



Documento di ePolicy SAVIANO I.C. 2 A. CICCONE -

VIALE LEONARDO SCIASCIA 33 - 80039 - SAVIANO

Napoli (NA) - Campania

Data di approvazione: 05/05/2025 - 08:07

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'e-policy del nostro Istituto mira a integrare le tecnologie digitali nel processo educativo per migliorare l'insegnamento e l'apprendimento per creare un ambiente di apprendimento inclusivo, accessibile ed equo, che prepari gli studenti alle sfide del mondo digitale.

La nostra e-policy ci consente di lavorare sui seguenti quattro obiettivi:

Piano di Azioni Triennale

Questo piano è essenziale per promuovere un uso sicuro, responsabile e positivo della rete all'interno della comunità scolastica. Un approccio triennale permette di pianificare e implementare iniziative a lungo termine, garantendo continuità e progressi misurabili. Coinvolgere l'intera comunità scolastica, inclusi studenti, docenti e genitori, è fondamentale per creare una cultura digitale consapevole e sicura.

Misure per la Prevenzione e Sensibilizzazione

Prevenire comportamenti online a rischio e sensibilizzare gli utenti è cruciale per proteggere gli studenti dai pericoli del web, come il cyberbullismo e la violazione della privacy. Programmi educativi e campagne di sensibilizzazione possono fornire le conoscenze necessarie per navigare in rete in modo sicuro e responsabile. Inoltre, coinvolgere i genitori e le famiglie aiuta a estendere queste pratiche anche al di fuori dell'ambiente scolastico.

Norme Comportamentali e Procedure di Utilizzo delle ICT

Stabilire norme comportamentali chiare e procedure di utilizzo delle ICT è fondamentale per garantire un uso corretto e sicuro delle tecnologie digitali. Queste norme devono essere ben comunicate e facilmente accessibili a tutti gli utenti. Le procedure di monitoraggio e controllo aiutano a mantenere un ambiente digitale sicuro e a prevenire abusi o usi impropri delle risorse tecnologiche.

Misure per la Rilevazione, Segnalazione e Gestione delle Situazioni Rischiose

Implementare misure efficaci per la rilevazione, segnalazione e gestione delle situazioni rischiose è essenziale per affrontare prontamente eventuali problemi legati all'uso delle tecnologie digitali. Sistemi di segnalazione anonimi e procedure di intervento rapide possono aiutare a proteggere gli studenti e a risolvere le situazioni problematiche in modo tempestivo. La collaborazione con autorità competenti e esperti esterni può fornire ulteriore supporto nella gestione di casi complessi.

Questi obiettivi, se ben implementati, possono contribuire a creare un ambiente scolastico sicuro e consapevole, dove le tecnologie digitali sono utilizzate in modo positivo e responsabile.

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

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

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

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

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

IL DIRIGENTE SCOLASTICO

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

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

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

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

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

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

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

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

Il Team ha il compito di:

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

I/LE DOCENTI

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

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

RESPONSABILE DELLA PROTEZIONE DEI DATI

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

co-responsabile delle azioni di informazione e formazione nell'Istituto sulla protezione dei dati personali

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

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

GLI STUDENTI E LE STUDENTESSE

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

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

I GENITORI/ADULTI DI RIFERIMENTO

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

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

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

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

1.3 Integrazione ePolicy nei documenti scolastici

(Il paragrafo spiega in che modo integrare il documento nel Regolamento dell'Istituto Scolastico da aggiornare con specifici riferimenti all'E-policy, così come nel RAV e all'interno del Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto).

La trasversalità dell'ePolicy rende necessaria una sua integrazione nell'ambito dei documenti che disciplinano il funzionamento dell'Istituto Scolastico.

Il Regolamento dell'Istituto scolastico, che rappresenta il principale punto di riferimento normativo, dovrà essere aggiornato in modo tale da dare contezza dell'adozione dell'ePolicy, e richiamare le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione in ambiente scolastico.

Anche il **Patto di Corresponsabilità educativa** tra scuola e famiglia dovrà essere integrato con gli opportuni riferimenti all'ePolicy, puntualizzando, da un lato l'impegno dell'Istituto ad organizzare eventi formativi/informativi a beneficio dei genitori, e dall'altro l'impegno di questi ultimi a partecipare in maniera proattiva a tali eventi.

Il **Piano Triennale dell'Offerta Formativa**, per la sua funzione di carta d'identità culturale e progettuale delle istituzioni scolastiche, nel quale si esplicita la progettazione curricolare, extracurricolare, educativa e organizzativa che le singole scuole adottano nell'ambito della loro autonomia, deve contenere anche le progettualità relative ad azioni media educative legate al percorso di ePolicy.

Così come il PTOF è il risultato di una consapevole concertazione fra le componenti delle istituzioni scolastiche (Dirigente Scolastico, docenti, alunni, genitori) e fra queste e il territorio, il patto di corresponsabilità rappresenta l'assunzione di responsabilità da parte di tutti coloro che svolgono un ruolo attivo nella Comunità educante.

Il Regolamento d'Istituto, che rappresenta il principale punto di riferimento normativo, sarà aggiornato per includere specifici riferimenti all'ePolicy, richiamando 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 sarà integrato con opportuni riferimenti all'ePolicy, sottolineando l'impegno dell'Istituto ad organizzare eventi formativi/informativi per i genitori e l'impegno di questi ultimi a partecipare attivamente. Il Piano Triennale dell'Offerta Formativa (PTOF), che esplicita la progettazione curricolare, extracurricolare, educativa e organizzativa delle scuole, dovrà includere le progettualità relative alle azioni educative legate all'ePolicy. Infine, il Rapporto di Autovalutazione (RAV) dovrà essere aggiornato per riflettere l'adozione e l'implementazione dell'ePolicy, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

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

realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

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

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

In tal senso, il documento è accompagnato da versioni, allegare 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.

Attraverso una serie di iniziative dedicate, l'IC 2 A. Ciccone si impegna ad assicurare la concreta promozione degli intenti dichiarati nel documento, valorizzando studenti e studentesse ed esplicitando ruoli e prerogative di tutte le figure operanti a vario titolo nella comunità scolastica. Al fine di condividere al meglio il documento di e-Policy a tutta la comunità scolastica, sono previste le seguenti azioni:

-) presentazione mirata del documento ai docenti,
-) agli studenti e alle studentesse
-) al personale A.T.A.,
-) ai rappresentanti dei genitori durante specifici incontri, appositamente organizzati ad inizio anno scolastico.

Si aggiunga infine che l'adozione dell'ePolicy nel nostro Istituto scolastico garantisce un presidio informato e attento sulle tecnologie e la rete, specialmente per i giovani: il nostro Istituto può diventare un punto di riferimento per le Istituzioni locali, le aziende e il Terzo Settore, favorendo la creazione di progetti di cittadinanza digitale per i giovani. La comunicazione dell'adozione dell'ePolicy avverrà tramite allegati sintetici inviati all'USR e al Municipio, evidenziando gli elementi del

documento e le prospettive per la comunità.

1.5 - I Piani di Azione dell'ePolicy

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

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

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

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

1° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

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

MODULO II

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

MODULO III

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

MODULO IV

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

2° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

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

MODULO II

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

L'IC 2 Antonio Ciccone intende realizzare le seguenti azioni con l'obiettivo di promuovere la conoscenza delle regole e dei protocolli di intervento che sono stati adottati con il documento di ePolicy nella comunità scolastica.

Eventi e azioni di presentazione e diffusione dell'ePolicy

1) Nel Collegio Docenti, nel corso della presentazione del documento e team antibullismo, si realizzerà un'attività interattiva per mostrare un breve caso studio utile per il confronto e l'informazione. La stessa attività può essere riproposta nelle classi per azioni di sensibilizzazione e prevenzione e per simulare una segnalazione. Al termine dell'attività può essere distribuita la versione friendly dell'ePolicy.

2) Si realizzerà un codice QR da diffondere negli ambienti scolastici che rimanda alla versione friendly del documento ePolicy per studenti e studentesse e per le famiglie

3) Si farà riferimento, promuovendone la consultazione, al database di "Buone Pratiche per la Prevenzione e il Contrasto al Bullismo e Cyberbullismo" presente sulla piattaforma Elisa.

4) Sarà ideato un contest/concorso nella scuola rivolto a studenti e studentesse per ideare e creare strumenti di diffusione dell'ePolicy alle famiglie.

5) Saranno affissi negli spazi comuni della scuola illustrazioni, disegni e altro sui temi dell'Educazione civica digitale e sugli strumenti di segnalazione.

Rilevazione del fabbisogno formativo dei docenti sui temi dell'educazione civica digitale.

1) Sarà somministrato il SELFIE FOR TEACHERS, strumento di autoriflessione sulle competenze digitali degli insegnanti di ogni ordine e grado, proposto gratuitamente dalla Commissione Europea sulle indicazioni del DigCompEdu, il framework delle competenze europee del docente/formatore.

2) Analogamente sarà somministrato, collegandolo al questionario precedente, il questionario SELFIE proposto dalla Commissione Europea gratuitamente, che aiuta a comprendere il livello di utilizzo positivo del digitale nell'Istituto.

Rilevazione di interessi, bisogni e comportamenti delle famiglie sull'uso positivo del digitale

1) Sarà somministrato un questionario di autovalutazione MYDIGISKILLS, gratuito e disponibile in diverse lingue, per permettere alle famiglie di valutare il proprio livello di competenze digitali rispetto al framework europeo DIGCOMP 2.2. Lo strumento permette di avere risultati chiari ed analitici sulle diverse competenze.

Team antibullismo

1) Saranno calendarizzate riunioni (trimestrali nel primo anno di adozione dell'e-policy, per gli anni successivi da stabilire in base ai bisogni) che vedano il coinvolgimento di D.S., Referente Cyberbullismo, DPO, Animatore Digitale, per verificare eventuali esigenze specifiche dell'istituto e condividere i risultati relativi alle azioni svolte.

2) La scuola metterà a disposizione della comunità educante un modulo di prima segnalazione (sul proprio sito web o in cartaceo presso la segreteria della scuola) per chiunque abbia necessità di segnalare situazioni a rischio di presunto o reale bullismo/cyberbullismo.

3) La scuola predispone un contenitore nelle sedi scolastiche come ulteriore strumento riservato per la segnalazione.

Azioni formative per studenti e studentesse sulla Piattaforma di Generazioni Connesse

1) Si farà riferimento ai progetti vincitori del primo e secondo contest The Kids are All Right realizzato da Generazioni Connesse tra il 2022 e il 2023.

2) Saranno utilizzati i video di approfondimento del canale YouTube con particolare riferimento alle serie SuperErrori rivolti alla scuola primaria e secondaria di primo grado

Il nostro istituto ha inoltre redatto nell'anno scolastico corrente i documenti la Politica d'Uso Accettabile (PUA) della scuola ed il regolamento BYOD dell'Istituto.

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

- [Kit Didattico](#)
- Area formazione (per docenti, famiglie, studenti/sse con ePolicy)

- Canale [Youtube](#) (webinar, video-stimolo, serie per target differenti)
- Canale [TikTok](#)
- Canale [Instagram](#)
- Canale [Facebook](#)

L'Istituto I.C. 2A.Ciccione attraverso appositi incontri formativi, presenterà alcune delle risorse di Generazioni Connesse proposte per il mondo della scuola, delle famiglie e dei giovani. Le risorse possono essere utilizzate per condividere l'ePolicy e le scelte definite dalla scuola e promuovere una cittadinanza digitale attiva all'interno dell'intera comunità scolastica. Le risorse a cui l'Istituto fa riferimento sono:

- [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.

Il nostro Istituto promuove la sensibilizzazione e la prevenzione su quelle tematiche che hanno a che fare con la cittadinanza digitale e che la legge 92 del 2019 all'articolo 5 definisce in modo puntuale:

- 1) Relazioni online
- 2) Cyberbullismo
- 3) Hate speech (linguaggio d'odio)
- 4) Sexting
- 5) adescamento
- 6) disinformazione
- 7) Intelligenza artificiali e algoritmi
- 8) Metaverso

Lavorare su queste tematiche significa prima di tutto occuparsi delle relazioni online, cioè del modo in cui interagiamo con gli altri in rete: infatti oggi molte interazioni che abbiamo con gli altri avvengono attraverso chat, social network e anche attraverso i videogiochi. A scuola diventa importante riflettere sulle caratteristiche della comunicazione online (ad esempio come cambia l'empatia? come si gestiscono le emozioni online?), anche per prevenire il cyberbullismo e l'hate speech (in italiano linguaggio d'odio).

Online si manifestano anche fenomeni come il sexting e l'adescamento, strettamente collegati all'educazione all'affettività e alla sessualità.

Altra questione centrale è la disinformazione che riguarda le cosiddette fake news, un'area che è strettamente collegata anche alle nuove questioni sull'intelligenza artificiale e gli algoritmi: questi due fattori entrano in gioco quando scegliamo i

contenuti che ognuno di noi visualizza in base alla nostra cronologia, ai nostri like, alle nostre condivisioni. Lavorare su questo tema diventa centrale anche per il futuro della democrazia, proprio per la capacità che possono avere questi sistemi di indirizzarci verso determinati contenuti piuttosto che altri.

Anche se ancora oggi non è così sviluppato come si pensava, il Metaverso è una delle frontiere nuove a cui bisogna prestare attenzione.

Infine, parlando di cittadinanza, per gli studenti è fondamentale conoscere i loro diritti e imparare a declinarli nel mondo online: la Convenzioni sui Diritti dell'Infanzia dell'Adolescenza sarà la guida per orientare i percorsi di prevenzione.

Nel nostro Istituto la conoscenza, la sensibilizzazione su queste tematiche hanno un ruolo centrale e quando ci si occupa di queste tematiche in continua evoluzione, la formazione dei docenti è fondamentale: in quest'ottica il DigComp, che contiene le indicazioni europee sulle competenze digitali, è sicuramente una guida eccezionale che ci fornisce gli indicatori utili a costruire un curriculum verticale sulla competenza digitale.

Altrettanto importante è il ruolo della famiglia: aderire alle proposte della scuola per sensibilizzare i propri figli/e, promuovere messaggi educativi in linea con la formazione che ricevono a scuola rende la prevenzione molto più efficace.

Infine, coinvolgere la comunità educante del territorio (istituzioni locali, organizzazioni, società sportive) aumenta ancora l'efficacia dei percorsi.

2.2 - Il Curriculum Digitale

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

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

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

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

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

“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.” È l'ottima descrizione che fa la Commissione Europea all'interno della Raccomandazione del Consiglio del 22 maggio 2018 relativa alle

competenze chiave per l'apprendimento permanente. La competenza digitale è dunque essenziale, nell'arco della vita, allo stesso modo delle competenze di base (linguistiche, scientifiche, civiche...). Tutte interagiscono alla pari, al fine di formare un cittadino competente e responsabile. Il curriculum digitale del nostro Istituto è un'applicazione del modello europeo DigComp al segmento della scuola dell'obbligo che per il nostro Istituto va dalla classe prima della scuola primaria alla classe terza della scuola secondaria di primo grado. Il percorso indicato nel nostro Curriculum, vuole aiutare ad individuare punti di riferimento, approfondire le aree della competenza digitale e agevolare un coerente percorso verticale.

Il Curriculum è strutturato:

- per bienni: si tratta di una scansione temporale indicativa e non rigida. Alcune competenze ed attività si ripetono nei bienni, perché nello sviluppo della competenza cambia il livello di autonomia degli studenti. Significativo è il terzo biennio, che aggancia fortemente l'ultimo anno della scuola primaria con il primo della scuola secondaria di primo grado, suggerendo così anche spunti per eventuali azioni di continuità tra i due ordini di scuola;
- secondo le 5 aree del DigComp: anche in questo caso, non può esservi una rigida separazione. Alcune competenze ed alcune attività si ripetono tra aree all'interno dello stesso o di diverso biennio, perché nella competenza digitale non avrebbe senso una netta separazione tra le aree;
- per sviluppo di competenza (prima colonna della progettazione): questa proposta vuole aiutare le scuole a tenere presente come una stessa area di competenza può svilupparsi in modo verticale ed orizzontale;
- per attività (seconda colonna della progettazione): si tratta di proposte non esaustive sul "come" la competenza può essere avviata, incrementata e agita;
- per esempi di risorse (terza colonna della progettazione): anche in questo caso, l'intento è quello di suggerire un ventaglio di supporti operativi (software, app, materiali, esempi...) che aiutino i docenti a realizzare attività in classe.

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.

Il Kit Didattico di Generazioni Connesse rappresenta uno strumento fondamentale per promuovere la cittadinanza digitale tra gli studenti poiché offre percorsi educativi strutturati per guidare gli insegnanti nella realizzazione di laboratori di educazione civica digitale. Basato sul metodo EAS (Episodi di Apprendimento Situato) e integrato con il quadro di riferimento DigComp 2.1, il kit copre cinque aree principali:

1. **Comprensione del cambiamento digitale:** Introduzione alle trasformazioni derivanti dalla convergenza tra tecnologie digitali e connettività.
2. **Educazione ai media:** Esplorazione delle implicazioni individuali e sociali delle tecnologie digitali.
3. **Educazione all'informazione:** Sviluppo delle competenze per la ricerca, raccolta, utilizzo e conservazione delle informazioni.
4. **Quantificazione e computazione:** Analisi delle dinamiche legate alla diffusione delle tecnologie digitali.
5. **Cittadinanza e creatività digitale:** Connessione tra cittadinanza attiva e creatività nell'uso delle tecnologie.

Ogni area include approfondimenti teorici e lesson plan dettagliati, adattabili alla programmazione curricolare della classe. L'adozione del Kit Didattico di Generazioni Connesse all'interno dell'ePolicy dell'Istituto Scolastico garantirà un approccio educativo coerente e integrato, favorendo lo sviluppo di competenze digitali essenziali per gli studenti.

Oltre al Kit Didattico di Generazioni Connesse, l'Istituto Scolastico adotterà altre risorse educative in linea con il quadro DigComp, come il **DigCompEdu** e il **DigComp 2.2**.

Il DigCompEdu è un quadro di riferimento europeo per le competenze digitali dei docenti, che fornisce un modello coerente per sviluppare la competenza pedagogica digitale degli insegnanti. Questo quadro copre sei aree di competenza, tra cui l'uso delle tecnologie digitali per la comunicazione organizzativa, la creazione di risorse educative digitali, e la valorizzazione delle potenzialità degli studenti.

Il DigComp 2.2, invece, è un quadro di riferimento per le competenze digitali dei cittadini, che fornisce un linguaggio comune per identificare e descrivere le aree chiave delle competenze digitali. Questo strumento è utile per migliorare le competenze digitali degli studenti, aiutandoli a impegnarsi in modo critico e sicuro con le tecnologie digitali e nuove emergenti.

L'adozione di queste risorse all'interno dell'ePolicy dell'Istituto Scolastico garantirà un approccio educativo coerente e integrato, favorendo lo sviluppo di competenze digitali essenziali per gli studenti e il personale 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.

La protezione dei dati personali dei nostri studenti, delle loro famiglie e del personale scolastico è una nostra priorità. La nostra [privacy policy](#) (presente sul nostro sito) è stata sviluppata per garantire che tutte le informazioni personali siano trattate con la massima cura e nel rispetto delle normative vigenti.

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.

La nostra scuola si impegna a garantire un uso sicuro e responsabile delle tecnologie dell'informazione e della comunicazione (TIC). Il nostro documento P.U.A. (pubblicato sul sito della scuola) stabilisce le linee guida per l'utilizzo di Internet e delle risorse digitali all'interno dell'istituto, assicurando che studenti, docenti e personale scolastico possano beneficiare delle opportunità offerte dalla rete in modo sicuro e consapevole.

Obiettivi della P.U.A.:

1. **Promuovere l'Eccellenza Didattica:** Utilizzare Internet per arricchire le attività didattiche e favorire l'innovazione e la comunicazione.
2. **Garantire la Sicurezza:** Implementare misure per proteggere gli utenti da contenuti inappropriati e rischi online.
3. **Responsabilità e Consapevolezza:** Educare gli utenti a un uso responsabile e consapevole delle risorse digitali.

Principali Linee Guida:

- **Accesso Controllato:** Limitare l'accesso a risorse online inadeguate e illegali.
- **Formazione:** Fornire formazione continua su un uso sicuro e responsabile di Internet.
- **Monitoraggio:** Monitorare l'uso delle TIC per prevenire abusi e garantire la conformità alle norme.

Diritti e Doveri degli Utenti: Gli utenti hanno il diritto di accedere alle risorse digitali per scopi educativi e devono rispettare le regole stabilite nel documento P.U.A. per garantire un ambiente sicuro e produttivo per tutti.

Contatti: Per ulteriori informazioni o chiarimenti sulla P.U.A., è possibile contattare il responsabile TIC della scuola all'indirizzo email: mariapia.alfieri.d09@ic2ciccone.edu.it

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.

La nostra scuola promuove l'uso delle tecnologie personali come strumenti di apprendimento attraverso la politica BYOD (Bring Your Own Device). Questa iniziativa permette agli studenti di portare e utilizzare i propri dispositivi elettronici, come tablet e laptop per supportare le attività didattiche.

Obiettivi della Politica BYOD:

1. **Integrazione Tecnologica:** Favorire l'integrazione delle tecnologie digitali nel processo educativo, migliorando l'accesso alle risorse e agli strumenti di apprendimento.
2. **Personalizzazione dell'Apprendimento:** Consentire agli studenti di utilizzare i dispositivi con cui si sentono più a loro agio, personalizzando così l'esperienza di apprendimento.
3. **Responsabilità Digitale:** Educare gli studenti a un uso responsabile e sicuro delle tecnologie, promuovendo la cittadinanza digitale.

Linee Guida Principali:

- **Accesso alla Rete:** Gli studenti possono connettersi alla rete Wi-Fi della scuola con i propri dispositivi, seguendo le regole di sicurezza stabilite.
- **Uso Responsabile:** I dispositivi devono essere utilizzati esclusivamente per scopi educativi durante l'orario scolastico.
- **Sicurezza e Privacy:** Gli studenti devono rispettare le norme di sicurezza e privacy, evitando di condividere informazioni personali o sensibili.

Supporto e Formazione: La scuola fornisce supporto tecnico e formazione continua per garantire che studenti e docenti possano sfruttare al meglio le opportunità offerte dalla politica BYOD.

Contatti: Per ulteriori informazioni o chiarimenti sulla politica BYOD, è possibile contattare il responsabile TIC della scuola all'indirizzo email: mariapia.alfieri.d09@ic2ciccone.edu.it

Cap 4 - Segnalazione e gestione dei casi

4.1 - Cosa Segnalare

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

Il nostro Istituto con l'adozione della presente e-policy adopera una procedura di segnalazione standardizzata e condivisa con tutta la comunità scolastica, inclusi docenti, famiglie, studenti e enti del territorio. Il gruppo incaricato della gestione delle segnalazioni comprende il Dirigente Scolastico, il responsabile anti bullismo e cyberbullismo, e i servizi e gli enti del territorio, coinvolti nei casi di particolare gravità.

La comunicazione della procedura avviene attraverso vari mezzi, come collegio docenti, il sito della scuola e locandine. La procedura identifica i comportamenti online a rischio, come cyberbullismo, adescamento online e sexting, e stabilisce le modalità di intervento.

Quando parliamo di cyberbullismo è necessario capire se si tratta effettivamente di cyberbullismo o di un'altra problematica. Il cyberbullismo è una forma di prepotenza virtuale attraverso l'uso di internet e tecnologie digitali. Simile al bullismo tradizionale, comporta la prevaricazione e l'oppressione ripetuta da parte di individui o gruppi più potenti verso quelli percepiti come più deboli.

È fondamentale analizzare il contesto e le modalità attraverso le quali si manifesta questo tipo di comportamento. Si manifesta in pubblico? Si manifesta tra coetanei? Si manifesta in modo ripetuto? Quali sono quindi le caratteristiche? Ci deve essere intenzionalità, ripetitività, disparità di forze e potere tra i soggetti coinvolti e l'isolamento della vittima. È necessario inoltre capire quello che è il grado di disagio vissuto dallo studente o dalla studentessa.

In caso di particolare gravità, eventualmente coinvolgere servizi esterni che possono offrire un supporto psicologico e di mediazione adatto alla situazione vissuta. Il Parlamento italiano ha approvato una legge del 71 del 2017, il 18 maggio 2017. La legge mira a proteggere i minori contro il cyberbullismo con misure educative e rieducative.

Se si sospetta di un caso di **adescamento online**:

È importante non eliminare le eventuali prove di questo comportamento nei suoi smartphone, tablet o computer. È fondamentale non sostituirsi al minore quindi non rispondere al posto della persona danneggiata e come dicevamo mantenere quelle che sono le prove di queste comunicazioni. È inoltre fondamentale valutare il grado di disagio vissuto dal minore ed eventualmente coinvolgere le agenzie competenti o un esperto che possa offrire un supporto psicologico o psichiatrico adatto al caso e alla situazione vissuta.

Quando parliamo di **sexting** è importante specificare che non è per sé condotta progeduzievole meglio piuttosto parlare di condivisione non consensuale di materiale sessualmente esplicito o simile. Il sexting, cioè lo scambio di contenuti sessualmente espliciti è considerato la stessa stregua di un atto sessuale e richiede il consenso di tutte le parti coinvolte. Questo deve avvenire all'interno di una relazione consensuale con particolare attenzione all'età e alla capacità di autodeterminazione dei minori come dichiarato dalla Corte di Cassazione.

Tuttavia la divulgazione di tali materiali senza consenso specialmente se riguardano minori può costituire un reato indipendentemente dall'età del minore coinvolto. Ciò che si rileva come pericolo quindi è da intendersi come la condivisione a terzi del materiale scambiato senza consenso anche se autoprodotta e anche se richiesto anche se su condivisione richiesto dal minore stesso. Questo vale per tutti i minori fino a 17 anni.

È fondamentale andare ad analizzare i sistemi di segnalazione per provvedere alla rimozione più rapida possibile di questo materiale con l'obiettivo di tutelare il minore e quindi bloccare la condivisione di queste immagini e di questi video. La segnalazione alla piattaforma può essere fatta da chiunque mentre quella tramite il garante della privacy è una procedura per la protezione dei dati personali che possono fare i minori con più di 14 anni autonomamente o l'adulto che lo tutela con lo scopo di porre in stanza di oscurare, rimuovere, bloccare dati personali diffusi su internet. Nel caso in cui non si riesca ad identificare il titolare del trattamento dei dati o quando questo, dopo che l'interessato ha mandato una richiesta, non abbia provveduto entro 48 ore ad oscurare le informazioni.

Per farlo bisogna compilare il modello che si trova sul sito www.garanteprivacy.it. Ci sono inoltre servizi esterni o enti del territorio che possono offrire supporto in caso di comportamenti online a rischio. Uno tra questi è l'[Helpline](#) del Telefono Azzurro, (19696) una linea telefonica gratuita attiva 24 ore su 24 365 giorni all'anno. È una linea telefonica alla quale rispondono operatori esperti che offrono consulenza psicopedagogica non solo ai minori ma anche adulti, a docenti o persone che ne richiedono aiuto.

Questa linea è raggiungibile anche attraverso una chat accessibile sul sito del telefono azzurro. Esistono oltre all'Helpline anche altri due strumenti di segnalazione di materiale pedopornografico online. Questi servizi di segnalazione esterni sono [click e segnala](#) di telefono azzurro [stop it](#) di Save the Children entrambi sono raggiungibili attraverso i link e servono appunto per segnalare contenuti pedopornografici online attraverso la compilazione di un form presente sui diversi siti.

Entrambi i servizi provvederanno alla segnalazione di questo materiale e alla condivisione con il Centro Nazionale per il Contrasto della Pedopornografia Internet il quale provvederà all'analisi di questo materiale ed eventualmente in caso necessario alla segnalazione alle realtà del territorio.

4.2 - Quali strumenti e a chi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Prevedere possibili incontri di mediazione tra i minori coinvolti vanno ponderati con la consapevolezza del loro stato

emotivo, anche e in base agli elementi raccolti in merito del fatto/episodio avvenuto (elementi che si dovrebbero valutare di caso in caso). Importante è prevedere il coinvolgimento dei genitori sia della vittima che del bullo (ove possibile).

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

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

Strumenti a disposizione di studenti/esse

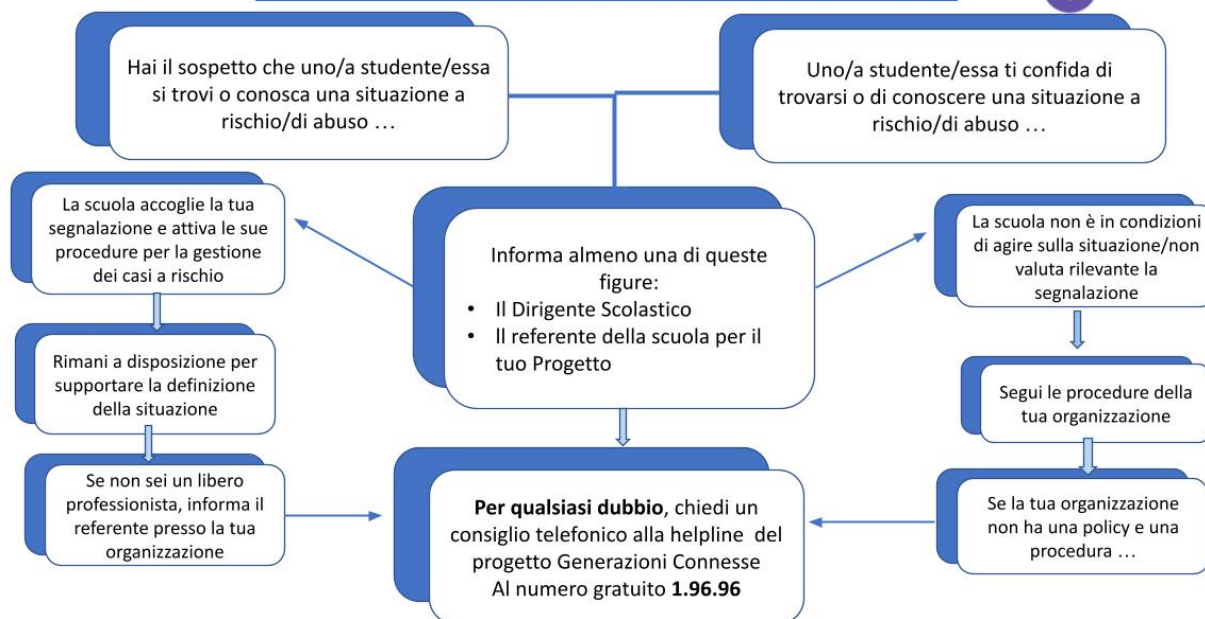
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

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

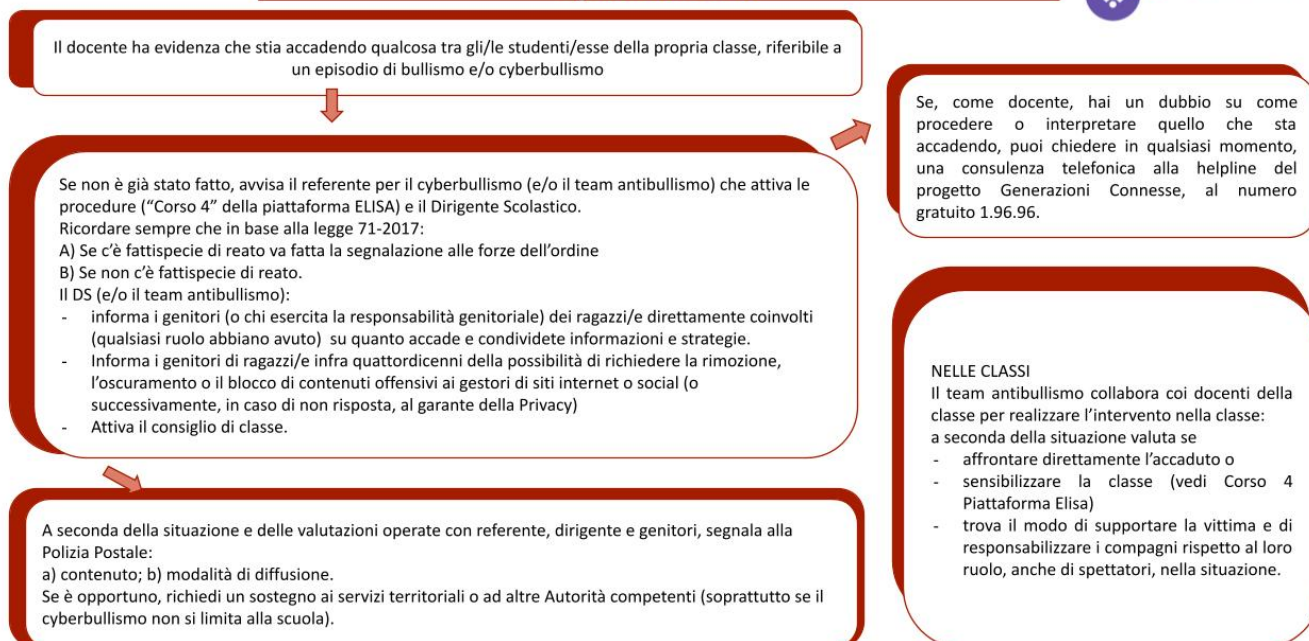
Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle [Linee di Orientamento per la prevenzione e il contrasto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

Procedure

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



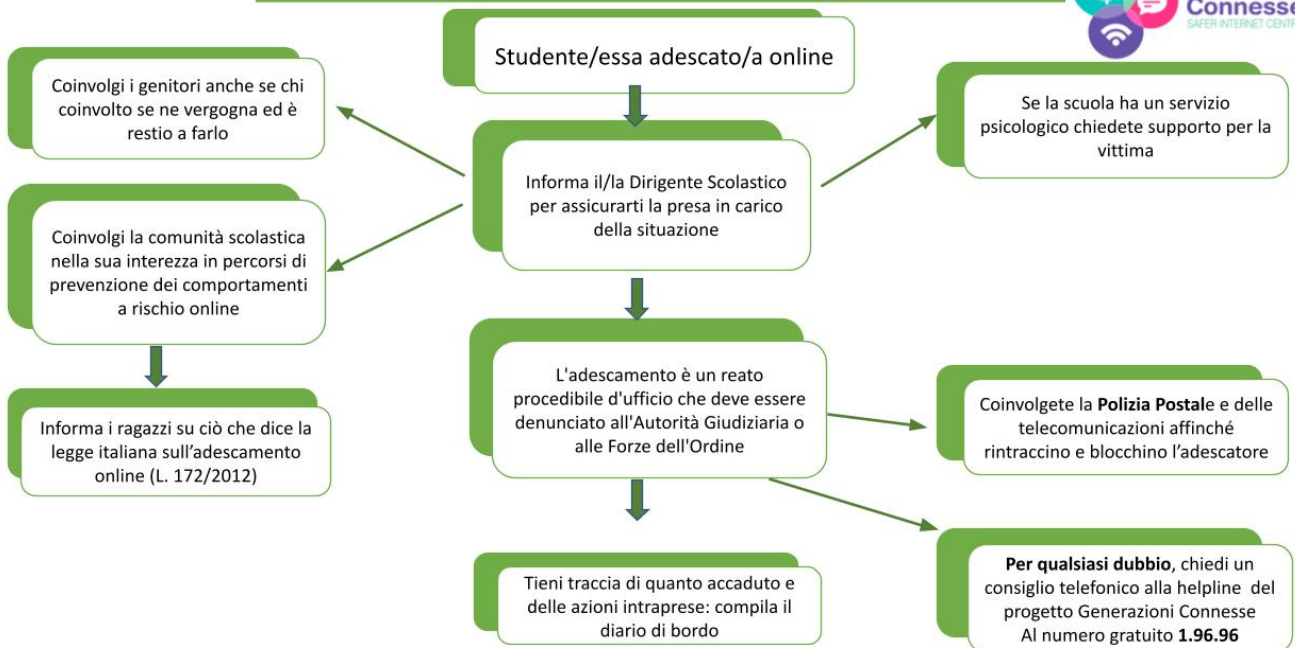
Procedure interne: cosa fare in caso di evidenza di Cyberbullismo



Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



Procedure interne: cosa fare in caso di Adescamento Online?



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

