



Documento di ePolicy

I.C. CORIGLIANO "ERODOTO"

VIA SAN GIOVANNI EVANGELISTA SNC - 87064 - CORIGLIANO-ROSSANO

Cosenza (CS) - Calabria

Data di approvazione: 30/08/2024 - 11:11

ePolicy

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.

Il nostro Istituto si vuole dotare, attraverso la stesura dell'E-policy, di uno strumento operativo comune per tutta la comunità educante, finalizzato ad assicurare un approccio corretto alle nuove tecnologie digitali, critico, consapevole ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso della rete internet. Dunque l'E-policy sarà una guida per garantire la sicurezza e il benessere nell'utilizzo della rete, definendo regole di utilizzo e di comportamento nonché azioni di formazione, finalizzate ad un uso corretto e critico delle tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

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'impegno 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 segua 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.

L'intera comunità educante dovrà dunque operare in sinergia per favorire un corretto utilizzo dell'E-policy .

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.

Tutti i documenti strategici dell'istituto verranno aggiornati secondo i riferimenti all'E-policy in coerenza con con le linee guida Miur e le indicazioni normative generali sui temi in oggetto.

Il documento di E-policy si armonizza con gli altri regolamenti vigenti nell'Istituto integrandosi pienamente con gli obiettivi enunciati nel PTOF, nel Rav, nel Patto di corresponsabilità controfirmato da scuola e genitori all'atto dell'iscrizione e con il regolamento d'Istituto.

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, 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 di E-policy verrà condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse. È importante che ogni attore della scuola si faccia promotore del documento.

L'E-policy verrà condiviso e comunicato al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso una serie di canali, dopo l'approvazione nel collegio dei docenti e del consiglio d'Istituto. Le azioni previste sono:

- Il documento verrà pubblicato sul sito istituzionale della scuola e sulle pagine social; Gli studenti e le studentesse dell'Istituto verranno informati attraverso lezioni guidate e adeguate al grado scolastico.

- Il patto di corresponsabilità verrà aggiornato e sottoscritto dalle famiglie all'inizio dell'anno scolastico;
- Il documento verrà inviato all'USR territoriale e al Municipio (servizio istruzione e servizi scolastici) ;
- Gli studenti e le studentesse dell'istituto verranno informati ed educati attraverso lezioni guidate e adeguate al grado scolastico; Il personale scolastico riceverà una adeguata informazione/formazione sull'uso sicuro e responsabile della Rete , attraverso materiali
- disponibili anche sul sito della scuola in una sezione dedicata;
Nel corso dell'anno i docenti dedicheranno alcune lezioni ,anche all'interno di progetti d'Istituto promossi dalle figure di sistema
- dedicate, alle buone pratiche per un uso sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al Cyberbullismo.
- Le famiglie saranno informate in merito alla linea di condotta adottata dalla scuola per un uso sicuro e responsabile delle tecnologie digitali e di internet, attraverso la condivisione del presente documento e di materiali specifici sul sito web della scuola.
- Con cadenza periodica la scuola organizzerà, anche in sinergia con enti e associazioni del territorio, incontri finalizzati a sensibilizzare e/o informare le famiglie sul tema della sicurezza informatica e sui comportamenti da monitorare o da evitare. La condivisione con le famiglie avverrà anche in seno ai consigli di interclasse e di classe.

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 e 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

Nel prossimo triennio le azioni che l'istituto intende sviluppare sono le seguenti:

ANNO SCOLASTICO 2024/2025

- Approvazione nel collegio docenti del documento E-policy;
- Pubblicazione e diffusione del documento E-policy con la comunità educante;
- Organizzazione di un evento di presentazione del documento di E-policy per Studenti, docenti e genitori;

Nelle successive annualità 2025/2026 e 2026/2027 si prevede di :

- organizzare degli eventi per la presentazione del progetto generazioni connesse a studenti, docenti e genitori. promuovere il
- progetto generazioni connesse tramite pubblicazione del link alla piattaforma sul sito istituzionale: monitoraggio e revisione del
- documento di E-policy

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 utilizzerà tutte le risorse digitali di generazioni connesse nella formazione di studenti, docenti e genitori , anche attraverso una sezione dedicata nel sito istituzionale, con i link di collegamento che verranno promossi anche attraverso i canali di Facebook e Istragram .

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.

Per la prevenzione dei rischi legati ad un uso scorretto delle Tic e per la corretta valorizzazione delle opportunità legate alle risorse digitali , è necessaria la collaborazione dell'intera comunità educante, ognuno con i propri ruoli, compiti e responsabilità. La scuola e la famiglia devono attivare un'allenza educativa forte e promuovere percorsi educativi continuativi e condivisi, per accompagnare insieme bambini/e e ragazzi/e verso un uso responsabile, consapevole e critico ma anche arricchente delle tecnologie digitali. L'istituto, garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'e-policy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, del Patto di corresponsabilità e attraverso una sezione dedicata sul sito istituzionale.

L'istituto promuovrà la sensibilizzazione delle famiglie attraverso le seguenti azioni:

- Pubblicare sul sito e diffondere il documento delle E-policy, al fine di garantire che i principi di comportamento sicuro online siano chiari;
- Organizzare percorsi di sensibilizzazione dei genitori su un uso responsabile e costruttivo delle Rete in famiglia e a scuola; Prevedere azioni e strategie per il coinvolgimento delle famiglie in questi percorsi di sensibilizzazione in cui anche gli studenti siano protagonisti.

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 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.

Sia i bambini che i ragazzi, usano spesso la rete in modo "intuitivo" ed "agile" rispetto agli adulti, ma non per questo hanno acquisito o sono dotati di "competenze digitali". Infatti la "competenza digitale" presuppone l'interesse per le tecnologie digitali ed un uso critico e consapevole nell'uso delle stesse per studiare, ricercare o lavorare. Essa comprende l'alfabetizzazione mediatica, la creazione di contenuti digitali, la sicurezza, la risoluzione dei problemi e il pensiero critico, così come espressamente dichiarato, nelle Raccomandazioni del Consiglio Europeo in merito alla competenza chiave "imparare per imparare".

Per questo l'Istituto si impegna ad attivare azioni volte a sviluppare tali competenze al fine di educare i bambini/e e i ragazzi/e ad un uso critico e responsabile delle tecnologie digitali.

Alla base del nostro curriculum digitale c'è lo studio accurato di alcuni documenti che consideriamo fondamentali, ossia:

- Piano Nazionale Scuola Digitale (PNSD), che è il documento di indirizzo del MIM, per il lancio di una strategia complessiva di innovazione della scuola italiana e per un nuovo posizionamento nell'era digitale;
- Sillabo sull'educazione civica digitale, che ha lo scopo di inquadrare il corpus dei temi e contenuti che sono alla base dello sviluppo di una piena cittadinanza digitale degli studenti attraverso il percorso educativo.
- Digicomp 2.2 che rappresenta un aggiornamento del quadro europeo delle competenze digitali dei cittadini. Introduce nuovi temi e pone un focus sull'intelligenza artificiale (IA) enfatizzando l'importanza di un approccio informato e responsabile verso le tecnologie emergenti.
- Raccomandazioni del Consiglio dell'Unione Europea relativa alla competenza chiave per l'apprendimento permanente (C189/9 pag.9). Rappresenta un documento in cui vengono espresse le conoscenze, le abilità e gli atteggiamenti legati a questa competenza.

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.

E' essenziale affrontare le tematiche legate all'uso corretto delle tecnologie durante le lezioni in classi e/o quando se ne ravvisi la necessità educativa. Importante sarà l'utilizzo del Kit didattico offerto dalla piattaforma Generazioni Connesse, che verrà messo a disposizione dei docenti attraverso un link di collegamento dalla sezione dedicata sul sito istituzionale.

Il kit didattico è uno strumento educativo completo, progettato per supportare le istituzioni scolastiche, nello sviluppo di una cittadinanza digitale consapevole e attiva tra gli studenti. Il kit è strutturato in 5 aree tematiche principali:

1. **Internet e cambiamento:** Questa sezione si concentra sulla comprensione generale dei cambiamenti portati dalla convergenza tra tecnologie e connettività;
2. **Educazione ai media:** Si occupa delle implicazioni che le tecnologie digitali hanno sulla nostra dimensione individuale e sociale;
3. **Educazione all'informazione:** Affronta le competenze necessarie per la ricerca, raccolta, utilizzo e conservazione delle informazioni;
4. **Quantificazione e computazione:** Esplora le dinamiche legate alla diffusione delle tecnologie digitali, come i dati e l'intelligenza artificiale ;
5. **Cultura e creatività digitale:** Sviluppa la connessione tra cittadinanza e la creatività digitale.

Il kit, include materiali didattici interattivi, proposte ludico-educative, approfondimenti e si basa sul metodo EAS (episodi di apprendimento situato).

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.

In una società complessa e globalizzata come la nostra, la scuola ha il dovere di educare le future generazioni al rispetto dei valori fondanti di una società. Soprattutto nell'era di internet e in presenza di nuovi modelli di comunicazione, questo compito diventa ancora più importante. E' necessario riaffermare quotidianamente, anche in ambito scolastico, i principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino, così come viene affermato dal garante della privacy.

A scuola, ogni giorno, vengono trattati dati personali e dati sensibili di studenti e famiglie. Il corretto trattamento dei dati personali a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni.

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione Europea (art.8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General data protection Regulation) e al D.Lgs 10 agosto 2018, n. 101 .

Nel seguente paragrafo dell'E-Policy , verrà affrontata questa problematica legata soprattutto all'uso delle tecnologie digitali e verranno indicate le misure che l'istituto intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori.

Nel nostro Istituto, vengono trattati ogni giorno, numerose informazioni sugli alunni/e e sulle loro famiglie, sui loro problemi sanitari o sui disagi sociali e alimentari.

In particolare, il compito della scuola non è solo quello di tutelare la privacy di ognuno, ma soprattutto di educare al rispetto del diritto alla riservatezza di se stessi e degli altri.

Nel dettaglio le misure che la nostra scuola adotta già da tempo e che intende migliorare sono:

- Implementazione delle procedure di identificazione e autenticazione informatica degli utenti.
- Definizione dei profili di autorizzazione per garantire un accesso selettivo ai dati.
- Limitare la raccolta dei dati allo stretto necessario.
- Assicurare la corretta gestione dei registri elettronici, proteggendo l'accesso ai dati sensibili.
- Regolamentare la pubblicazione di foto e video, soprattutto in occasione di eventi scolastici.
- Fornire formazione regolare a docenti e personale sulla privacy e sulla sicurezza dei dati.
- Sensibilizzare studenti e famiglie sull'importanza della protezione dei dati personali.
- Nominare un RPD/DPO che sovrintenda alle pratiche di privacy e protezione dei dati.
- Adottare misure tecniche e organizzative adeguate a garantire la privacy.
- Promuovere una politica di trasparenza nella gestione dei dati personali.
- Adottare politiche per prevenire fenomeni di cyberbullismo e sexting.
- Promuovere buone prassi di educazione digitale.

Le scuole, inoltre, hanno l'obbligo di rendere noto (tramite apposita informativa) agli interessati le caratteristiche e modalità del trattamento dei loro dati, indicando i responsabili del trattamento. Gli interessati non solo gli alunni, ma anche le famiglie e gli stessi docenti. E' importante che, le scuole verifichino i loro trattamenti, controllando se i dati siano essedenti rispetto alle finalità del progetto.

La Liberatoria

La scuola deve richiedere l'autorizzazione attraverso liberatoria nel caso di divulgazione di immagini e/o video sul sito web della scuola, ma anche alle pagine Facebook o whatsapp.

In generale il garante dei dati personali stabilisce che le scuole devono rendere noto alle famiglie e ai ragazzi, attraverso un'adeguata informativa, quali dati raccolgono e come li utilizzano. E' bene ricordare che nel trattare queste categorie di informazioni gli Istituti scolastici devono porre estrema cautela, in conformità al "Regolamento sui dati sensibili" adottato dal Ministero dell'istruzione e del Merito.

Famiglie e studenti hanno il diritto di conoscere quali informazioni sono trattate dall'Istituto scolastico, farle rettificare se inesatte, incomplete e non aggiornate.

Nel caso di violazione, l'interessato potrà rivolgersi al Garante per la Protezione dei dati personali con apposita "segnalazione" gratuita o con un "reclamo" (più circostanziato rispetto alla semplice segnalazione e con pagamento di diritti di segreteria).

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.

1. L'accesso a internet è un 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 da Commissione per i diritti e i doveri di Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà.

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 quei 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 realtà, a partire dalla scuola.

Questo perché le nuove tecnologie permettono alla scuola di creare un ambiente aperto, flessibile e inclusivo e di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa.

Le scuole hanno la responsabilità di creare un ambiente sicuro non solo fisicamente, ma anche digitalmente. Questo impegno è supportato da diverse normative vigenti che mirano a proteggere gli studenti e il personale dai rischi online.

- **Legge sui Servizi Digitali (DSA)**, che impone obblighi alle piattaforme per ridurre i rischi, limitando la diffusione di contenuti illegali e aumentando la trasparenza;
- **Regolamento generale sulla Protezione dei dati (GDPR)**, secondo cui le scuole devono implementare misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio.
- **Regolamento per l'Uso delle Tecnologie Informatiche e della Comunicazione**, per un uso responsabile e sicuro di Internet e delle TIC(Tecnologie dell'informazione e della Comunicazione).Questo regolamento fornisce linee guida per l'accesso sicuro alle risorse online e la protezione contro i rischi digitali, come il cyberbullismo e l'accesso a contenuti inappropriati.

Dunque la scuola deve considerare l'ambiente online alla stregua dell'ambiente fisico e valutarne tutti gli aspetti legati alla sicurezza nel momento in cui permette l'accesso alla rete tramite i dispositivi della scuola o tramite anche i dispositivi personali nel caso del BYOD(Bring your own device) .

Indipendentemente dalle scelte dell'Istituto rispetto alla tipologia di strumentazioni e alle impostazioni di connessione, è necessario dotarsi di un regolamento d'Istituto sull'uso delle TIC da allegare alla e-Policy, dove saranno elencate in modo puntuale le regole nell'utilizzo della strumentazione tecnologica della scuola, ovvero le azioni che i docenti, personale scolastico e alunni/e possono e non possono compiere quando si connettono alla Rete e/o accedono a un dispositivo. Tale regolamento deve prevedere una parte sull'uso della strumentazione personale a scuola, sia nel caso del BYOD, qualora i docenti proponessero ai propri studenti l'uso di dispositivi personali (Tablet, PC o smartphone) in classe, ma anche regole per quanto riguarda la presenza degli smartphone a scuola, non a supporto delle attività didattiche.

Cloud e strumenti online

Il nostro Istituto ha già provveduto a creare un account istituzionale per ogni docente e ogni studente, con accesso alla piattaforma G.Suit. Questo facilita la comunicazione tra docenti, tra docenti e alunni e la gestione del cloud dovrebbe facilitare la gestione delle attività sia a scuola che a casa.

Per la gestione della comunicazione online la scuola si doterà di una Netiquette (regole di comportamento). Ogni classe sulla base della Netiquette generale potrebbe dotarsi di una netiquette di classe.

Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento rendendoli inclusivi e collaborativi. Sono diversi gli strumenti di comunicazione online che si possono utilizzare a scuola e che vanno ad integrare quelli tradizionali, rendendo la comunicazione più veloce e interattiva.. Tuttavia bisogna attivare una serie di azioni per prevenire i rischi online. Infatti, quando ci relazioniamo attraverso l'uso di strumenti di comunicazione online, mettiamo in atto una modalità comunicativa che ha caratteristiche e logiche proprie. Nella comunicazione attraverso le tecnologie non condividiamo lo stesso spazio e lo stesso contesto comunicativo con i nostri interlocutori. Per questo, alcune volte, può accadere che si forniscano cornici interpretative molto diverse dai messaggi e dai contenuti scambiati.

Inoltre la comunicazione non è mediata dall'interazione fisica (sguardo, tono della voce, gesti del corpo...) e non siamo in grado di vedere e di ascoltare direttamente gli effetti della nostra comunicazione sull'interlocutore. Ciò comporta che difficilmente potremo adeguare il nostro comportamento a partire da tali segnali poichè la distanza, la separazione attraverso lo schermo ci rendono meno empatici e attenti. Inoltre la comunicazione online si avvale di messaggi scritti che possono essere memorizzati, diffusi e permangono nel tempo.

D'altro canto, grazie agli strumenti di comunicazione online, possiamo usare un linguaggio accattivante, mediato da immagini, suoni e strumenti multimediali, coinvolgendo i genitori e i diversi attori nel processo educativo degli alunni.

E' importante mettere in evidenza che l'istituto si è dotato di strumenti di comunicazione sia interna che esterna .

Sono diversi gli strumenti di comunicazione online di cui la scuola si è dotata per raggiungere target esterni, al fine di valorizzare e promuovere le attività portate avanti dall'Istituto e per far circolare all'interno della scuola informazioni di servizio o contenuti importanti fra i diversi attori scolastici.

Fra gli strumenti di comunicazione esterna, troviamo in primis il sito web della scuola e poi profili social su Facebook e Instagram .

Tali strumenti, naturalmente, possono essere utilizzati, anche per fornire informazioni di servizio rivolte a studenti e famiglie. La nostra scuola , nella comunicazione esterna online parte da un piano di comunicazione in grado di trasmettere in modo chiaro e coinvolgente la mission e la vision educativa che l'istituto porta avanti.

Fra gli strumenti di comunicazione interna troviamo il registro elettronico, la classica mail, gli strumenti di messaggistica istantanei, la piattaforma G-Suite, che sono ampiamente utilizzati anche per facilitare e rendere più partecipata la didattica e la comunicazione a scuola.

In riferimento all'uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne, come avviene generalmente tra docenti mediante, ad esempio whatsapp o telegram, è importante ricordare quello che viene definito il "diritto alla disconnessione". L'art. 22 del CCNL 2016-2018, infatti, fa riferimento ai criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione fra la vita lavorativa e la vita familiare. E' importante, sottolineare che, per le chat informali fra colleghi, o fra docenti e genitori, non esiste una vera e propria regolamentazione, e per tale ragione è fondamentale, a partire dal buon senso e da una riflessione sulle peculiarità del mezzo, che si elaborino regole condivise sull'uso delle stesse.

Altro strumento essenziale a disposizione dell'istituto per la gestione delle presenze, assenze, valutazioni, prenotazioni di incontri e comunicazioni con le famiglie è il registro elettronico.

Il registro elettronico ci permette di gestire la comunicazione con le famiglie, le quali attraverso di esso possono visualizzare molte informazioni utili, interagendo con la scuola su:

- . andamento scolastico;
- . risultati scolastici;
- . eventi;
- . comunicazioni varie.

La finalità è che i docenti, i genitori e gli alunni utilizzino appieno le funzionalità del registro elettronico e della piattaforma G-Suite quali canali privilegiati per la comunicazione interna.

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.

Nell'ambito dell'adozione della politica BYOD(Bring Your Own Device), l'istituto promuove un uso responsabile e sicuro delle tecnologie dell'informazione e della comunicazione (ICT) da parte degli alunni e del personale. Gli alunni sono incoraggiati a portare i propri dispositivi personali (come laptop, tablet e smartphone) per supportare le attività didattiche , a condizione che tali dispositivi siano utilizzati in conformità con le linee guida stabilite dall'istituto.

L'uso dei dispositivi personali deve rispettare i seguenti criteri:

Sicurezza e Privacy: Gli alunni devono garantire che i loro dispositivi siano protetti da password e aggiornati con le ultime misure di sicurezza. E' vietato l'uso di dispositivi per scopi non didattici durante l'orario scolastico;

Accesso e Utilizzo: L'accesso alla rete scolastica deve avvenire tramite le credenziali fornite dalla scuola. L'uso delle risorse ICT deve essere finalizzato esclusivamente a scopi educativi e in conformità con le politiche di utilizzo accettabili dell'istituto;

Responsabilità: Gli alunni sono responsabili della cura e della manutenzione dei propri dispositivi. L'istituto non è responsabile per eventuali danni, perdite o furti dei dispositivi personali;

Formazione e Supporto: L'istituto fornirà formazione e supporto tecnico per garantire un uso efficace e sicuro delle tecnologie. Eventuali problemi tecnici devono essere segnalati tempestivamente al personale di supporto.

Attraverso queste misure, l'istituto mira a integrare le tecnologie digitali nell'insegnamento e nell'apprendimento, promuovendo un ambiente educativo e sicuro.

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 analogha 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 personale scolastico del nostro Istituto quando ha il sospetto o la certezza che un/a alunna possa essere vittima o responsabile di una situazione di cyberbullism, sexting o adescamento online ha a disposizione un protocollo con procedure definite e può fare riferimento a tutta la comunità scolastica.

Inoltre, un alunno, un genitore o chiunque voglia segnalare una situazione di bullismo o cyberbullismo, può fare riferimento ad un qualsiasi operatore scolastico (docente e non docente) che ha il compito di riferire immediatamente al Dirigente scolastico o al referente.

Questa sezione dell'E-policy contiene tutte le procedure definite all'interno del protocollo d'istituto per la gestione e segnalazione dei casi di bullismo e cyberbullismo .

(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 gli alunni in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola.

Nelle procedure:

- 1) sono indicate le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso;
- 2) le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

Inoltre, la scuola individua le figure che costituiranno un team preposto alla gestione della segnalazione.

Nell'affrontare i casi prevediamo la collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio, che verranno chiamati, 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.

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro agli alunni, alle famiglie e a tutti coloro che vivono la scuola, che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con la mobilitazione attenta di tutta la comunità.

(Link: Protocollo per la prevenzione e gestione dei casi di Bullismo e di Cyberbullismo)

https://drive.google.com/file/d/1PayA80O856KHkDUmZ6OlrCDyO3ZOT2wm/view?usp=drive_link

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

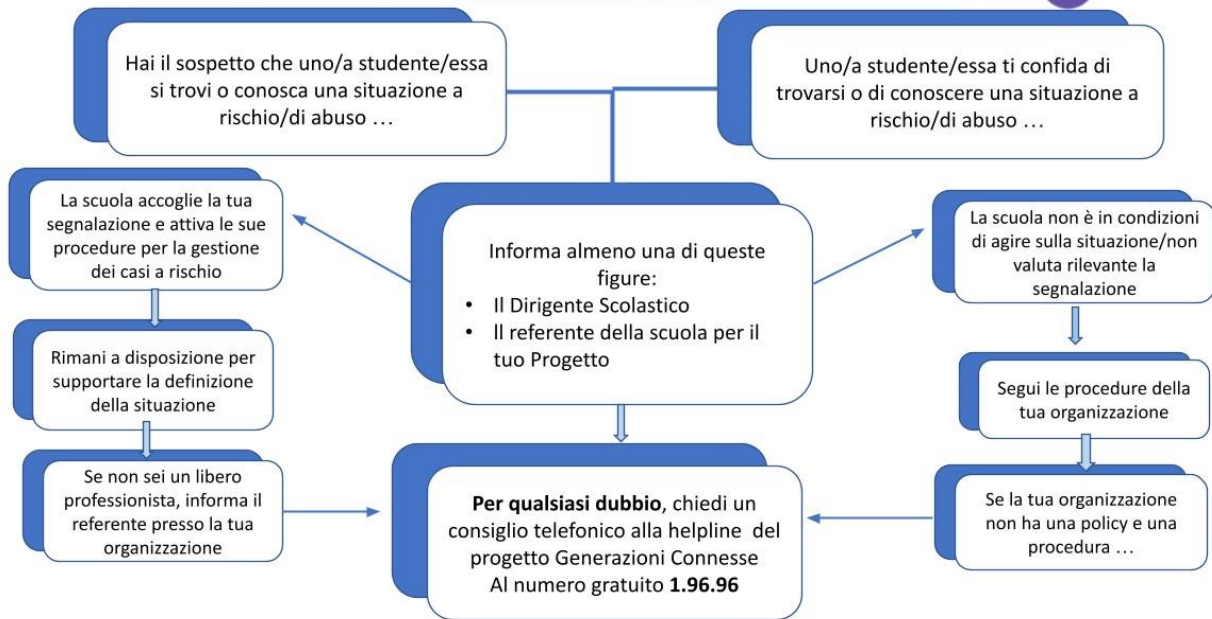
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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



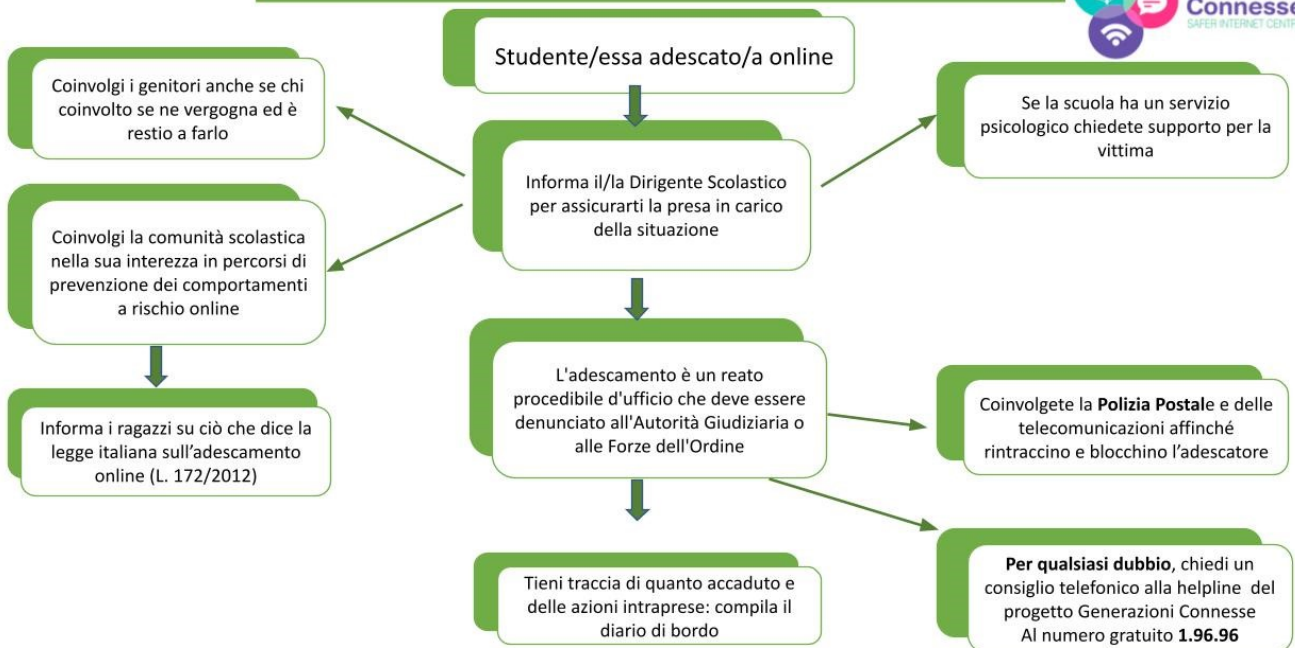
Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

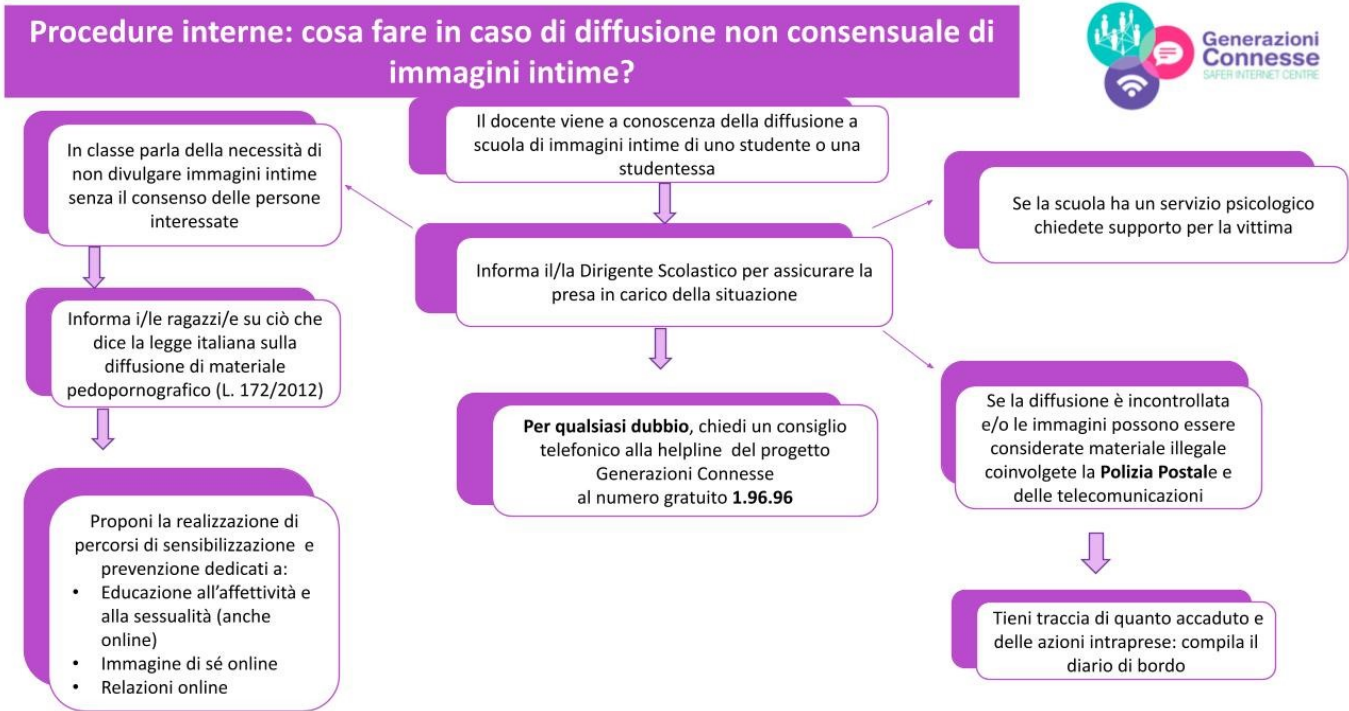


Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



Procedure interne: cosa fare in caso di Adescamento Online?





Per aiutare gli alunni, le famiglie e i docenti a segnare situazioni problematiche l'istituto ha redatto un vademecum per i docenti e un documento con le linee guida per docenti, alunni e famiglie con tutti gli strumenti e le procedure da attivare. (In Allegato)

La scuola mette a disposizione una serie di strumenti per la segnalazione dei casi di bullismo e cyberbullismo:

- . Modulo di segnalazione per docenti, genitori e alunni;
- . Indirizzo mail e numero di telefono dedicato e esposto in ogni aula dell'istituto;
- . Cassetta di raccolta segnalazioni ubicata nell'androne dei diversi plessi;
- . sportello di ascolto e consulenza psicopedagogica;
- . Referente per il Bullismo e Cyberbullismo e Gruppo di lavoro integrato, con supervisione del DS.

ALLEGATI

- Vademecum Docenti
- https://drive.google.com/file/d/1nQ91ehEhyro72vIraXrY25TvrfgWyxW4/view?usp=drive_link Linee guida per la prevenzione e la gestione dei casi di bullismo e cyberbullismo.
- https://drive.google.com/file/d/12wnh7d1WboCnYU88bC-udqOxmIMF5YZC/view?usp=drive_link Linee di orientamento ministeriali per la prevenzione e il contrasto al Bullismo e Cyberbullismo
- https://drive.google.com/file/d/1rLI9jUdJ0zUjETJSUEzxfTXoo7GfHTix/view?usp=drive_link Linee Guida Ministeriali 2017
-
-
-

https://drive.google.com/file/d/1gXR_DPaLKOK7ei2laQY9PoZqWx98Gg2j/view?usp=drive_link Modulo di segnalazione doc
https://docs.google.com/document/d/1ii1jto83LtQLVEykJsiOeDEubvV_BoSu/edit?usp=drive_link&oid=110215373797181687043&rtpof=true&sd=true