



Documento di ePolicy

D. D. FIDENZA

VIA XXV APRILE 24 - 43036 - FIDENZA
Parma (PR) - Emilia-Romagna
Data di approvazione: 27/04/2026 - 15:14

Cap 1 - Lo scopo della ePolicy

1.1 Scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

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

Capitolo 2 - Sensibilizzazione e prevenzione

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

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

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

Capitolo 4 - Segnalazione e gestione dei casi

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

1.1 Scopo dell'ePolicy

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

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

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

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

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

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

Questo documento spiega come la Direzione Didattica intenda porsi e agire, in considerazione degli obiettivi didattici ed educativi espressi nel PTOF e nel Regolamento d'Istituto, ma anche rispetto alla Legge 13 luglio 2015, n.107, al PNSD- Piano Nazionale Scuola Digitale, al DigComp 2.2 e alle linee guida per l'Educazione Civica (Decreto 7/09/2024) per aiutare e favorire gli alunni, i loro genitori e chiunque partecipi al processo educativo nell'utilizzo responsabile e sicuro di Internet e delle tecnologie della comunicazione per scopi didattici, personali e ricreativi.

Attraverso l'e Policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che consapevole, critica ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

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

Scopo del presente documento è quello di informare l'utenza su un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla scuola, nel rispetto della normativa vigente. Gli utenti, siano essi docenti o alunni, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la scuola promuove l'adozione di strategie e di strumentazioni tecnologiche che limitino l'accesso a siti e/o applicazioni illecite. In questo contesto gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiave per un uso critico e consapevole di Internet anche a casa, per evitare il verificarsi di situazioni potenzialmente pericolose. Le strategie previste dalla scuola per garantire la sicurezza in rete sono le seguenti:

- avvio di percorsi di formazione per un uso consapevole delle nuove tecnologie didattiche agli insegnanti nel corso dell'anno scolastico;
- coinvolgimento dei genitori come partner educativi nei percorsi di formazione che riguardano gli studenti;
- controllo random del sistema informatico (cronologia, cookies, etc...) da parte dei responsabili;
- installazione di firewall sull'accesso Internet;
- presenza di un docente o di un adulto responsabile durante l'utilizzo di Internet della piattaforma o di altre nuove tecnologie didattiche;
- aggiornamento periodico del software antivirus e scansione delle macchine in caso di sospetta presenza di virus;
- utilizzo di penne USB, CD/DVD o altri dispositivi esterni personali, solo se autorizzati.

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

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

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

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

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

IL DIRIGENTE SCOLASTICO

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

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

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

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

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

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

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

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

Il Team ha il compito di:

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

I/LE DOCENTI

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

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

RESPONSABILE DELLA PROTEZIONE DEI DATI

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

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

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

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

GLI STUDENTI E LE STUDENTESSE

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

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

I GENITORI/ADULTI DI RIFERIMENTO

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

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

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

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

Le nuove tecnologie sono ormai diventate parte integrante della vita di ogni individuo di ogni età e, in particolare, dei bambini e dei ragazzi, sia nella scuola che nell'extra-scuola. Esse sono strumenti potenti che offrono nuove ed eccitanti

opportunità in diversi ambiti, primo fra tutti quello della comunicazione. Attraverso l'uso delle tecnologie i docenti possono comunicare fra loro, con le famiglie, con gli alunni, in un mutuo scambio apprenditivo.

Le tecnologie, infatti, stimolano la discussione, promuovono la creatività, sviluppano e amplificano competenze, se opportunamente utilizzate aumentano la consapevolezza di sé e l'autostima, inoltre favoriscono gli apprendimenti significativi. Sono inclusive: abbattano o riducono distanze, barriere e differenze di genere, cultura e di abilità.

Ai bambini e ai ragazzi dovrebbe essere sempre garantita un accesso sicuro a Internet. In caso contrario, essi potrebbero incorrere in diversi rischi:

Accesso a video o a giochi on line inadatti.

Incapacità di valutare la qualità, l'accuratezza e l'affidabilità delle informazioni reperite in Internet.

Plagio e violazione dei diritti d'autore.

Download illegale di file video e/o musicali (Pirateria informatica).

Uso eccessivo e indiscriminato delle tecnologie e dei dispositivi.

Come per tutti gli altri rischi è impossibile eliminarli completamente. Diventa perciò essenziale, mettendo in atto strategie educative opportune, costruire nei bambini/ragazzi una resilienza ai rischi a cui possono essere esposti, in modo che essi possano acquisire la sicurezza e le abilità necessarie per affrontarli e gestirli.

Assicurarsi che i bambini e i ragazzi siano in grado di utilizzare Internet e le tecnologie della comunicazione in modo appropriato e sicuro diventa perciò un'esigenza da considerarsi attinente e derivante dal dovere di sorveglianza e di presa in carico a cui tutti coloro che lavorano nella scuola sono tenuti.

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

Inoltre 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.

I REFERENTI PER IL BULLISMO E CYBERBULLISMO

I referenti bullismo e cyberbullismo sono co-responsabili dell'attuazione dei piani di azione e coordinano le iniziative di prevenzione e contrasto del cyberbullismo.

In coerenza con le Linee di Orientamento per la prevenzione del Bullismo e Cyberbullismo del Ministero dell'Istruzione (D.M. n.18 del 13/01/2021), 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 di istituto che coinvolgano i 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.

I referenti hanno 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).

Intervenire (come gruppo ristretto, composto da Dirigente e referenti per il bullismo e cyberbullismo, psicologo e pedagogo, se presente) nelle situazioni acute di bullismo.

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

Anche i soggetti esterni che operino anche solo temporaneamente o occasionalmente a titolo di esperti nella nostra Scuola sono perciò tenuti a conoscere e rispettare tutti i regolamenti vigenti nell'Istituto in materia di uso del digitale.

Esiste per tutti l'obbligo di rispettare la privacy, soprattutto dei minori, in termine di fotografie, immagine, video o scambio di contatti personali (numero, mail, chat, profili di social network).

Pertanto tutti i soggetti interni ed esterni che sono responsabili di iniziative educative e formative nella nostra Scuola prendono visione e accettano la politica dell'Istituto riguardo all'uso consapevole e responsabile della rete e delle TIC, promuovono la sicurezza online durante le attività di cui sono responsabili e segnalano ai docenti referenti e/o al Dirigente Scolastico eventuali comportamenti a rischio o casi di condotte scorrette nell'uso della rete informatica e delle tecnologie digitali.

Per quanto non espressamente indicato sui ruoli e sulle responsabilità delle figure presenti all'interno dell'Istituzione scolastica, si rimanda: all'art 21 comma 8, Legge 15 marzo 1997, n. 59; all'art. 25 della Legge 30 marzo 2001, n. 165; al CCNL in vigore; al D.P.R. 8 marzo 1999, n. 275; alla Legge 13 luglio 2015, n. 107; al Piano Nazionale Scuola Digitale; a quanto stabilito in materia di colpa in vigilando, colpa in organizzando, colpa in educando.

Ruoli, compiti e responsabilità delle figure all'interno della Direzione Didattica Ilaria Alpi

DIRIGENTE SCOLASTICO

- Garantire la sicurezza, anche online, di tutti i membri della comunità scolastica.
- Garantire la tutela della privacy.
- Promuovere la formazione dei docenti sull'utilizzo positivo e responsabile delle tecnologie.
- Intervenire nei casi di gravi episodi di bullismo e cyberbullismo e di uso improprio delle tecnologie digitali.

ANIMATORE DIGITALE

- Redigere l'ePolicy, insieme ai referenti per il Bullismo e il Cyberbullismo, e provvedere alla diffusione del documento.
- Stimolare la formazione interna all'Istituzione degli ambiti di sviluppo della digitalizzazione.
- Gestire le piattaforme digitali dell'Istituto (GWorkspace) per scopi istituzionali consentiti: istruzione e formazione.

REFERENTI BULLISMO E CYBERBULLISMO

- Coordinare e promuovere iniziative per la prevenzione del bullismo e del cyberbullismo (incontri con le Forze dell'Ordine, laboratori con enti territoriali e regionali).
- Coinvolgere studenti, docenti e i genitori in progetti inerenti le problematiche del bullismo e del cyberbullismo.
- Coadiuvare il Dirigente Scolastico negli interventi di prevenzione del bullismo e del cyberbullismo.

DOCENTI

- Supervisionare e guidare gli alunni in attività di apprendimento che coinvolgano le tecnologie online.
- Segnalare prontamente al Dirigente Scolastico e alle famiglie eventuali episodi di violazione delle norme sull'utilizzo della rete da parte degli alunni.
- Vigilare sulla navigazione dei siti durante le lezioni che prevedono l'uso di internet.

RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD o DPO)

- Sorvegliare sull'osservanza della normativa in materia di tutela dei dati personali.

PERSONALE AMMINISTRATIVO E AUSILIARIO (ATA)

- Segnalare comportamenti non adeguati e/o episodi di bullismo o cyberbullismo.

ALUNNI

- Seguire le indicazioni dei docenti per un uso responsabile delle tecnologie digitali.
- Adottare comportamenti rispettosi anche durante la comunicazione in rete.

FAMIGLIE

- Contribuire, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete.
- Condividere quanto indicato nell'ePolicy dell'Istituto e nel Patto educativo di Corresponsabilità nell'ottica della collaborazione reciproca.

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 presente documento si integra per obiettivi e contenuti con i seguenti documenti che specificano le politiche del nostro

Istituto per un uso efficace e consapevole del digitale della didattica:

- PTOF
- RAV
- PdM
- Patto Educativo di Corresponsabilità
- Regolamento d'Istituto
- Codice interno di prevenzione del bullismo e del cyberbullismo

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.

Il documento di E-policy viene condiviso e comunicato a tutta la comunità educante, al personale, agli studenti e alle studentesse e alle loro famiglie attraverso:

- la pubblicazione sul sito istituzionale della scuola, in sezione dedicata raggiungibile anche dalla Home page;
- riferimenti e indicazioni sintetiche contenute nel Patto di Corresponsabilità, sottoscritto dalle famiglie e rilasciato alle stesse all'atto di iscrizione;
- momenti di formazione e informazione rivolti al personale/ studenti/ famiglie organizzati dal team per l'E-policy e dal Dirigente Scolastico.

Ciascun attore scolastico, personale docente e non docente e studenti, formati sulle regole di condotta da tenere in Rete e in merito all'uso corretto delle TIC a scuola, dovrà impegnarsi a sua volta a farsi promotore dello stesso all'interno della comunità.

Il documento e le sue eventuali modifiche e integrazioni, così come approvato dal Collegio dei Docenti e dal Consiglio d'Istituto, è esposto in versione cartacea semplificata, sotto forma di brochure/poster o infografiche, in vari punti strategici dell'Istituto, al fine di darne massima diffusione tra il personale docente e non docente e facilitare la consultazione da parte degli alunni.

Il monitoraggio periodico del documento, con cadenza triennale, che sarà realizzato con sondaggi tra il personale e gli studenti, mirerà a valutare la sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

In relazione agli esiti del suddetto monitoraggio, l'E-policy potrà essere aggiornata e sarà comunque implementata in ogni caso in cui intervengano cambiamenti significativi sia riguardo all'uso delle tecnologie digitali che alla normativa.

L'aggiornamento del documento di E-policy sarà curato dal Team costituito preposto alla sua stesura, in collaborazione con il Team per l'Innovazione Digitale e il Team Antibullismo.

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

Il nostro Istituto, nell'arco delle tre annualità, si propone di:

- formare un gruppo di docenti sul tema del cyberbullismo che siano di riferimento agli utenti dell'Istituto;
- diffondere l'ePolicy redatta e inserita nel Regolamento della Scuola e negli atti ad esso correlati;
- diffondere il documento ePolicy tra gli studenti/famiglia nell'ambito del curriculum di educazione civica;
- formulare il Regolamento per garantire l'uso corretto e sicuro delle tecnologie da parte di studenti e personale scolastico (PUA - Politica d'Uso Accettabile);
- organizzare annualmente interventi con le Forze dell'Ordine;
- elaborare attività a tema da proporre nelle classi;
- organizzare laboratori sull'educazione alle reazioni e alle emozioni.

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

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

Il nostro Istituto si propone di fare riferimento al Kit didattico di Generazioni Connesse, mettendo a disposizione di tutti i docenti il link di riferimento sul Sito della Scuola.

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.

Infatti, si considera necessaria la collaborazione di tutti gli attori educanti per perseguire la finalità comune di prevenire i rischi connessi ad un uso non consapevole delle TIC e promuovere un uso positivo, capace di coglierne le opportunità da queste offerte. La nostra Scuola si propone, in questa ottica, di rinforzare l'allenanza educativa con le famiglie e promuovere percorsi educativi continuativi e condivisi con queste ultime, per accompagnare insieme bambini e ragazzi verso un uso critico, consapevole, competente e responsabile delle tecnologie digitali.

Con l'ePolicy il nostro Istituto si impegna ad accompagnare la comunità educante e gli studenti verso una trasformazione digitale, offrendo strumenti per affrontare le sfide di un mondo in costante evoluzione tecnologica.

Attraverso interventi mirati e strategie condivise, la scuola punta a costruire un ambiente in cui ognuno, secondo il proprio ruolo, possa contribuire attivamente alla creazione della cultura digitale basata su:

- rispetto
- partecipazione
- responsabilità

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.

Il nostro Istituto si impegna a promuovere le competenze digitali seguendo il Piano Nazionale Scuola Digitale e le Raccomandazioni del Consiglio Europeo. Ogni intervento didattico previsto dal Curriculum Digitale viene progettato con riferimento alle aree fondamentali delle competenze digitali (DigComp 2.2):

Area 1 - Informazione: identificare, organizzare e analizzare le informazioni digitali

Area 2 - Comunicazione: saper comunicare e collaborare in ambienti digitali

Area 3 - Creazione di contenuti: creare e modificare contenuti digitali, rispettando i diritti di proprietà e le licenze

Area 4 - Sicurezza: proteggere i dati personali e l'identità digitale

Area 5 - Problem solving: risolvere problemi attraverso i mezzi digitali e utilizzare creativamente le tecnologie

mentre l'ePolicy definisce gli obiettivi e le strategie dell'Istituto per promuovere una cultura digitale consapevole e responsabile, il DigComp 2.2 fornisce una cornice metodologica precisa per identificare e sviluppare le competenze digitali necessarie per tutta la comunità scolastica.

Attraverso un approccio inclusivo e calibrato, il Curriculum Digitale risponde alle esigenze normative e si propone di contribuire in modo significativo alla formazione di cittadini attivi e responsabili del futuro.

In particolare i bambini saranno accompagnati a:

- conoscere e rispettare le regole di netiquette, indispensabili matrici di comunicazione tra utenti della rete per mantenere privati i dati sensibili propri e degli altri;
- saper distinguere il reale dal virtuale, saper identificare i rischi e comprendere come non cadere nella Rete;
- comprendere che la rete traccia e tiene memoria di tutto ciò che viene pubblicato e che la nostra web-reputation dipende dal nostro atteggiamento e dalla complessità dei nostri comportamenti in Rete;
- comprendere che le immagini in rete possono essere manipolate o utilizzate per scopi diversi da quelli della loro pubblicazione e che possono essere lesive della tutela della nostra privacy o di quella di terzi;
- comprendere il motivo per cui non bisogna pubblicare foto o video di altre persone senza il loro consenso esplicito;
- conoscere e riconoscere le diverse forme di cyberbullismo e di altri rischi on-line, imparando a difendersi e denunciare situazioni dannose per sè, senza rendersi complici di azioni a discapito di terzi;
- saper individuare persone e/o associazioni a cui rivolgersi per chiedere consiglio o aiuto in caso di bisogno;
- conoscere le conseguenze civili e penali delle proprie azioni sbagliate perpetuate in rete;
- appurare sempre l'attendibilità delle informazioni trovate in rete per difendersi dalle fake news e dall'utilizzo ingenuo

dell'intelligenza artificiale;

- rispettare il diritto d'autore on-line e imparare a citare sempre le fonti di riferimento delle informazioni acquisite.

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 nostro Istituto prevede, per docenti e studenti di ogni segmento interessato, l'utilizzo del Kit didattico sviluppato da Generazioni Connesse, uno strumento che raccoglie tematiche e contenuti che sono alla base dello sviluppo della cittadinanza digitale.

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.

Il nostro Istituto si occupa della fascia d'età dai 3 ai 10 anni, per questo è fondamentale evitare che gli alunni siano esposti ai contenuti inappropriati.

In fase di iscrizione le famiglie sottoscrivono un'informativa sul trattamento dei dati personali e rilasciano il consenso all'utilizzo di materiale fotografico ed audiovisivo e all'esposizione di elaborati dei propri figli nell'ambito dell'Istituto di appartenenza. Le fotografie e i video da pubblicare sul sito istituzionale che includano gli alunni sono selezionati con cura e non permettono l'identificazione del nome, a meno che non si tratti di eventi particolari per i quali viene richiesta specifica autorizzazione alle famiglie.

I dati personali degli alunni vengono trattati in conformità alla normativa vigente.

L'accesso ai dati riportati nel Registro Elettronico è riservato ai genitori dell'Istituto, tramite l'invio di una password di accesso strettamente personale. La Segreteria utilizza password nelle postazioni informatiche di lavoro, individua soggetti preposti alla gestione delle password, utilizza programmi antivirus. L'accesso agli atti è regolato dall'Amministrazione che deve valutare l'esistenza di presupposti normativi che permettano la presa visione o estratto copia conforme dei documenti ai soggetti con un "interesse diretto, concreto e attuale" alla conoscibilità degli atti.

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.

In un momento di transizione digitale significativo come quello che la Scuola sta attualmente vivendo, le tecnologie informatiche e le risorse di Rete si configurano come elementi strategici per innovare gli ambienti di apprendimento e sostenere la didattica a scuola, facilitando un approccio sempre più collaborativo tra studenti e all'interno del team educativo. L'uso degli strumenti di comunicazione on-line a scuola, che affianca senza sostituire l'utilizzo di quelli più tradizionali, ha quindi l'obiettivo non solo di rendere lo scambio comunicativo tra docenti, alunni e famiglie maggiormente interattivo e dinamico, ma di facilitare l'inclusione e la peer education, incrementando le competenze e l'autonomia degli studenti in ogni fascia di età. Nel nostro Istituto l'uso delle TIC segue obiettivi e regole precise, così come articolate nel Regolamento per l'uso corretto delle tecnologie digitali e di Internet, che integra al suo interno le misure relative alla Politica d'Uso Accettabile e Responsabile della Rete.

La comunicazione tra amministrazione e docenti, studenti e famiglie è affidata ai canali di comunicazione telematici: e-mail istituzionali all'interno della piattaforma LMS Google Workspace con dominio dell'Istituto, software di gestione amministrativa e bacheche di comunicazione sul registro elettronico che consentono comunicazioni personalizzate e possibilità di riscontro dell'avvenuta lettura.

Le comunicazioni interne rivolte al personale docente e non docente, dalle quali derivano impegni e obblighi di servizio per il personale stesso, vengono quotidianamente pubblicate sulla bacheca del registro elettronico e inviate via mail. Le operazioni sono svolte a cura del personale ATA di segreteria preposto, operativo nelle sole ore di servizio.

Le comunicazioni tra docenti e studenti e/o con le famiglie di questi avvengono principalmente attraverso il registro elettronico o attraverso la piattaforma Google Workspace, strumenti integrati occasionalmente da più tradizionali annotazioni scritte sul diario o da fonogrammi.

La comunicazione esterna istituzionale è invece effettuata attraverso il sito web ufficiale.

Il nostro sito utilizza il protocollo HTTPS, protocollo per la comunicazione Internet che protegge l'integrità e la riservatezza dei dati scambiati online.

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.

Il nostro Istituto riconosce il potenziale educativo dell'utilizzo di dispositivi a supporto delle attività didattiche. Tuttavia, l'uso di tali dispositivi è strettamente regolamentato e garantito solo previa autorizzazione del docente e per scopi specifici legati al percorso educativo-didattico.

È severamente vietato l'uso di dispositivi non autorizzati, come i cellulari, durante l'orario scolastico.

Agli alunni può essere consentito l'uso di dispositivi solo dietro precisa indicazione del docente, in presenza di una liberatoria firmata dai genitori e per specifiche attività didattiche o per l'inclusione degli alunni con disabilità e/o BES.

La Scuola non si assume responsabilità per danni, furti o smarrimenti dei dispositivi personali.

Eventuali violazioni delle regole comportano interventi disciplinari.

Nel fruire delle risorse sul web all'interno delle reti di Istituto, gli alunni si impegnano a:

- non scaricare materiali e software senza autorizzazione;
- non utilizzare device personali o unità esterne di archiviazione dati senza autorizzazione;
- segnalare immediatamente materiali inadeguati ai propri insegnanti;
- mettere in atto misure preventive per tutelare essi stessi e la privacy di soggetti terzi.

Mentre i docenti si impegnano a:

- guidare gli alunni all'uso della rete;
- dare consegne chiare e definire gli obiettivi delle attività;
- monitorare l'uso che gli studenti fanno delle tecnologie a scuola;
- mettere in atto misure preventive per tutelare essi stessi e la privacy di soggetti terzi.

Gestione dell'Infrastruttura e della strumentazione ICT della e nella scuola

PIANO DI AZIONI da sviluppare a partire dall'a.s. 25/26 e per il prossimo triennio:

- organizzare incontri in seduta plenaria con gli studenti in merito ai regolamenti sull'uso dei dispositivi digitali personali (BYOD) o prevedere momenti di confronto a piccoli gruppi nelle classi;
- organizzare incontri con le famiglie per fornire indicazioni o chiarimenti relativi ai regolamenti sull'uso dei dispositivi digitali personali;
- organizzare uno o più eventi volti a formare il personale in servizio sul tema delle tecnologie digitali e della protezione dei dati personali;
- organizzare uno o più eventi volti a formare i genitori/tutori sul tema delle tecnologie digitali e della protezione dei dati personali;
- organizzare uno o più eventi volti a formare il personale in servizio sui temi dell'accesso ad Internet e della cybersecurity.

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 si è dotato di un "Codice interno per la prevenzione e il contrasto dei fenomeni di bullismo e di cyberbullismo".

Il documento definisce le figure coinvolte e le procedure da seguire in caso di segnalazione.

Le procedure prevedono una serie di azioni strutturate:

- segnalazione
- valutazione del caso
- intervento
- monitoraggio e prevenzione.

L'obiettivo primario del documento è definire un protocollo di buone pratiche chiaro e accessibile a tutti, per prevenire, individuare e contrastare all'interno della nostra scuola qualsiasi atto riconducibile a tali fenomeni e, più in generale, a qualsiasi forma di violenza e di prevaricazione.

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

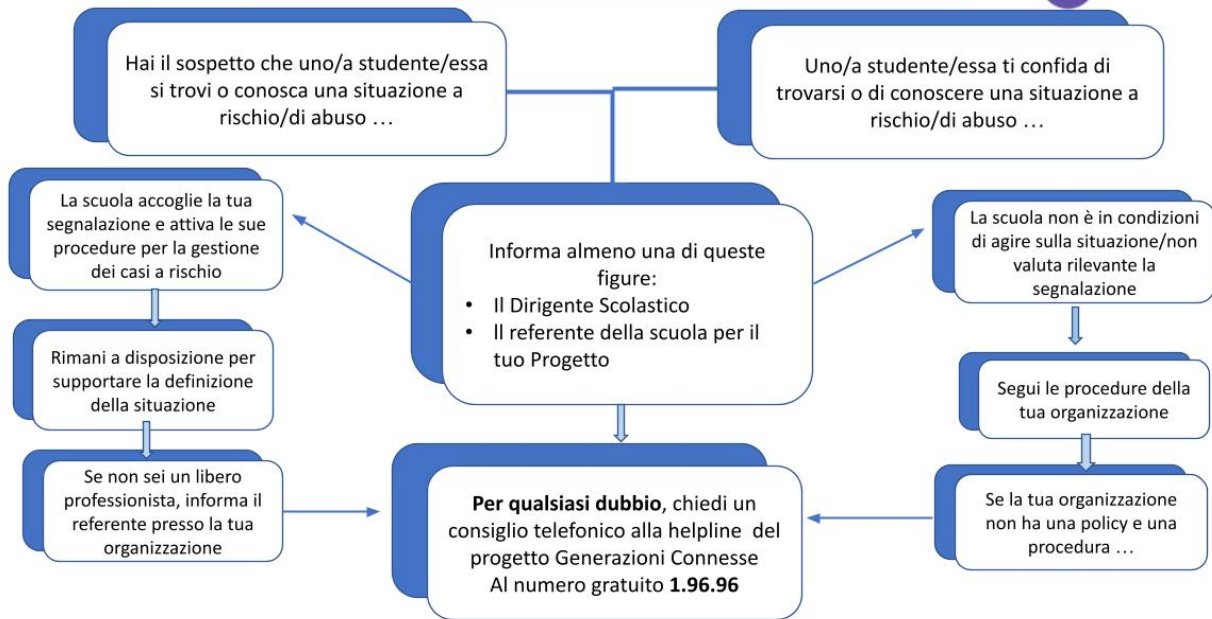
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

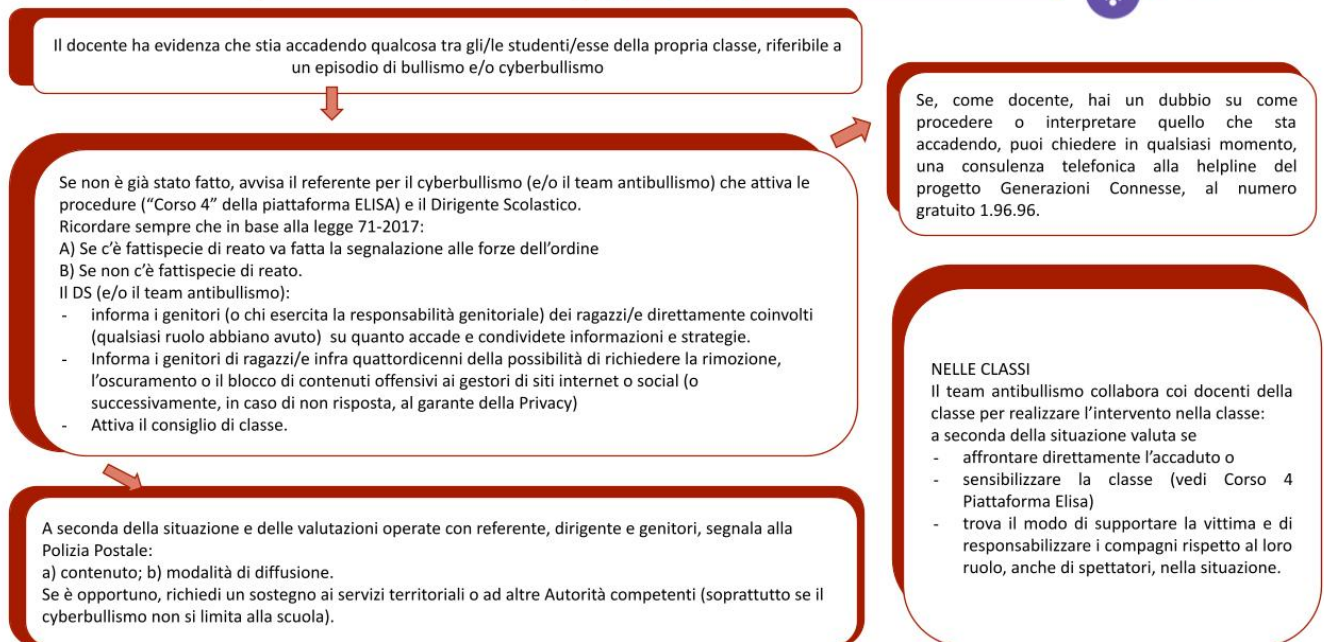
Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle [Linee di Orientamento per la prevenzione e il contrasto 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



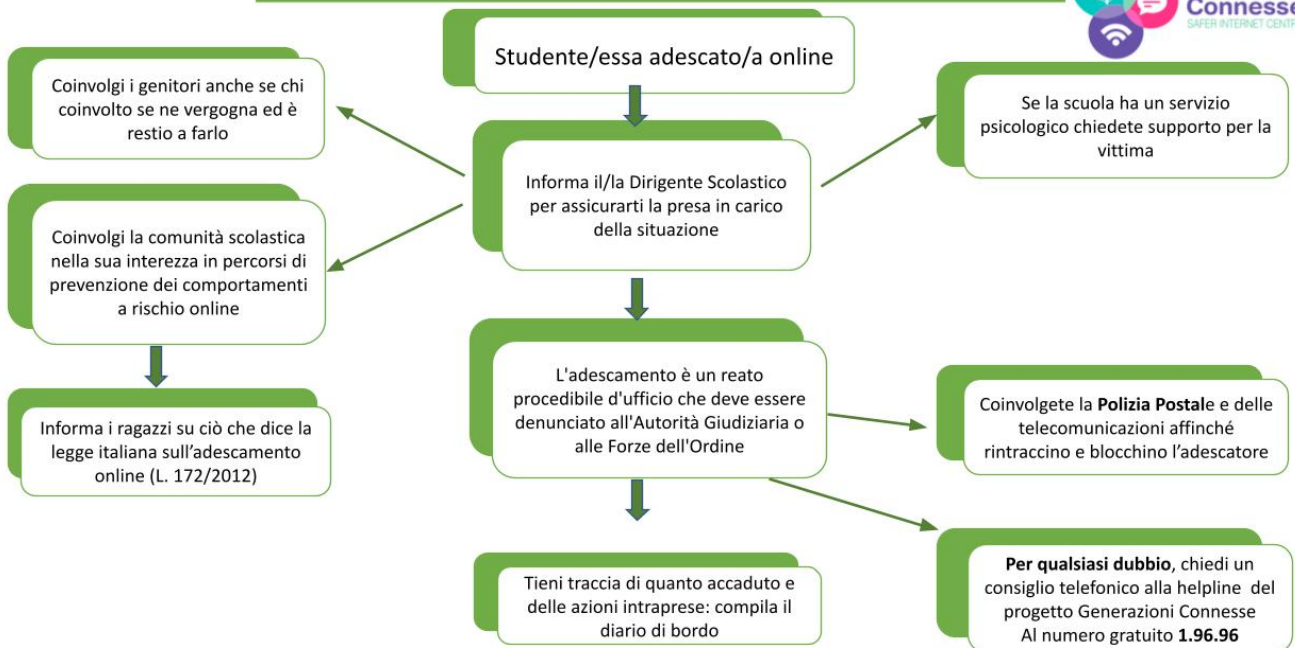
Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

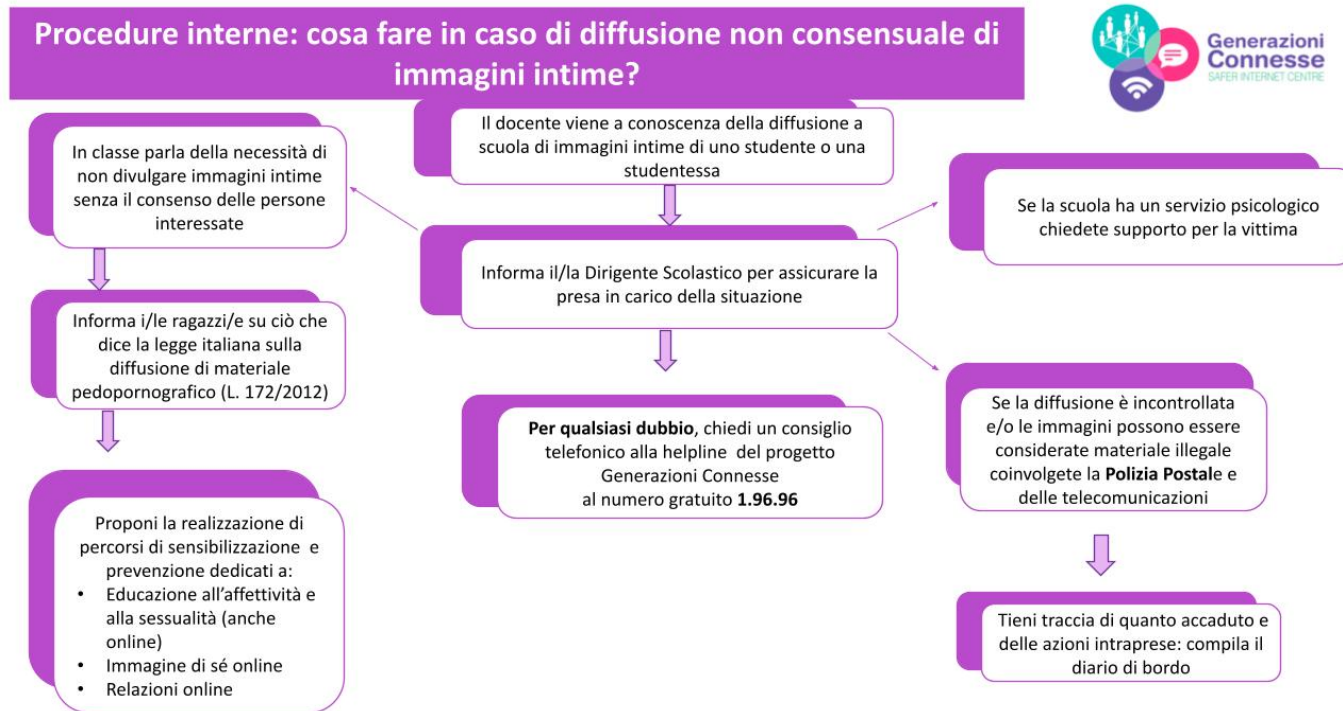


Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



Procedure interne: cosa fare in caso di Adescamento Online?





Strumenti a disposizione di studenti/esse e famiglie

Per prevenire i rischi sopra elencati la Direzione Didattica di Fidenza promuove la discussione sulle tematiche della Sicurezza in rete, cyberbullismo e sexting, attraverso:

- l'adesione a progetti dedicati,
- l'adesione a progetti a titolo gratuito,
- l'introduzione e l'adeguamento del Regolamento d'Istituto e del Patto di Corresponsabilità,
- la sensibilizzazione e l'attenzione alle tematiche con comunicazioni sul sito istituzionale della scuola,
- il continuo colloquio aperto con i docenti dei Team, dei membri delle Interclassi, del CDI (Consiglio d'Istituto) e del CDU (Collegio Docenti Unificato),
- incontri di formazione sull'utilizzo dei mezzi tecnologici raccolti ai genitori.

Le famiglie vengono sensibilizzate e invitate a incontri organizzati sul tema della Sicurezza in rete.

Tutti coloro che lavorano a scuola e sono coinvolti a vario titolo nei percorsi educativi degli alunni sono tenuti all'ascolto attento, ad essere d'esempio col proprio comportamento personale e a fornire spiegazioni e risposte chiare ai piccoli utenti e alle famiglie qualora se ne ravvisi la necessità.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali saranno gestite da:

- Dirigente Scolastico
- Referenti Bullismo e Cyberbullismo

Per aiutare i docenti a segnalare eventuali situazioni problematiche di cui sono venuti a conoscenza, la scuola prevede un indirizzo e-mail dei referenti bullismo e cyberbullismo:

referentibullismo@ddfidenza.istruzione.it

ePolicy