



Documento di ePolicy

P. DAGOMARI

VIA DI REGGIANA 86 - 59100 - PRATO

Prato (PO) - Toscana

Data di approvazione: 23/09/2025 - 14:16

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.

L' E-policy fornisce delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative sulle tecnologie digitali. L'ePolicy è un documento programmatico volto a promuovere le competenze digitali ed un uso positivo, critico e consapevole delle nuove tecnologie, sia da parte degli studenti che da parte del personale scolastico. Nello specifico, è un documento programmatico autoprodotta dalla scuola volto a descrivere:

- il proprio approccio alle tematiche legate alle competenze digitali, alla sicurezza online e ad un uso positivo delle tecnologie digitali nella didattica;
- il proprio approccio alle tematiche legate alle competenze digitali, alla sicurezza online e ad un uso positivo delle tecnologie digitali nella didattica;
- le norme comportamentali e le procedure per l'utilizzo delle Tecnologie dell'informazione e della comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione;
- le misure per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

Tra i principi che l'Istituto Dagomari riconosce e garantisce, vi sono il rispetto reciproco e la condivisione delle regole scolastiche, il diritto alla riservatezza, la trasparenza dell'attività amministrativa.

In merito al rispetto reciproco e alla condivisione delle regole scolastiche, tutte le componenti che operano all'interno dell'Istituto (studenti, docenti, Dirigente scolastico e collaboratori, personale amministrativo, genitori) si impegnano a collaborare in maniera costruttiva nell'assolvere le rispettive funzioni, scongiurando e condannando atteggiamenti arroganti, intimidatori, prevaricatori o violenti, soprattutto quelli a danno dei soggetti socialmente più deboli e svantaggiati. Per tale ragione tutte le componenti scolastiche si impegnano a conoscere e a rispettare, oltre che la normativa vigente, anche il Piano triennale dell'offerta formativa (PTOF), il Regolamento di Istituto (in particolare le sezioni relative al Regolamento di disciplina e al Regolamento sul bullismo e il cyberbullismo), il Patto di corresponsabilità scuola- famiglie e il presente documento di ePolicy.

In riferimento alla riservatezza, Dirigente scolastico e collaboratori, docenti e personale amministrativo, si impegnano a non divulgare dati personali e notizie riservate di cui vengano a conoscenza nell'esercizio delle loro funzioni. Gli studenti si impegnano a rispettare il diritto alla riservatezza dei propri compagni e degli operatori scolastici non diffondendo in alcun modo informazioni riservate, immagini, audio, video ecc. senza il consenso dei diretti interessati (a tale proposito si veda la Sezione "Uso dei cellulari e di altri dispositivi elettronici" del Regolamento di Istituto).

L'Istituto Dagomari, inoltre, si conforma ai principi della trasparenza, imparzialità e buon andamento dell'azione amministrativa. Si impegna pertanto ad agevolare gli interessati all'accesso alle informazioni e a comunicarle in modo tempestivo anche tramite il Registro elettronico. Si sottolinea che gli studenti hanno diritto alla trasparenza del processo valutativo, ossia di conoscere in modo chiaro e tempestivo le modalità e i criteri di valutazione.

Le modalità di comunicazione con docenti, studenti e genitori comprendono il Registro elettronico, il Sito web della scuola, la posta elettronica ordinaria ed, eventualmente, la posta elettronica certificata (PEC). Il personale in servizio può comunicare via chat, e-mail, telefono o social media ecc. con gli studenti esclusivamente per svolgere od organizzare attività di natura puramente didattica. E' fatto assoluto divieto di pubblicare audio, video, immagini senza il previo consenso dei soggetti interessati. Chiunque venga a conoscenza di attività espressamente vietate dalla legge o dal Regolamento d'Istituto è tenuto a darne comunicazione al Dirigente scolastico.

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 segue le pratiche migliori possibili nella gestione dei dati stessi;
- deve tutelare la scuola e garantire agli utenti la sicurezza di navigazione utilizzando adeguati sistemi informatici e servizi di filtri Internet;
- ha il compito di garantire a tutto il personale una formazione adeguata sulla sicurezza online per essere tutelato nell'esercizio del proprio ruolo educativo e non;

- deve essere a conoscenza delle procedure da seguire in caso di un grave incidente di sicurezza online;
- deve garantire adeguate valutazioni di rischio nell'usare strumenti e TIC, effettuate in modo che comunque quanto programmato possa soddisfare le istanze educative e didattiche dichiarate nel PTOF di Istituto;
- deve garantire l'esistenza di un sistema che assicuri il monitoraggio e il controllo interno della sicurezza online in collaborazione con le figure di sistema;
- deve essere a conoscenza ed attuare le procedure necessarie in caso di grave incidente di sicurezza online.

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

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

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

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

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

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

Il Team ha il compito di:

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

I/LE DOCENTI

I/le docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Possono, innanzitutto, integrare la propria disciplina con approfondimenti, promuovendo l'uso delle tecnologie digitali nella didattica. I docenti devono accompagnare e supportare gli/le studenti nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete. Inoltre, educano gli studenti alla prudenza, a non fornire dati ed informazioni personali, ad abbandonare un sito dai contenuti che possono turbare o spaventare e a non

incontrare persone conosciute in Rete senza averne prima parlato con i genitori. Informano gli alunni sui rischi presenti in Rete, senza demonizzarla, ma sollecitandone un uso consapevole, in modo che Internet possa rimanere per bambini/e e ragazzi/e una fonte di divertimento e uno strumento di apprendimento.

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

RESPONSABILE DELLA PROTEZIONE DEI DATI

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

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

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

GLI STUDENTI E LE STUDENTESSE

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

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

I GENITORI/ADULTI DI RIFERIMENTO

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

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

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

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

1.3 Integrazione ePolicy nei documenti scolastici

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

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

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

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

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

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

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore dello studente, ascoltare e prendere in seria considerazione le opinioni ed i desideri degli alunni, soprattutto se preoccupati o allertati per qualcosa. Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse, oltre che quelli legati a tollerare o a partecipare a comportamenti di minori che siano illegali, abusivi, o che mettano a rischio la loro sicurezza. Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto che disciplinano le modalità di utilizzo dei dispositivi personali (smartphone, tablet, pc, ecc.) e di quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto nel corso delle attività organizzate con gli studenti. Nel nostro Istituto vige l'obbligo di rispettare la privacy, soprattutto dei

soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network). Al fine di rendere l'ePolicy uno strumento efficace per la tutela degli studenti e delle studentesse, si individua un insieme di regole o norme di comportamento da condividere con le organizzazioni/associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve e/o lungo periodo. Dotarsi di un'informativa sull'ePolicy comprensiva delle procedure di segnalazione da

condividere con tutte le figure che operano con gli studenti, significa non solo tutelare questi ultimi e la scuola stessa, ma anche porre in essere nuove modalità per rilevare, limitare e contrastare possibili pericoli legati a condotte educative non professionali.

Le organizzazioni/associazioni extrascolastiche e gli esperti esterni sono tenuti a rilevare e a segnalare al Dirigente scolastico e ai Referenti bullismo e cyberbullismo le problematiche connesse ad un uso non corretto delle tecnologie digitali. In questo modo, si facilita l'intervento della scuola in chiave di prevenzione e di contrasto dei comportamenti scorretti e illeciti connessi all'utilizzo delle nuove tecnologie.

In coerenza con il percorso intrapreso e con le azioni che l'Istituto già pone in essere, la predisposizione di un'informativa sintetica sull'ePolicy, comprensiva delle procedure di segnalazione, garantisce un migliore rapporto fiduciario fra scuola e famiglia, consente di distinguere i ruoli e le azioni da compiere e di attivare direttamente, a seconda della tipologia dei casi da segnalare, le autorità competenti, collaborando con i servizi del territorio per la prevenzione e la gestione di quanto rilevato, in un'ottica di gestione condivisa degli interventi.

Tutti i soggetti esterni che erogano attività in ambito scolastico sono informati sui rischi online che possono correre gli studenti e le studentesse e sui comportamenti corretti che devono adottare a scuola.

I soggetti esterni sono tenuti a segnalare qualsiasi comportamento scorretto ai docenti responsabili del progetto, al Dirigente scolastico e ai Referenti bullismo e cyberbullismo, in qualsiasi forma, comunicando, per quanto possibile, i soggetti responsabili, le eventuali vittime, una descrizione il più possibile circostanziata dell'episodio.

La presente informativa è condivisa con il personale e le associazioni esterne: le figure professionali e le organizzazioni coinvolte in progetti, laboratori e attività ne prendono visione e si impegnano a rispettarla preliminarmente all'avvio dei programmi con gli studenti, in classe o fuori.

E' a discrezione dell'Istituto richiedere agli attori esterni, eventualmente, il casellario giudiziale come fattore ulteriormente protettivo verso i minori. L'obiettivo è quello di verificare l'esistenza (o meno) di condanne per alcuni reati previsti dal Codice penale e nello specifico gli articoli 600-bis (prostituzione minorile), 600-ter (pornografia minorile), 600-quater (detenzione di materiale pornografico), 600-quinquies (iniziative turistiche volte allo sfruttamento della prostituzione minorile), 609-undecies (adescamento di minorenni), o l'irrogazione di sanzioni interdittive all'esercizio di attività che comportino contatti diretti e regolari con i minori. L'eventuale presenza di un codice di condotta adottato dalla propria organizzazione o associazione (cooperativa, ente di formazione, servizio, etc.) è un fattore preferenziale.

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 viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/le studenti/esse) si faccia a sua volta promotore del documento.

L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene pubblicato sul sito istituzionale dell'Istituto.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

Il documento di ePolicy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. Nello specifico è importante tener presente che:

- condividere e comunicare il documento agli studenti e alle studentesse significa dare loro una base di partenza per un uso consapevole e corretto dei dispositivi e della tecnologia informatica;
- dare loro regole condivise di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici;
- dare loro elementi per poter riconoscere e quindi prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e.
- è importante condividere e comunicare il documento al personale scolastico in modo da poter orientare tutte le figure sui temi in oggetto, a partire da un uso corretto dei dispositivi e della Rete, in linea anche con il Codice di comportamento dei pubblici dipendenti;
- è fondamentale condividere con i genitori il documento e pubblicarlo sul sito istituzionale della scuola. La condivisione può avvenire anche tramite momenti di formazione specifici e durante gli incontri scuola-famiglia.

E' necessario, inoltre, che ciascun attore scolastico (dai docenti agli studenti) si faccia a sua volta promotore del documento. Ogni Consiglio di classe si occupa di informare gli studenti della classe e di verificare che si adottino comportamenti corretti nell'utilizzo delle nuove tecnologie.

Tutti gli atti fondamentali dell'Istituto contengono una o più sezioni nelle quali sono esplicitati diritti e doveri degli operatori scolastici, degli alunni e dei genitori o di coloro che esercitano la responsabilità genitoriale. Tali documenti sono pubblicati sul sito dell'Istituto.

Il genitore, sottoscrivendo l'istanza d'iscrizione, assume l'impegno di:

- a) osservare le disposizioni contenute nel Patto di corresponsabilità e nel Regolamento d'Istituto;
- b) sollecitarne l'osservanza da parte dello studente.

Il genitore è consapevole che:

- a) le infrazioni disciplinari da parte dell'alunno possono dar luogo a sanzioni disciplinari;
- b) in caso di danneggiamenti o lesioni a persone, la sanzione è ispirata al principio della riparazione del danno (art. 4, comma 5 del DPR 249/1998, come modificato dal DPR 235/2007);
- c) il Regolamento d'Istituto disciplina le modalità d'irrogazione delle sanzioni disciplinari e i mezzi d'impugnazione verso i provvedimenti disciplinari.

All'inizio dell'anno scolastico, in occasione della presentazione del Regolamento d'istituto agli alunni da parte dei docenti, verrà analizzata la ePolicy d'Istituto. Nel corso dell'anno ogni docente dedicherà alcune lezioni alle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al cyberbullismo (anche nell'ambito delle attività di Educazione civica).

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 Piano d'Azione dell'IIS P. Dagomari.

Azioni da svolgere entro un anno scolastico:

- Organizzare un evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti;
- Organizzare un evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti.

Azioni da svolgere nelle prossime tre annualità:

- Organizzare un evento di presentazione del progetto di Generazioni Connesse rivolto agli studenti;
- Organizzare un evento di presentazione del progetto di Generazioni Connesse rivolto ai docenti e personale ATA;
- Organizzare un evento di presentazione del progetto di Generazioni Connesse rivolto ai genitori.

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

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

Cap 2 - Sensibilizzazione e prevenzione

2.1 - Sensibilizzazione e prevenzione

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

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

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

L'Istituto Dagomari, si impegna a promuovere una cultura digitale consapevole e responsabile all'interno della propria comunità scolastica. La quotidianità in rete di ciascun membro della comunità scolastica 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. Per questo, la scuola si impegna a portare avanti percorsi volti a promuovere le competenze digitali, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie. Tali percorsi mirano a sviluppare l'alfabetizzazione informatica, la capacità di comunicazione e collaborazione online, la creazione di contenuti, la risoluzione di problemi e, soprattutto, la sicurezza online. L'Istituto si concentra su tre dimensioni chiave:

- **Dimensione Tecnologica:** Acquisizione di competenze di base, come la gestione degli strumenti digitali e la navigazione sicura.
- **Dimensione Cognitiva:** Sviluppo del pensiero critico per la ricerca, l'analisi e il trattamento delle informazioni online, imparando a distinguere fonti affidabili da quelle non veritiere.
- **Dimensione Etica:** Promozione di un comportamento corretto e rispettoso, basato sul riconoscimento dei diritti e dei rischi in rete, per una partecipazione attiva e responsabile.

A tal fine, l'Istituto si impegna a prevenire i rischi online.

Tale attività di prevenzione riguardano:

1. **Le minacce agli strumenti ICT:** mantenere aggiornato il sistema operativo dei dispositivi fissi e mobili, installare e aggiornare frequentemente i programmi antivirus e browser, attivare il firewall e mantenere il livello di sicurezza su medio-alto nelle impostazioni del browser per la navigazione in internet.
2. **Gli accessi a Internet:** mantenere riservate le credenziali (LOGIN e PASSWORD) di accesso alla rete Internet e ai servizi online, non accedere a siti web non certificati (deep web), non aprire email con mittente sconosciuto e non scaricare allegati, e non fornire le proprie credenziali tramite email (phishing).
3. **Le normative sulla privacy e il copyright:** l'Istituto si impegna nella formazione educativa sul rispetto della privacy delle persone (legge 196/2003). Vengono fornite indicazioni precise, come non fare foto e video senza autorizzazione delle persone ritratte o riprese (e se minorenni senza autorizzazione di entrambi i genitori), non pubblicare dati personali completi (cognome, nome, data e luogo di nascita) su social media e siti web sconosciuti, e

non utilizzare prodotti intellettuali digitali (foto, video, e-book, ecc.) senza rispettare il copyright o le licenze creative commons. I dispositivi personali possono essere usati a fini didattici solo se autorizzati dal docente.

Riconoscendo il ruolo cruciale dei docenti, l'Istituto, attraverso il team antibullismo e l'Animatore Digitale, organizza corsi di formazione specifici. Questi percorsi, in accordo con il Dirigente Scolastico, hanno l'obiettivo di aggiornare gli insegnanti sulle nuove sfide e opportunità del mondo digitale, fornendo loro gli strumenti didattici e le conoscenze necessarie per guidare gli studenti in modo efficace. L'Istituto si è impegnato concretamente nella sensibilizzazione e prevenzione attraverso diverse iniziative, che si integrano con le azioni previste dal Piano Nazionale Scuola Digitale (PNSD) e dal PNRR. Nel corso degli anni, l'Istituto Dagomari ha effettuato specifici interventi di sensibilizzazione, in particolare nelle classi del primo biennio, per il contrasto al bullismo e al cyberbullismo. Per rafforzare l'alleanza educativa, l'Istituto si impegna a coinvolgere attivamente le famiglie nell'educazione digitale, tramite attività di informazione e sensibilizzazione, creando una rete di supporto che si estende oltre le mura scolastiche.

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.

L'Istituto Dagomari si impegna a promuovere attivamente le competenze digitali in tutta la comunità scolastica, riconoscendole come essenziali per il successo personale e professionale nel XXI secolo.

A tal fine, la scuola integra le indicazioni del Piano Nazionale Scuola Digitale e della Raccomandazione del Consiglio Europeo sulle Competenze Chiave per l'Apprendimento Permanente (2018/C 189/01).

Il nostro approccio si basa sul Quadro di Riferimento Europeo DIGCOMP 2.2, che individua cinque aree di competenza digitale da sviluppare in modo organico e trasversale lungo l'intero percorso di studi. Queste aree non rappresentano semplici abilità tecniche, ma un insieme di conoscenze, attitudini e strategie necessarie per operare in modo consapevole e responsabile in un contesto digitale.

Le cinque aree, che costituiscono il fulcro del nostro curriculum digitale, sono:

- **ALFABETIZZAZIONE SU DATI E INFORMAZIONI:** Gli studenti imparano a identificare, localizzare, recuperare,

conservare, organizzare e analizzare le informazioni digitali. Questa competenza include la capacità di valutare l'affidabilità e la pertinenza delle fonti, distinguendo fatti da opinioni e riconoscendo le fake news.

- **COMUNICAZIONE E COLLABORAZIONE DIGITALE:** Vengono sviluppate le competenze necessarie per comunicare e interagire in ambienti digitali. Gli studenti imparano a condividere risorse, a collaborare su progetti online e a partecipare attivamente a comunità e reti digitali, nel pieno rispetto delle regole di convivenza civica e della netiquette.
- **CREAZIONE DI CONTENUTI DIGITALI:** Questa area si concentra sulla capacità di creare e modificare nuovi contenuti, dai testi alle immagini, dai video ai contenuti multimediali. Si incoraggia la creatività, l'integrazione e la rielaborazione di conoscenze, sviluppando anche competenze di base nella programmazione e nel rispetto dei diritti di proprietà intellettuale.
- **SICUREZZA:** L'Istituto pone un'attenzione particolare alla sicurezza online. Le attività formative mirano a educare gli studenti alla protezione personale, alla tutela dei dati e dell'identità digitale, e all'adozione di misure di sicurezza proattive. L'obiettivo è promuovere un uso del digitale che sia non solo sicuro, ma anche sostenibile e rispettoso della propria persona e degli altri.
- **RISOLUZIONE DI PROBLEMI:** Gli studenti sono guidati a utilizzare le tecnologie digitali per identificare e risolvere problemi. Questo include la capacità di valutare gli strumenti digitali più appropriati per un dato scopo, di risolvere problemi tecnici e di aggiornare le proprie competenze in un mondo in costante evoluzione. Questa area stimola il pensiero critico e l'adattabilità, essenziali per il loro futuro professionale.

Il Curricolo Digitale sarà strettamente collegato ai percorsi di Educazione Civica, come previsto dalla Legge 92/2019, per rafforzare l'educazione alla cittadinanza digitale in maniera organica e strutturata

2.3 - Il Kit Didattico

L'e-Policy prevede, a livello macro, un lavoro di lettura e d'intenti condivisi dall'intera comunità scolastica, a livello micro, invece, immagina che la singola classe lavori anche su tematiche direttamente collegate alla sicurezza in rete, ma complesse e di non immediata ricaduta nelle programmazioni scolastiche (etica e digitale, algoritmi, datafication). A tal fine si è progettato e predisposto del materiale che possa funzionare sia da attivatore, sia d'accompagnamento ai docenti e agli studenti nella fase più delicata ed incisiva del processo di prevenzione: la lezione in classe.

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

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

3.1 - Protezione dei dati personali e GDPR

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

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

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

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

Le istituzioni scolastiche, tra cui l'Istituto "Dagomari, affrontano quotidianamente la complessa sfida di educare le nuove generazioni non solo alla conoscenza di nozioni fondamentali, ma anche al rispetto dei valori cardine della nostra società.

Nell'era digitale, questo compito è ancora più cruciale, poiché richiede un'attenzione particolare ai principi di civiltà come la riservatezza e la dignità della persona.

Ogni giorno, la scuola tratta una vasta gamma di dati personali relativi a studenti, famiglie e personale. In alcuni casi, queste informazioni possono essere sensibili, come dati sanitari o relativi a particolari situazioni sociali. Pertanto, il "corretto trattamento dei dati personali" è una condizione essenziale per il rispetto della dignità e del diritto alla riservatezza di ogni individuo.

È fondamentale che la nostra scuola operi nel pieno rispetto della privacy, tutelando specialmente i dati dei minorenni. L'articolo 8 della Carta dei diritti fondamentali dell'Unione europea riconosce la protezione dei dati personali come un diritto fondamentale. Questo diritto è ulteriormente garantito dal Regolamento (UE) 2016/679, noto come GDPR (General Data Protection Regulation), e dal Decreto Legislativo 10 agosto 2018, n. 101. L'Istituto "Archimede" si impegna a rispettare scrupolosamente queste normative.

3.2 - Strumenti di comunicazione online (PUA)

La Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) è un documento che racchiude una serie di regole legate

all'utilizzo della rete a scuola e a casa da parte di studenti e di tutto il personale (compresi i professionisti esterni che lavorano in contesto scolastico), integrante il DPS (Documento programmatico sulla Sicurezza). Il documento, che funge da raccordo, si compone di punti strategici riguardanti non solo i vantaggi di internet a scuola ma anche i rischi connessi all'online, nella valutazione di quei contenuti presenti in rete e di quelle azioni negative che possono comprometterne l'uso positivo. Fra queste attività: ricercare materiale non consono allo stile educativo della scuola; produrre vere e proprie azioni illecite; giocare online con la rete scolastica; violare la privacy e i diritti d'autore, etc... Nella Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) vengono definite, dunque, le regole di utilizzo fra tutti gli attori in gioco, nel rispetto dei dati sensibili di ciascuno, in particolar modo degli alunni e delle alunne.

La rivoluzione digitale ha trasformato in profondità la società, il mondo del lavoro e, di conseguenza, l'ambiente scolastico. L'accesso a Internet e l'uso delle tecnologie digitali sono ormai parte integrante del processo educativo e della vita quotidiana di ogni studente e membro del personale. In questo contesto, l'Istituto "Dagomari" ritiene fondamentale non solo fornire una strumentazione all'avanguardia, ma anche educare a un uso consapevole e responsabile di tali risorse.

L'obiettivo è duplice: garantire la sicurezza e la protezione di tutti, e promuovere un approccio etico e costruttivo al mondo digitale, in linea con i principi di rispetto, privacy e cittadinanza digitale. L'Istituto "Dagomari" considera la sua infrastruttura ICT un pilastro strategico per la didattica innovativa e la gestione scolastica.

La nostra rete è progettata per essere robusta, sicura e scalabile, in grado di supportare una connettività ad alte prestazioni e un ambiente di apprendimento collaborativo. Il backbone di rete è basato su una connessione in fibra ottica a banda ultra-larga, che assicura un accesso a Internet veloce e affidabile in tutte le aree dell'istituto. L'intera struttura è dotata di un cablaggio strutturato (LAN) e di un'ampia copertura Wi-Fi (W-LAN).

A livello software, l'istituto ha adottato l'ecosistema Google Workspace for Education, che rappresenta la nostra piattaforma digitale centrale per la collaborazione. Tutti i membri della comunità scolastica (personale e studenti) hanno un account istituzionale che funge da identità digitale istituzionale. Tale account consente un accesso controllato e sicuro a tutti i servizi, come Google Classroom, Drive, Meet e la posta elettronica. Oltre a Google Workspace, l'intera gestione quotidiana delle attività istituzionali si avvale della piattaforma Argo del registro elettronico. Tale sistema è accessibile tramite profilo personale da parte di docenti, studenti, studentesse e famiglie. Offre strumenti essenziali per la gestione delle presenze, la documentazione della progettazione didattica, la prenotazione dei colloqui individuali scuola-famiglia e la consultazione di una bacheca per le circolari. La piattaforma è fondamentale anche per la gestione degli scrutini intermedi e finali. Il suo utilizzo è esteso anche ai servizi generali e amministrativi, con specifiche funzioni dedicate al personale ATA.

3.3 - BYOD

La presente ePolicy conterrà indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device"). Risulta infatti fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

La presente e-policy, integrando e specificando le disposizioni del Regolamento d'Istituto, definisce le regole sull'uso dei

dispositivi personali. L'obiettivo principale è avviare un dialogo costruttivo all'interno della comunità scolastica e dotarsi di una regolamentazione condivisa e chiara che, pur valorizzando le potenzialità della tecnologia, gestisca in modo efficace anche le eventuali criticità.

La nostra politica sull'uso dei dispositivi personali si basa sui principi sanciti dallo Statuto delle studentesse e degli studenti (DPR 249/1998). Pur riconoscendo il diritto a una "adeguata strumentazione tecnologica" che la scuola si impegna a fornire nei suoi laboratori e aule, viene ribadito il dovere di studenti e docenti di mantenere un comportamento rispettoso e coerente con i principi educativi.

Per questo motivo, l'Istituto "Dagomari" ha adottato una politica chiara:

- **Divieto di utilizzo dello smartphone:** In base a una recente circolare ministeriale, l'uso dei telefoni cellulari è sempre vietato sia agli studenti che al personale. Tale divieto risponde a una norma di correttezza e rispetto, mirata a favorire la concentrazione e la qualità del processo di insegnamento-apprendimento. Eventuali eccezioni sono ammesse esclusivamente per specifiche e documentate finalità autorizzate dalla Presidenza, che esulano dall'attività didattica ordinaria (ad esempio, per motivi di salute o situazioni di emergenza).
- **Utilizzo degli altri dispositivi personali (BYOD - Bring Your Own Device):** A differenza degli smartphone, l'uso di altri dispositivi personali come tablet e notebook può essere autorizzato dai docenti durante le lezioni, purché sia strettamente funzionale e integrato in attività didattiche specifiche. Questa flessibilità permette di valorizzare lo spirito di iniziativa degli studenti e di integrare strumenti personali che possono arricchire l'esperienza formativa.

L'Istituto si impegna a promuovere la cittadinanza digitale come dovere educativo primario. Formare i futuri cittadini della società della conoscenza significa educare alla partecipazione responsabile, all'uso critico delle tecnologie e alla costruzione delle proprie competenze in un mondo sempre più connesso.

Il Regolamento d'Istituto elenca in modo puntuale i comportamenti scorretti nell'uso dei dispositivi digitali e le sanzioni corrispondenti, in un'ottica di responsabilità condivisa tra scuola e famiglia. L'e-policy, come documento di indirizzo e programmazione, mira a perseguire tali obiettivi, potenziando le competenze digitali e favorendo un utilizzo costruttivo e consapevole delle tecnologie.

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 minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

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

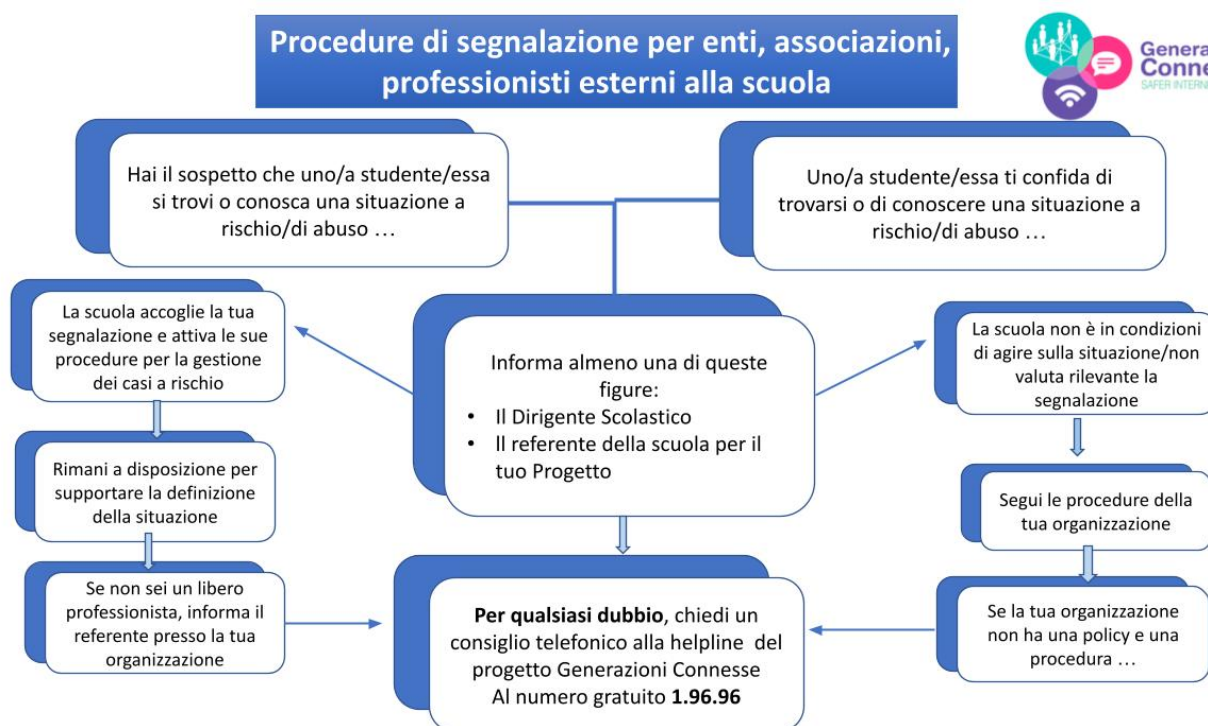
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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



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

Se non è già stato fatto, avvisa il referente per il cyberbullismo (e/o il team antibullismo) che attiva le procedure ("Corso 4" della piattaforma ELISA) e il Dirigente Scolastico.

Ricordare sempre che in base alla legge 71-2017:

A) Se c'è fattispecie di reato va fatta la segnalazione alle forze dell'ordine

B) Se non c'è fattispecie di reato.

Il DS (e/o il team antibullismo):

- informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto) su quanto accade e condivide informazioni e strategie.
- Informa i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy)
- Attiva il consiglio di classe.

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

NELLE CLASSI

Il team antibullismo collabora coi docenti della classe per realizzare l'intervento nella classe:

a seconda della situazione valuta se

- affrontare direttamente l'accaduto o
- sensibilizzare la classe (vedi Corso 4 Piattaforma Elisa)
- trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.

A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla Polizia Postale:

a) contenuto; b) modalità di diffusione.

Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



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

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

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

Insieme si valuta se è il caso

- di avvisare il consiglio di classe;
- di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.

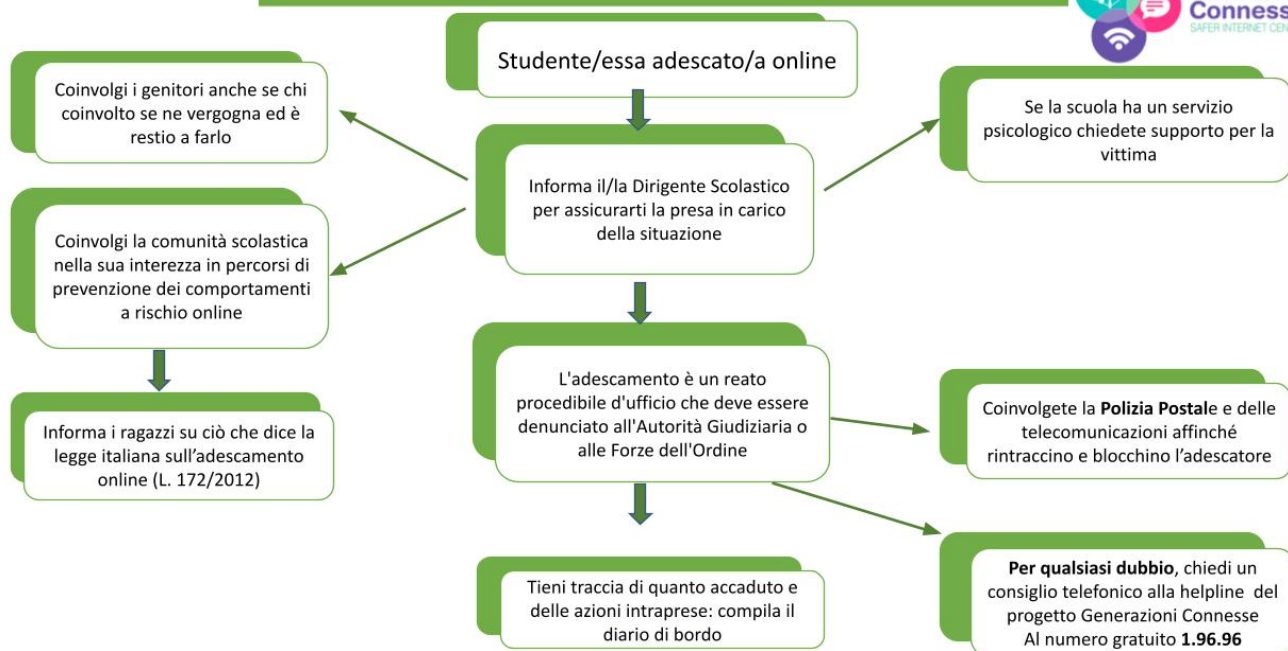
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

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

Se emergono evidenze passa allo schema successivo

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

Procedure interne: cosa fare in caso di Adescamento Online?



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

