surace.

Responsabili del trattamento: l'elenco dei responsabili esterni del trattamento dei dati personali, costantemente aggiornato, è disponibile presso il titolare su esplicita e motivata richiesta.

Responsabile Protezione dei Dati. Dott. Grimaldi Mario - tel. 3493424766 - email. dpo.grimaldi@proton.ne

Finalità: i dati personali forniti alla presente Istituzione scolastica, anche se raccolti presso il Ministero dell'Istruzione e le sue articolazioni periferiche, saranno trattati dal personale della scuola soltanto nell'ambito delle finalità istituzionali, che sono quelle relative all'istruzione ed alla formazione degli alunni e quelle amministrative ad esse strumentali. Il trattamento dei dati sarà improntato ai principi di correttezza, liceità, trasparenza, limitazione delle finalità, esattezza, limitazione della conservazione, integrità e tutela della riservatezza e dei diritti individuali. I dati personali saranno trattati esclusivamente dal personale della scuola, appositamente incaricato, secondo quanto previsto dalle disposizioni di Legge e di Regolamento nel rispetto del principio di stretta indispensabilità dei trattamenti.

Conservazione e trattamento: i dati saranno conservati presso gli archivi del Titolare per tutta la durata del rapporto tra la famiglia e l'istituzione scolastica, per l'espletamento di tutti gli adempimenti di legge e per un tempo non superiore agli scopi per i quali sono stati raccolti. I dati saranno altresì comunicati esclusivamente ai soggetti competenti per l'espletamento di servizi necessari ad una corretta gestione del rapporto scolastico, con garanzia di tutela dei diritti dell'interessato. Sono autorizzati al trattamento dei dati: il personale amministrativo, tecnico e ausiliario in servizio presso l'Istituto; i docenti in servizio presso l'Istituto; eventuali docenti ed esperti esterni incaricati dalla scuola di svolgere attività di ampliamento dell'offerta formativa, come previsto dal PTOF. Il personale incaricato ha accesso ai dati a seconda delle mansioni e si attiene alle norme impartite e alle disposizioni di legge. È vietato all'incaricato qualsiasi forma di diffusione e comunicazione di dati personali che non sia funzionale allo svolgimento dei compiti affidati ed è adeguatamente istruito sulle norme privacy previste dal Regolamento Ue 2016/679.

Il trattamento sarà effettuato sia con strumenti cartacei che elettronici, nel rispetto delle misure di sicurezza minime, così come previsto dal Regolamento Europeo, ad opera di soggetti appositamente incaricati.

Legittimazione e consenso: nel corso del rapporto con la presente Istituzione scolastica, i dati personali verranno trattati dal personale della scuola nell'ambito delle finalità istituzionali, così come definite dalla normativa vigente: R.D. n. 653/1925, D.Lgs n. 297/1994, D.P.R. n. 275/1999; D.I. n. 44/2001 e le norme in materia di contabilità generale dello Stato; L. n. 104/1992, L. n. 53/2003, D.Lgs n. 165/2001, D.Lgs 196/2003, D.M 305/2006; D.Lgs 76/05; D.Lgs 77/05; D.Lgs 226/05; D.Lgs n. 151/2001; D.P.C.M. n. 185/2006; D.P.R. n. 89/2009; L. 170/2010; D.M. n. 5669/2011; D.P.R. 80/2013, D. Lgs 33/2013, D.L. 104/2013, convertito, con modificazioni, dalla L. 128/2013, L. 107/2015, D. Lgs 50/2016 e relativi decreti applicativi e tutta la normativa collegata alle citate disposizioni.

Si fa presente che il conferimento dei dati richiesti e il conseguente trattamento sono obbligatori, in quanto previsti dalla normativa sopra citata; l'eventuale rifiuto a fornire tali dati potrebbe comportare il mancato perfezionamento dell'iscrizione e l'impossibilità di fornire all'alunno tutti i servizi necessari per garantire il suo diritto all'istruzione ed alla formazione. Dovrà essere invece ottenuto dalla presente Istituzione scolastica il consenso dell'interessato per raccogliere e trattare i dati relativamente ai trattamenti complementari alle finalità istituzionali.

Destinatari: i dati personali potranno essere comunicati a soggetti pubblici (quali, ad esempio, ASL, Comune, Provincia, Ufficio scolastico regionale, Ambiti Territoriali, organi di polizia giudiziaria, organi di polizia tributaria, guardia di finanza, magistratura) nei limiti di quanto previsto dalle vigenti disposizioni di Legge e di Regolamento e degli obblighi conseguenti per codesta Istituzione scolastica; i dati relativi agli esiti scolastici degli alunni potranno essere pubblicati mediante affissione all'albo della scuola secondo le vigenti disposizioni in materia. I dati da forniti potranno essere comunicati altresì alle altre istituzioni scolastiche, statali e non statali, per la trasmissione della documentazione attinente alla carriera scolastica degli alunni, limitatamente ai dati indispensabili all'erogazione del servizio. Potranno infine venire a conoscenza

dei dati personali terzi soggetti che forniscono, a questa Istituzione scolastica, servizi strumentali (alle finalità di cui sopra), ferma restando la garanzia di tutela dei diritti dell'interessato. Tali soggetti agiranno in qualità di Responsabili o Incaricati del trattamento. La realizzazione di questi trattamenti costituisce una condizione necessaria affinché l'interessato possa usufruire dei relativi servizi.

Ai sensi dell'art. 96 del Codice della Privacy, ferma restando la tutela della riservatezza dell'alunno, al fine di agevolare l'orientamento, la formazione e l'inserimento professionale dell'alunno, i dati relativi agli esiti scolastici, intermedi e finali, e altri dati personali diversi da quelli sensibili o giudiziari, potranno essere comunicati o diffusi, anche a privati e per via telematica. La comunicazione avverrà esclusivamente a seguito di sua richiesta e i dati saranno poi trattati esclusivamente per le predette finalità.

I dati sensibili e giudiziari non saranno oggetto di diffusione; tuttavia, alcuni di essi potranno essere comunicati ad altri soggetti pubblici nella misura strettamente indispensabile per svolgere attività istituzionali previste dalle vigenti disposizioni di legge in materia sanitaria, previdenziale, tributaria, giudiziaria e di istruzione. I dati non verranno trasferiti a destinatari residenti in paesi terzi rispetto all'Unione Europea né ad organizzazioni internazionali, fatta eccezione per i casi in cui i dati siano gestiti in cloud ed i server siano fisicamente collocati all'estero. In ogni caso i server sono fisicamente ubicati in un paese appartenente all'Unione Europea.

Diritti: al Titolare del trattamento o al Responsabile l'interessato potrà rivolgersi senza particolari formalità, per far valere i propri diritti, così come previsto dal Regolamento Europeo 2016/679; ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile. L'interessato ha i seguenti diritti: di accesso; di rettifica; di cancellazione (diritto all'oblio); di limitazione del trattamento; di revoca del consenso, nei casi previsti dal Regolamento. L'interessato ha inoltre diritto alla portabilità dei dati e di proporre reclamo all'Autorità di controllo dello Stato di residenza (Garante Privacy).

Informazioni aggiuntive: per consentire ai genitori l'assolvimento dell'obbligo di garantire l'istruzione dei figli maggiorenni, che siano ancora non autosufficienti e conviventi, così come indicato dalle norme vigenti e dai pronunciamenti giurisprudenziali, è permesso ai genitori medesimi l'accesso alle informazioni riguardanti il rendimento scolastico e la frequenza dei figli maggiorenni rientranti nelle categorie sopra indicate (non autosufficienti e ancora conviventi).

..... lì .....2025 IL DIRIGENTE SCOLASTICO

Dott. Fortunato Surace

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 ad Internet

1. L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.

2. Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.

3. Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.

4. L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.

5. Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola".

Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

L'infrastruttura tecnologica dell'Istituto IC "BOVA MARINA - CONDOFURI - BRANCALEONE - BRUZZANO" è in parte cablata e principalmente funzionante tramite wi- fi.

La scuola dispone in tutte le sue sedi di una rete internet, cui accedono i computer delle aule e dei laboratori (rete didattica) separatamente da quelli dell'amministrazione (rete segreteria). Per quanto concerne la rete amministrativa, lo storage è garantito da backup automatico su altra postazione. L'ottenimento delle credenziali per l'utilizzo della rete wifi è riservato ai docenti e al personale dell'Istituto. Le regole di comportamento sono analoghe a quelle per la connessione alle reti cablate di Istituto.

L'Istituto può controllare periodicamente i file utilizzati, i file temporanei e i siti visitati da ogni dispositivo tramite la verifica della cronologia di navigazione. È vietato installare e scaricare da Internet software non autorizzati dall'amministrazione. L'utilizzo di unità di archiviazione e chiavette usb è autorizzata, previa opportuna scansione antivirus, per evitare qualsiasi tipo di infezione alla rete d'Istituto. Sui dispositivi della scuola non è garantito alcun servizio di backup.

Non è previsto l'accesso al wi-fi della scuola per gli studenti, che possono utilizzare la rete esclusivamente in presenza dei

docenti, attraverso gli strumenti informatici in dotazione nella scuola.

Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali. Il nostro istituto utilizza strumenti di comunicazione sia interni (come il registro elettronico, l'email, applicativi e piattaforme di lavoro condiviso come Onedrive) che esterni (il sito della scuola). Ecco gli strumenti e i canali di comunicazione online dell'Istituto:

- email. L'account di posta elettronica della scuola è quello istituzionale, rcic85200d@istruzione.it utilizzato dagli uffici amministrativi.
- Microsoft365 per l'attività didattica e nei periodi di attivazione della Didattica Digitale Integrata.
- sito istituzionale: https://www.icbovamarinacondofuri.edu.it/ La gestione del sito della scuola, la realizzazione, la progettazione e la rispondenza alle normative sono attualmente a cura della segreteria e di Easyteam.org. La scuola detiene i diritti d'autore (tramite protocollo informatico) dei documenti che si trovano sul proprio sito.
- Axios/Spaggiari : il registro elettronico che permette di gestire la comunicazione con le famiglie

---

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.

Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente ePolicy contiene 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 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.

La scuola fornisce un indirizzo di posta elettronica personale a tutti gli studenti, le studentesse e a tutto il personale docente, attivo per il tempo di permanenza nell'istituto (la scadenza degli accessi è programmata al 31 agosto dell'anno di fine percorso scolastico). Studenti e docenti possono utilizzarlo per accedere alla piattaforma e-learning e a tutte le attività proposte dalla scuola, nonché permette di mettere in contatto più facilmente studenti e docenti.

La scuola non consente l'utilizzo del cellulare personale degli alunni all'interno dell'Istituto e in orario scolastico, se non su esplicita autorizzazione del docente e per determinate attività didattiche, previo accordo con studenti/esse e genitori; la scuola deve chiedere ai genitori dei minori di 16 anni di età il consenso all'uso di Internet a scuola per

il loro figlio e per la pubblicazione dei suoi lavori e delle sue fotografie. Si ricorda che in Italia, con il recepimento del GDPR, l'età minima per l'accesso ai social network è di 14 anni, 13 con il consenso genitoriale (relativamente ai social statunitensi)

Il presente documento di e-Policy sanziona eventuali usi illeciti dei dispositivi digitali e l'Istituto è dotato di una P.U.A. (Politica d'Uso Accettabile delle tecnologie a scuola) sull'uso delle TIC.

Per i docenti e per il personale della scuola è consentito l'uso dello smartphone e di altri dispositivi elettronici personali durante le ore di lezione solo a scopo didattico ed integrativo di quelli scolastici disponibili.

La nostra scuola ha in progetto di dotarsi di una netiquette (ovvero tutte quelle regole di comportamento che devono essere osservate dagli utenti di Internet), da pensare, realizzare e condividere con studenti e genitori dell'Istituto.

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.

Tabella della gestione delle infrazioni all'e-Policy con annesse sanzioni disciplinari. La tabella è desunta dal Regolamento d'Istituto, recentemente aggiornato.

TABELLA SANZIONI DISCIPLINARI A CARICO DEGLI STUDENTI		
MANCANZA DISCIPLINARE	SANZIONE/ PROVVEDIMENTO	ORGANO COMPETENTE E PROCEDURA
Mancato assolvimento dei doveri scolastici (compiti a casa non svolti e dimenticanze per materiale didattico)	• Annotazione sul registro del docente (fino a 3 volte) • Comunicazione scritta alla famiglia.	Docente dell'ora interessata
Abbigliamento non idoneo al contesto scolastico ed educativo (come indicato nel Regolamento)	• Richiamo verbale (1 v.) • Comunicazione scritta alla famiglia. • Nota sul registro elettronico	Docente dell'ora interessata
Fumare all'interno dell'edificio e negli spazi esterni di pertinenza dell'edificio scolastico	• Nota sul registro elettronico (1v.), accompagnata da comunicazione scritta alla famiglia o telefonata a casa (a discrezione del docente) e sanzione amministrativa secondo le vigenti disposizioni di legge (multa di € 27,50 ai sensi L.10.01.2005); si aggiunge confisca del materiale e consegna ai genitori ed esclusione dalle uscite didattiche. • Dalla seconda violazione e per ogni successiva, sospensione dalle attività scolastiche da 1 a 2 giorni	Il docente che verificherà la trasgressione procederà alla verbalizzazione dell'infrazione e alla comunicazione necessaria all'amministrazione per l'irrogazione della sanzione amministrativa. Se la trasgressione verrà contestata da personale diverso dal docente dell'ora interessata, lo stesso comunicherà la trasgressione al coordinatore di classe. Dalla seconda violazione in poi il coordinatore di classe segnalerà al Dirigente la mancanza disciplinare, il quale convocherà il Consiglio di Classe per la contestazione di addebito.
Disturbi reiterati e intenzionali dell'attività didattica	• Richiamo verbale (1 v.) • Annotazione sul registro elettronico • Nota sul registro di classe (2v.) • Convocazione dei genitori • Richiamo del Dirigente.	Docente dell'ora interessata o Coordinatore di classe ed eventualmente il Dirigente scolastico.

Allontanamento dall'aula senza autorizzazione	• Richiamo verbale e convocazione dei genitori. • Nota sul registro di classe. • Comunicazione scritta alla famiglia • Richiamo del Dirigente.	Docente dell'ora interessata. Se la trasgressione verrà contestata da personale diverso dal docente dell'ora interessata, lo stesso comunicherà la trasgressione al docente in classe. Eventuale comunicazione al Dirigente scolastico.
Allontanamento dalla scuola senza autorizzazione	• Telefonata tempestiva alla famiglia, subito dopo si contattano le forze dell'ordine. Nota sul registro di classe. Richiamo del Dirigente. • Nel caso la famiglia dichiari per iscritto di essere in contatto con il figlio, non si chiamano le forze dell'ordine ma si annota la trasgressione sul registro di classe. Richiamo del Dirigente.	Docente dell'ora interessata e il Dirigente scolastico.
Scorrettezze, offese o molestie con parole, gesti o azioni verso il personale scolastico o i compagni.	• Richiamo verbale e nota sul registro elettromnico(a seconda della gravità è possibile adottare direttamente i provvedimenti successivi). (1v) • Richiamo da parte del Dirigente scolastico. • Esclusione dalla partecipazione alle uscite didattiche e convocazione dei genitori. (2v) A seconda della gravità anche sospensione dalle attività didattiche da 1 a 5 giorni e percorso di recupero educativo.	Docente dell'ora interessata, Coordinatore di classe ed eventualmente il Dirigente Scolastico. Se necessario, il Dirigente scolastico convocherà il consiglio di classe per discutere l'adozione della sanzione della sospensione.

Uso di telefoni cellulari e altri dispositivi elettronici senza il consenso del docente. Uso non consentito e/o scorretto della navigazione in rete L'alunno ha il cellulare acceso in mano o nello zaino. L'alunno utilizza il cellulare a scuola per chiamate e/o messaggistica o altri usi non consentiti (giochi, ascolto musica, ecc.) L'alunno fa foto e/o video in classe o negli ambienti della scuola, anche riprendendo se stesso o i compagni. L'alunno diffonde anche in rete e nei social network immagini/video/audio non autorizzati effettuati a scuola	Nel caso il docente non ne ottenesse la consegna spontanea, l'allievo verrà accompagnato dal Dirigente. Durante le attività parascolastiche l'uso del cellulare è vietato salvo autorizzazione. • Annotazione sul registro di classe elettronico e confisca immediata e convocazione dei genitori per la consegna del dispositivo utilizzato. • Metacognizione sul comportamento adottato • Intervento e richiamo del Dirigente. Uso che compromette in modo lesivo la dignità personale: • Confisca immediata con consegna ai genitori, allontanamento dello studente dalla comunità scolastica da 1 a 15 giorni. • Metacognizione sul comportamento adottato. • Esclusione dalla partecipazione a uscite didattiche, visite guidate, viaggi 'istruzione, in proporzione alla gravità della mancanza. • In caso di diffusione non autorizzata, convocazione della famiglia, provvedimento disciplinare di sospensione di almeno 15 giorni, in base alla gravità, ed eventuale denuncia alla polizia postale.	Il docente che verificherà la trasgressione procederà alla verbalizzazione dell'infrazione. Nei casi più gravi il docente segnalerà al Dirigente scolastico la mancanza disciplinare, il quale convocherà il Consiglio di Classe per la contestazione di addebito. In caso di episodio di Cyberbullismo o di violazione della privacy, il coordinatore di Classe informerà il Referente bullismo di Istituto o un membro della Commissione Bullismo (in caso la trasgressione si verifichi in uno dei plessi non della sede centrale) che poi riferirà al referente. Può rendersi necessario denunciare la trasgressione al Garante della Privacy.

Esercizio di qualsiasi forma di violenza fisica e/o atti di bullismo o presunto tale. Scorrettezze, offese o molestie con parole, gesti o azioni verso il personale scolastico o i compagni	• Nota disciplinare sul registro elettronico e convocazione della famiglia. • Metacognizione sul comportamento adottato • Allontanamento dello studente dall'istituzione scolastica, da 1 a 5 giorni. (1v) • Percorso di recupero educativo mediante la pedagogia del service learning per lo sviluppo del comportamento prosociale legato ad attività (al servizio della comunità) di cittadinanza attiva. A seconda della gravità è possibile adottare direttamente il secondo provvedimento. • Nel caso di violenze fisiche senza gravi conseguenze, provvedimento di sospensione dalle attività scolastiche da 1 a 3 giorni • Nel caso di violenze fisiche con gravi conseguenze e accertati atti di bullismo: allontanamento dalla comunità scolastica superiore da 3 a 15 giorni.	Il docente che verificherà la trasgressione procederà alla verbalizzazione dell'infrazione. In caso di presunto bullismo, viene coinvolto il Referente Bullismo della scuola e il dirigente scolastico. Nei casi più gravi il Dirigente scolastico, rilevata la mancanza disciplinare, convocherà il Consiglio di Classe per la contestazione di addebito.
Danneggiamento intenzionale e/o furto a strutture, arredi o attrezzature scolastiche.	• Nota disciplinare sul registro di classe elettronico e comunicazione ai genitori, riparazione economica del danno. (1v) • Metacognizione sul comportamento adottato • Percorso di recupero educativo. • Allontanamento dello studente dall'istituzione scolastica da 1 a 2 giorni. (2v) • Esclusione dalla partecipazione a uscite didattiche, visite guidate, viaggi d'istruzione, in proporzione alla gravità della mancanza.	Il docente dell'ora interessata avviserà tempestivamente il Dirigente scolastico, il quale darà tempestiva comunicazione alla famiglia e concorderà le modalità per la riparazione personale del danno. Se previsto, il Dirigente scolastico convocherà il Consiglio di classe per discutere la contestazione di addebito.
Comportamenti scorretti durante attività parascolastiche (uscite sul territorio, viaggi e visite d'istruzione, manifestazioni sportive, ecc...)	• Nota sul registro di classe, seguita da convocazione della famiglia • Richiamo da parte del Dirigente scolastico • Provvedimento di sospensione dalle attività scolastiche da 1 a 3 giorni o superiore	In caso di gravità, verrà informato il Dirigente scolastico per la mancanza disciplinare, il quale si riserverà di convocare il Consiglio di Classe per discutere la contestazione di addebito.

Il nostro Istituto ritiene importante che le sanzioni possano trasformarsi anche in occasione di recupero e di crescita. Accanto ad esse, infatti, è opportuno stimolare comportamenti, volti al perseguimento di una finalità educativa. Risulta perciò possibile commutare il provvedimento di sospensione con attività socialmente utili alla comunità scolastica o ad associazioni convenzionate, quali:

- Attività di studio e ricerca a favore della classe e/o della comunità scolastica;
- Preparazione di materiale da utilizzare nell'ambito di attività didattiche;
- Riordino della biblioteca scolastica e/o di materiali utilizzati nelle lezioni di scienze motorie, arte o musica;

- Altre attività suggerite dai componenti il Consiglio di classe, dallo studente interessato dal provvedimento e/o i suoi genitori per i minorenni.

Sulla base dell'ePolicy d'Istituto, dello Statuto delle studentesse e degli studenti e del Regolamento d'Istituto, gli studenti protagonisti di atti di bullismo verranno coinvolti in un percorso di comprensione della gravità degli atti compiuti e, se possibile, a mettere in atto comportamenti attivi riparatori (es. attività di volontariato, pulizia degli spazi scolastici, piccole manutenzioni, svolgimento di attività di assistenza o di volontariato nell'ambito della comunità scolastica o delle associazioni del territorio convenzionate).

4.2 - Quali strumenti e a chi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

discriminare tra vittime, testimoni e/o autori.

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

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

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

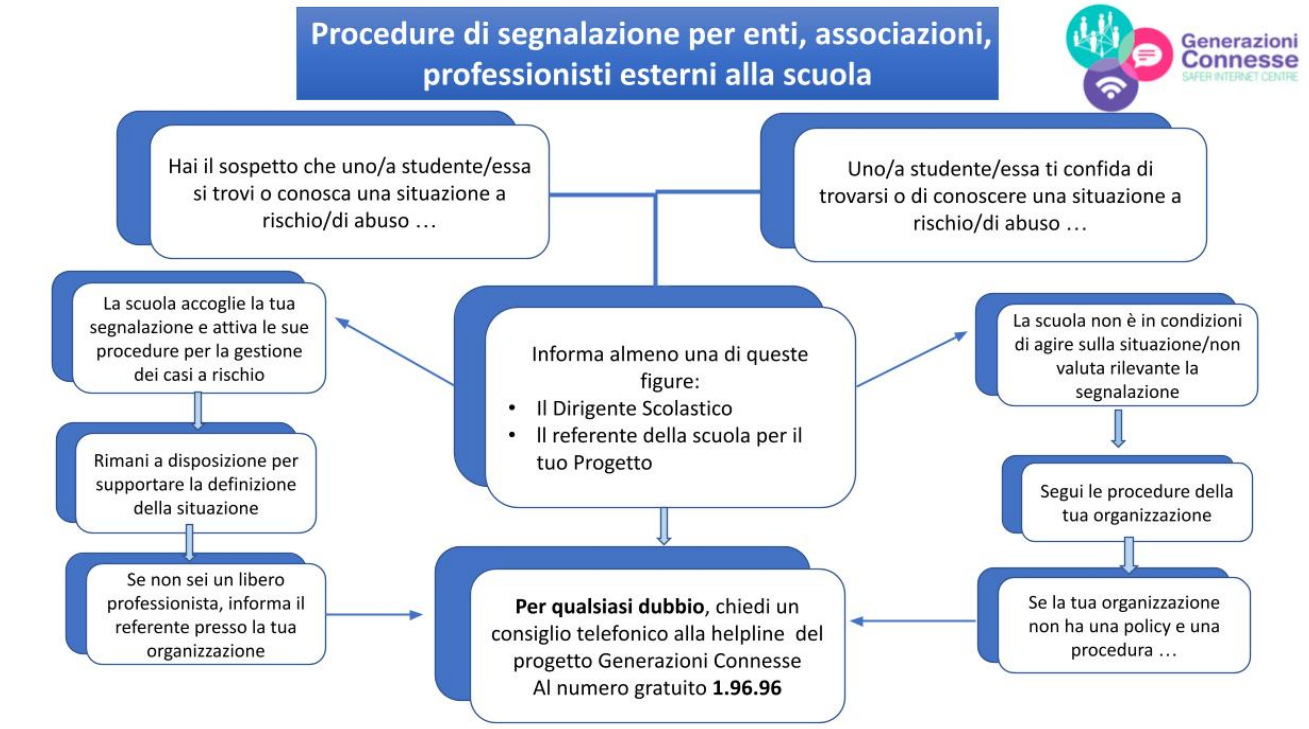
Strumenti a disposizione di studenti/esse

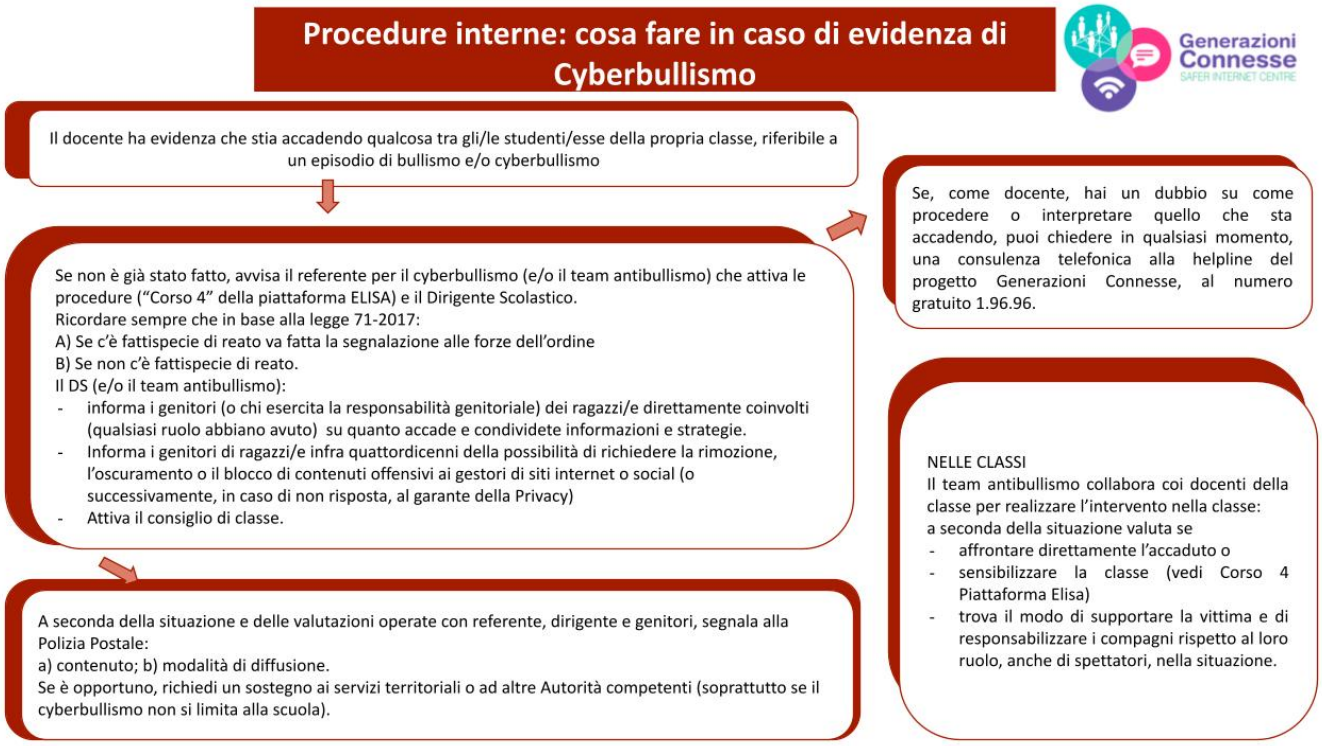
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

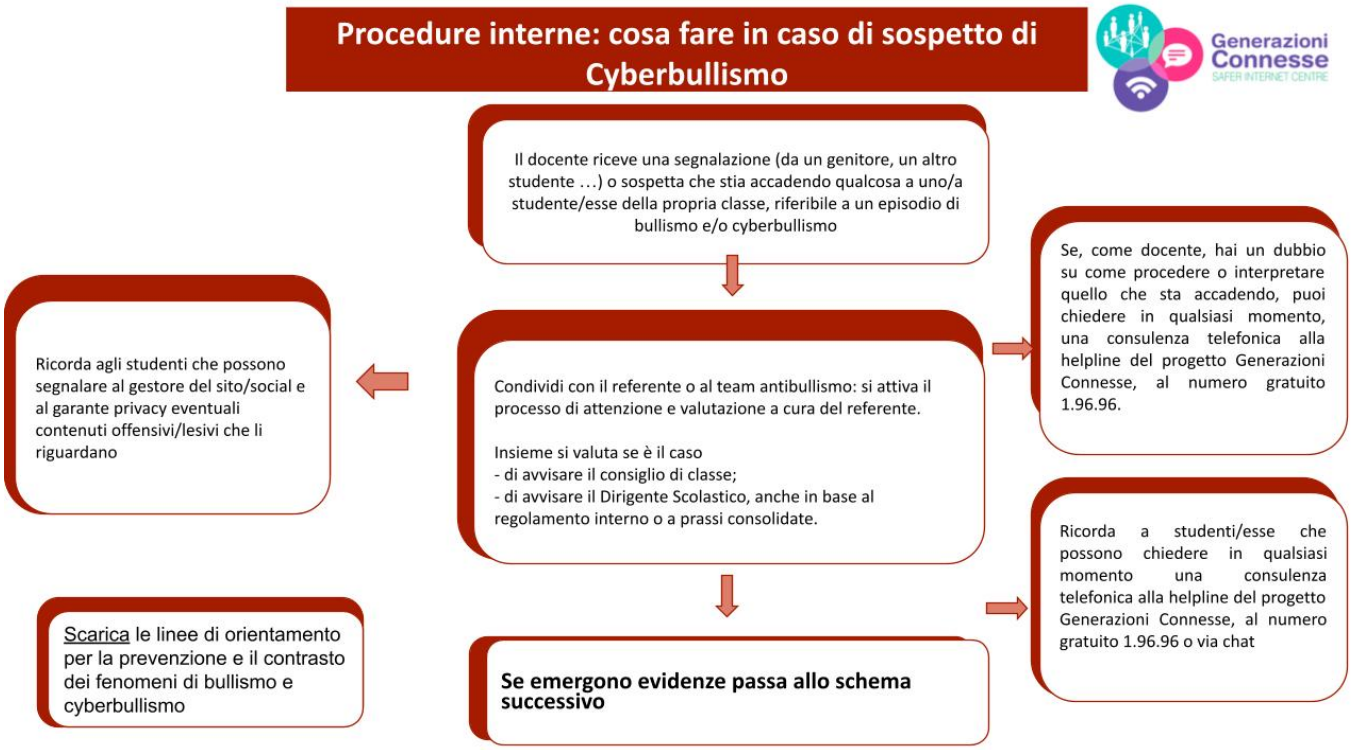
In particolare, sarebbe utile che la scuola attivi un sistema di segnalazione utile anche al monitoraggio dei fenomeni dal quale partire per integrare azioni didattiche preventive e giornate di sensibilizzazione, insieme agli Enti/Servizi presenti sul territorio di riferimento. Importante, altresì, immaginare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

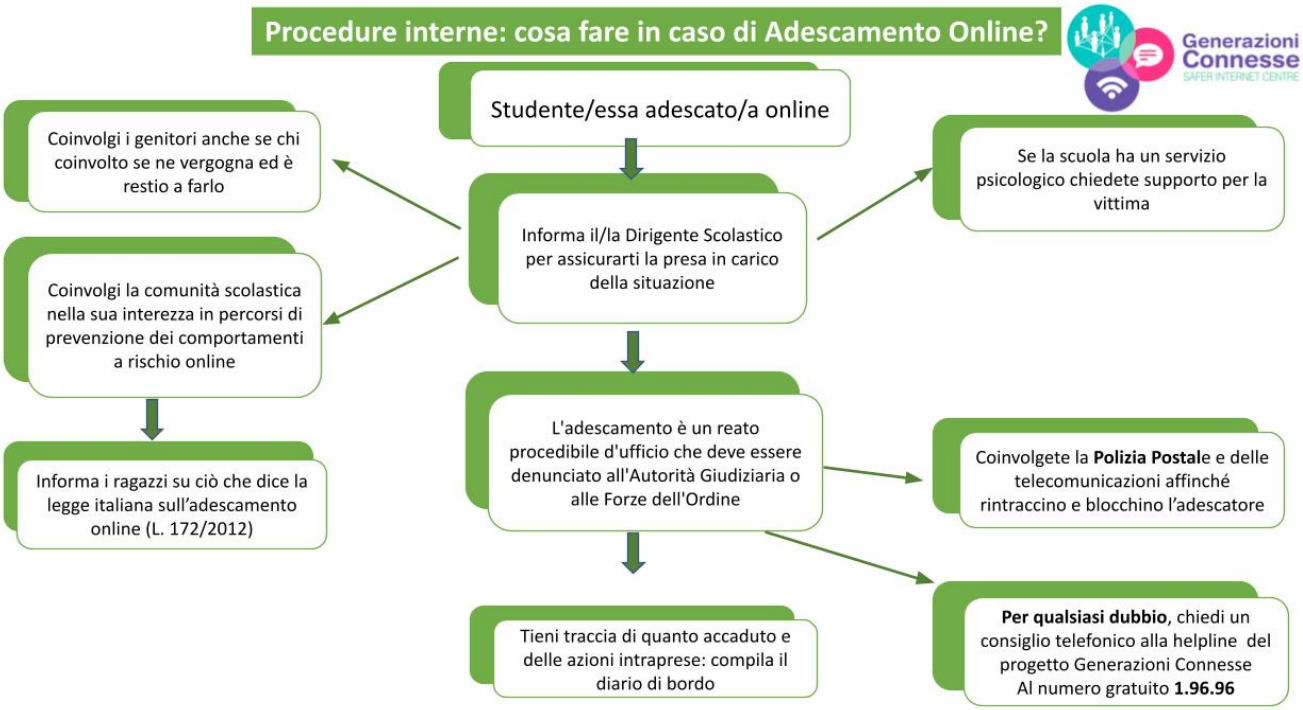
Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle Linee di Orientamento per la prevenzione e il contrasto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

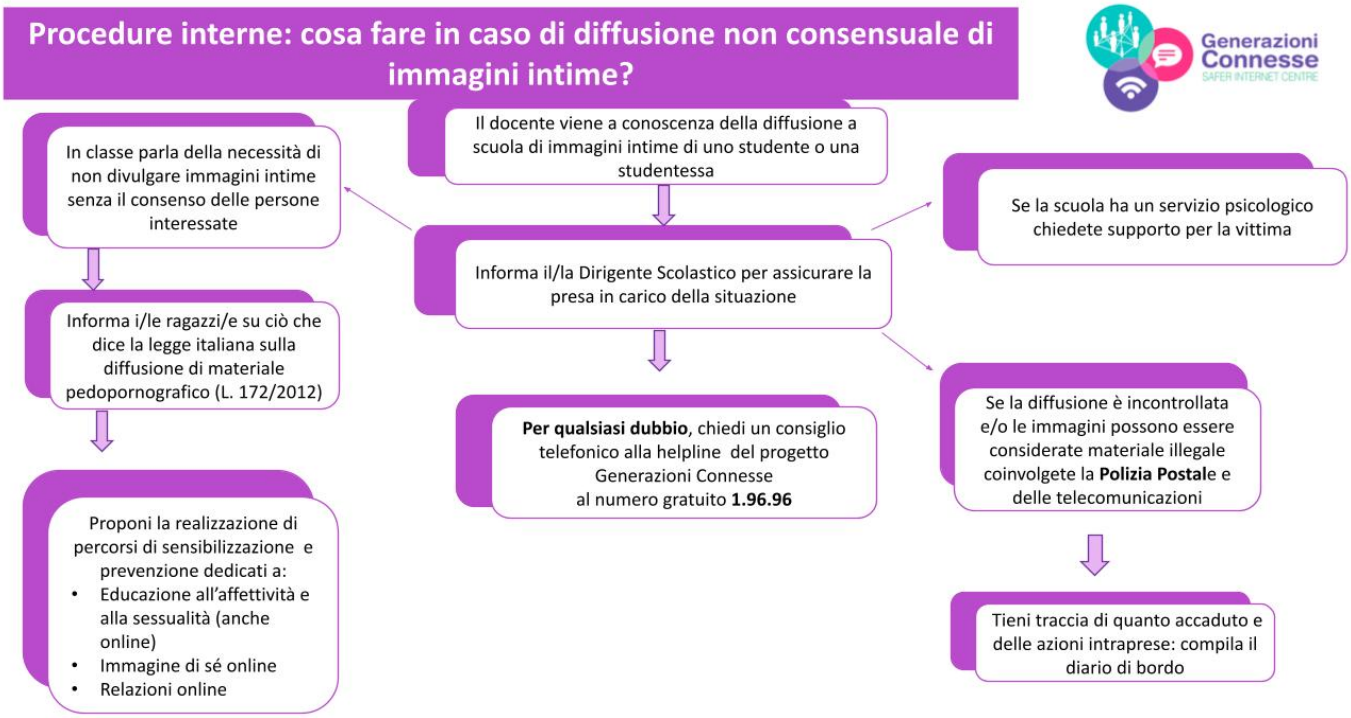
Procedure


Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola
Generazioni Connesse
Hai il sospetto che uno/a studente/essa si trovi o conosca una situazione a rischio/di abuso …
Uno/a studente/essa ti confida di trovarsi o di conoscere una situazione a rischio/di abuso …
La scuola accoglie la tua segnalazione e attiva le sue procedure per la gestione dei casi a rischio
Rimani a disposizione per supportare la definizione della situazione
Se non sei un libero professionista, informa il referente presso la tua organizzazione
Informa almeno una di queste figure:
• Il Dirigente Scolastico
• Il referente della scuola per il tuo Progetto
La scuola non è in condizioni di agire sulla situazione/non valuta rilevante la segnalazione
Segui le procedure della tua organizzazione
Se la tua organizzazione non ha una policy e una procedura …
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 evidenza di Cyberbullismo
Generazioni Connesse
Il docente ha evidenza che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo
Se non è già stato fatto, avvisa il referente per il cyberbullismo (e/o il team antibullismo) che attiva le procedure ("Corso 4" della piattaforma ELISA) e il Dirigente Scolastico.
Ricordare sempre che in base alla legge 71-2017:
A) Se c'è fattispecie di reato va fatta la segnalazione alle forze dell'ordine
B) Se non c'è fattispecie di reato.
Il DS (e/o il team antibullismo):
- informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto) su quanto accade e condividete informazioni e strategie.
- Informa i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy)
- Attiva il consiglio di classe.
A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla Polizia Postale:
a) contenuto; b) modalità di diffusione.
Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.
NELLE CLASSI
Il team antibullismo collabora coi docenti della classe per realizzare l'intervento nella classe:
a seconda della situazione valuta se
- affrontare direttamente l'accaduto o
- sensibilizzare la classe (vedi Corso 4 Piattaforma Elisa)
- trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.


Procedure interne: cosa fare in caso di sospetto di Cyberbullismo
Generazioni Connesse
Il docente riceve una segnalazione (da un genitore, un altro studente …) o sospetta che stia accadendo qualcosa a uno/a studente/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano
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.
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
Scarica le linee di orientamento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo
Se emergono evidenze passa allo schema successivo


Procedure interne: cosa fare in caso di Adescamento Online?
Generazioni Connesse
Studente/essa adescato/a online
Coinvolgi i genitori anche se chi coinvolto se ne vergogna ed è restio a farlo
Se la scuola ha un servizio psicologico chiedete supporto per la vittima
Informa il/la Dirigente Scolastico per assicurarti la presa in carico della situazione
Coinvolgi la comunità scolastica nella sua interezza in percorsi di prevenzione dei comportamenti a rischio online
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
Informa i ragazzi su ciò che dice la legge italiana sull'adescamento online (L. 172/2012)
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
Il docente viene a conoscenza della diffusione a scuola di immagini intime di uno studente o una studentessa
In classe parla della necessità di non divulgare immagini intime senza il consenso delle persone interessate
Informa il/la Dirigente Scolastico per assicurare la presa in carico della situazione
Se la scuola ha un servizio psicologico chiedete supporto per la vittima
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