



Documento di ePolicy I. C. ARZACHENA N. 1

VIA PIETRO NENNI10 - 07021 - ARZACHENA

Sassari (SS) - Sardegna

Data di approvazione: 18/09/2024 - 12:17

Cap 1 - Lo scopo della ePolicy

1.1 Scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

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

Capitolo 2 - Sensibilizzazione e prevenzione

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

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

Capitolo 4 - Segnalazione e gestione dei casi

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

1.1 Scopo dell'ePolicy

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

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

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

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

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

Le "competenze digitali" sono fra le abilità chiave all'interno del [Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente](#) e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una ePolicy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'ePolicy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

Perché è importante dotarsi di una ePolicy?

Attraverso l'ePolicy 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 sia consapevole, critico 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 TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

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

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

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

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

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

educante.

IL DIRIGENTE SCOLASTICO

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

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

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

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

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

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

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

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

famiglie e tutto il personale scolastico dell'esistenza del team, a cui poter fare riferimento per segnalazioni o richieste di informazioni sul tema.

Il Team ha il compito di:

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

I/LE DOCENTI

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

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

RESPONSABILE DELLA PROTEZIONE DEI DATI

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

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

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

GLI STUDENTI E LE STUDENTESSE

Gli studenti e le studentesse devono, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti. Con il supporto della scuola dovrebbero imparare a

tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le. Affinché questo accada devono partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

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

I GENITORI/ADULTI DI RIFERIMENTO

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

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

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

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

Il presente documento è condiviso da tutte le componenti educative che operano nella scuola ed in esso sono individuati ruoli e responsabilità correlate, così come di seguito indicati.

Il **Dirigente Scolastico** individua attraverso il Collegio dei Docenti un referente per il contrasto al cyberbullismo. Coinvolge, nella prevenzione e contrasto ai fenomeni del bullismo e cyberbullismo, tutte le componenti della comunità scolastica, particolarmente quelle che operano nell'area dell'informatica, partendo dall'utilizzo sicuro di Internet a scuola. Prevede all'interno del PTOF corsi di aggiornamenti e formazione in materia di prevenzione dei fenomeni di bullismo e cyberbullismo. Promuove azioni di sensibilizzazione dei fenomeni del bullismo e cyberbullismo nel territorio in rete con enti, associazioni, istituzioni locali ed altre scuole, coinvolgendo alunni, docenti, genitori ed esperti. Favorisce la discussione all'interno della scuola, attraverso i vari organi collegiali, creando i presupposti di regole condivise di comportamento per il contrasto e prevenzione dei fenomeni del bullismo e cyberbullismo. Prevede azioni culturali ed educative rivolte agli studenti, per acquisire le competenze necessarie all'esercizio di una cittadinanza digitale consapevole.

L'**Animatore Digitale** supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale". Monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola e ha il compito di controllare che gli utenti autorizzati usino gli account

forniti dall'Istituto e accedano alla Rete della scuola con apposita password solo per scopi istituzionali e consentiti (istruzione e formazione).

Il **Referente per il contrasto al Bullismo e Cyberbullismo** avvalendosi anche delle Forze di Polizia, delle associazioni e degli enti territoriali, coordina iniziative specifiche per: 1) la prevenzione e il contrasto del bullismo e cyberbullismo 2) la sicurezza, le problematiche connesse all'utilizzo della RETE e l'uso consapevole di internet. Cura rapporti di rete fra scuole per eventuali progetti/corsi/convegni/seminari e per la giornata mondiale sulla Sicurezza in Internet la "Safer Internet Day". Promuove la partecipazione a eventi specifici riguardanti la "Sicurezza in Internet" e "il Cyberbullismo" diretti agli studenti, allo scopo di informare i discenti dei pericoli e dei rischi connessi alla navigazione online, nonché di diffondere i criteri per l'individuazione e le modalità denuncia di fenomeni legati al bullismo e cyberbullismo. Supporta i docenti coinvolti in situazioni di emergenza e nella valutazione dell'accaduto e, se necessario, informa e coinvolge, genitori, docenti, dirigente e, infine, Autorità di Polizia, per l'immediato contrasto a quanto accaduto. Controlla che vengano applicati i protocolli per la corretta segnalazione e procedura nella gestione di eventuali casi di cyberbullismo.

Il **Collegio Docenti** promuove scelte didattiche ed educative, anche in collaborazione con altre scuole in rete, per la prevenzione del fenomeno. Promuove, approva e verifica l'attuazione di tutti i progetti e le azioni volte al contrasto di bullismo e cyberbullismo.

Il **Consiglio di Classe** pianifica attività didattiche e/o integrative finalizzate al coinvolgimento attivo e collaborativo degli studenti e all'approfondimento di tematiche che favoriscano la riflessione e la presa di coscienza della necessità dei valori di convivenza civile, in reciproca coerenza con quanto progettato e proposto dal referente per il bullismo e cyberbullismo. Favorisce un clima collaborativo all'interno della classe e nelle relazioni con le famiglie propone progetti di educazione alla legalità e alla cittadinanza attiva.

Il **Docente** intraprende azioni congruenti con l'utenza del proprio ordine di scuola, tenuto conto che l'istruzione ha un ruolo fondamentale sia nell'acquisizione e rispetto delle norme relative alla convivenza civile, sia nella trasmissione dei valori legati ad un uso responsabile di internet. controlla che vengano applicati i protocolli per la corretta segnalazione e procedura nella gestione di eventuali casi di cyberbullismo controlla che vengano applicati i protocolli per la corretta segnalazione e procedura nella gestione di eventuali casi di cyberbullismo. Valorizza, nell'attività didattica, modalità di lavoro di tipo cooperativo e spazi di riflessioni adeguati al livello di età degli alunni. Si confronta periodicamente e quando necessario con i Referenti per il cyberbullismo e il Dirigente Scolastico allo scopo di analizzare e descrivere i fenomeni aggregativi e disgregativi del gruppo classe. È il primo canale di informazione verso i genitori degli alunni nel caso si verificano casi legati a bullismo e cyberbullismo, in stretto contatto e con la collaborazione dei Referenti e del Dirigente Scolastico. Promuove un uso corretto delle tecnologie da parte dei ragazzi. È responsabile dell'utilizzo dei dispositivi digitali e tecnologici di classe (LIM, pc etc...) e relativo accesso al web. Dispone e programma, sotto la propria responsabilità e autorizzazione, l'utilizzo di device degli alunni al solo scopo didattico.

I **Genitori** partecipano attivamente alle azioni di formazione/informazione, istituite dalla Scuola, sui comportamenti sintomatici del bullismo e del cyberbullismo. Sono attenti ai comportamenti dei propri figli. Vigilano sull'uso delle tecnologie da parte dei ragazzi, con particolare attenzione ai tempi, alle modalità, agli atteggiamenti conseguenti (i genitori dovrebbero allertarsi se uno studente, dopo l'uso di internet o del proprio telefonino, mostra stati depressivi, ansiosi o paura). Conoscono le azioni messe in campo dalla scuola e collaborano secondo le modalità previste dal Patto di corresponsabilità. Conoscono il codice di comportamento dello studente. Conoscono le sanzioni previste da regolamento d'Istituto nei casi di bullismo, cyberbullismo e navigazione on-line a rischio.

Gli **Alunni** sono coinvolti nella progettazione e nella realizzazione delle iniziative scolastiche, al fine di favorire un miglioramento del clima relazionale. Imparano le regole basilari, per rispettare gli altri, quando sono connessi alla Rete, facendo attenzione alle comunicazioni (email, sms, mms) che inviano. Non è loro consentito, durante le attività didattiche o comunque all'interno della scuola, acquisire mediante telefonini cellulari o altri dispositivi elettronici immagini, filmati o registrazioni vocali, se non per finalità didattiche, previo consenso del docente. La divulgazione del materiale acquisito all'interno dell'Istituto è utilizzabile solo per fini esclusivamente personali di studio o documentazione, e comunque nel rispetto del diritto alla riservatezza di tutti, sempre sotto il diretto controllo e autorizzazione del docente. Egli vigila ed è

responsabile dell'eventuale utilizzo di dispositivi tecnologici individuali in classe. Durante le lezioni o le attività didattiche in genere non possono usare cellulari, giochi elettronici e riproduttori di musica, se non per finalità didattiche, previo consenso del docente.

Gli **enti educativi esterni** e le **associazioni** che entrano in relazione con il nostro Istituto Comprensivo si impegnano a condividere ed osservare le politiche interne sull'uso consapevole della Rete e delle TIC, attivando altresì procedure e comportamenti sicuri per la protezione degli studenti e delle studentesse durante le attività che vengono svolte in collaborazione con la scuola.

Ricordiamo, inoltre, che esiste una corresponsabilità educativa e formativa che riguarda sia i genitori che la scuola nel percorso di crescita degli studenti e delle studentesse.

Per un approfondimento sui ruoli e le responsabilità delle figure presenti a scuola si rimanda ai seguenti riferimenti normativi: Legge 59/97, Art. 21 CO° 8; Legge N.165/2001 Art. 25; CCNL; DPR n. 275/99; Legge n.107/2015; Piano Nazionale Scuola Digitale.

1.3 Integrazione ePolicy nei documenti scolastici

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

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

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

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

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

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

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'ePolicy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

Il nostro Istituto nel redigere questo documento fa espressamente richiamo ai contenuti del Regolamento d'istituto e in

modo particolare al Patto di Corresponsabilità educativa in adozione dal-- /--/20-- deliberato dal Consiglio di Istituto con delibera n. --.

Per l'istituto, il Patto di Corresponsabilità educativa rappresenta lo strumento cardine d' interrelazione fra scuola e famiglia. Il patto in questione è un "contratto educativo" che richiama alla responsabilità tutti gli attori coinvolti nel processo educativo.

Il documento che più trova affinità con ePolicy è il Regolamento di Istituto, che nasce dall'esigenza, attraverso norme e regole, di garantire un corretto funzionamento all'interno della comunità scolastica, anche quando si tratta della comunità scolastica virtuale.

I sopracitati regolamenti sono visibili e consultabili nel sito dell'istituto:

<https://www.comprensivoarzachena1.edu.it/scuola/le-carte-della-scuola/regolamenti>

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 ePolicy 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'ePolicy 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 esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali 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.

L'ePolicy è condiviso con gli alunni per fornire una base di partenza per un uso consapevole e maturo dei dispositivi e della tecnologia informatica; per dare loro regole condivise di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici; per dare loro elementi di riconoscimento e quindi prevenzione dei rischi sia personali che dei/delle propri/e compagni/e.

Momento privilegiato per la conoscenza del documento sarà l'inizio dell'anno scolastico, in occasione della illustrazione dei Regolamenti d'istituto, insieme ai regolamenti correlati. Nel corso dell'anno saranno dedicate da ciascun docente alcune lezioni, nell'ambito dell'Educazione Civica, alle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della Rete e alla lotta al cyberbullismo.

Tutto il personale sarà messo a conoscenza dell'informativa, in modo da acquisire consapevolezza in merito al fatto che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

1.5 - I Piani di Azione dell'ePolicy

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

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

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

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

1° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

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

MODULO II

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

MODULO III

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

MODULO IV

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

2° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

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

MODULO II

- L'istituto utilizza il kit didattico come pratica metodologica e risorse a disposizione dei docenti per i percorsi di ECD attraverso la formazione specifica sviluppata per i docenti attraverso il sito di Generazioni Connesse;
- Effettuare una rilevazione di interessi, bisogni, comportamenti, abitudini di studenti e studentesse sui temi

dell'educazione civica digitale;

- Realizzare una formazione rivolta agli studenti e alle studentesse attraverso il percorso previsto sulla piattaforma di Generazioni Connesse;
- Realizzare una formazione rivolta alle famiglie attraverso il percorso previsto sulla piattaforma di Generazioni Connesse

L'ePolicy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

Il monitoraggio dell'implementazione della ePolicy avverrà:

- contestualmente al Rapporto di Autovalutazione e sulla base dei casi problematici riscontrati e della loro gestione;
- contestualmente alla revisione del PTOF, a seguito di verifica atta a constatare l'insorgenza di nuove necessità e la revisione di tecnologie esistenti.

Anche i docenti saranno coinvolti nel monitoraggio del presente documento, allo scopo di verificare l'impatto che l'epolicy ha su tutta la comunità educante.

La revisione e/o l'aggiornamento del documento sarà curato dal gruppo di lavoro ePolicy di Istituto con la partecipazione, qualora si ritenesse opportuno, dei componenti del team digitale.

Il Piano d'Azione standard del nostro Istituto

Azioni da svolgere entro un'annualità scolastica:

- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Effettuare una rilevazione di interessi, bisogni e comportamenti delle famiglie sull'uso positivo del digitale

Azioni da svolgere nei prossimi 3 anni:

- Sperimentare il kit didattico elaborato da Generazioni Connesse e integrarlo nel curricolo di Educazione Civica, Ambito 3 - Cittadinanza digitale
- Monitorare le azioni adottate e l'uso della Rete da parte degli studenti

Il Piano d'Azione autoprodotta dal nostro Istituto

Azioni da svolgere entro un'annualità scolastica:

- Organizzare un percorso formativo rivolto ai docenti e svolto da esperti esterni con metodo teorico-pratico, sulla tematica della *Peer Education* come strumento per il contrasto al cyberbullismo (in raccordo al progetto di reti di scuole "CiSi@mo!!! EcoLOGIC@Mente" - Tutti insieme per contrastare e prevenire fenomeni di cyberbullismo e garantire la promozione del benessere)
- Organizzare laboratori formativi in classe svolti in favore degli alunni da esperti esterni per accrescere l'empatia e la responsabilità sociale, ridurre il pregiudizio (in raccordo al progetto di reti di scuole "CiSi@mo!!! EcoLOGIC@Mente" - Tutti insieme per contrastare e prevenire fenomeni di cyberbullismo e garantire la promozione del benessere)
- Costituire un team docenti di Antibullismo e per l'Emergenza

Azioni da svolgere nei prossimi 3 anni:

- Attivare processi di *Peer Education* per prevenire comportamenti socialmente negativi (come bullismo e cyberbullismo) e sviluppare le abilità socio-emotive negli studenti
 - Organizzare uno o più incontri dedicati alla prevenzione dei rischi associati all'utilizzo di Internet e delle tecnologie digitali, rivolti agli studenti, ai docenti e ai genitori con il coinvolgimento di esperti esterni.
-

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.

Il rischio online si configura come la possibilità per il minore di:

- commettere azioni online che possano danneggiare sé stessi o altri;
- essere una vittima di queste azioni; osservare altri commettere queste azioni.

È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e contenerli, ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. Ciò è possibile lavorando su aspetti di ampio raggio che possano permettere una riduzione dei fattori di rischio e di conseguenza una minore probabilità che i ragazzi si trovino in situazioni non piacevoli. È importante che abbiano gli strumenti idonei per riconoscere possibili situazioni di rischio e segnalarle ad un adulto di riferimento.

Gli strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio si configurano come interventi di sensibilizzazione e prevenzione.

Nel caso della **sensibilizzazione** si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.

Nel caso della **prevenzione** si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.

La responsabilità dell'azione preventiva ed educativa chiama in campo diverse agenzie educative oltre alla scuola, come la famiglia, le istituzioni, le associazioni e la società civile, ciascuna con un proprio compito nei confronti di bambini e bambine e di adolescenti. Tali agenzie sono chiamate a collaborare ad un progetto comune, nell'ambito di funzioni educative condivise. La necessità di questa collaborazione nasce, più o meno consapevolmente, dal riconoscimento sia da parte dei genitori che da parte degli insegnanti della rispettiva difficoltà a svolgere da soli la propria funzione formativa ed educativa. La necessità di sensibilizzare gli studenti ad un utilizzo sicuro e consapevole delle tecnologie digitali, sia in un'ottica di tutela dai rischi potenziali che di valorizzazione delle opportunità esistenti, pone tutta la comunità educante di fronte alla sfida di riconsiderare la propria identità, le proprie risorse e il proprio ruolo educativo.

Il nostro Istituto intende perseguire azioni di prevenzione universale e di sensibilizzazione, attraverso un'efficace integrazione con la rete dei servizi territoriali locali (Polizia postale, ASL...), al fine di formare e consolidare quelle competenze educative di base necessarie a poter gestire le situazioni di vita che i ragazzi sperimentano online. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.

L'Istituto si prefigge di intraprendere le seguenti azioni per la prevenzione dei rischi on line:

- Monitorare la realtà dell'istituto per la rilevazione delle problematiche derivanti da un uso non consapevole di internet e delle tecnologie digitali (in particolare violazione della Privacy, Cyberbullismo, Accesso a contenuti non adeguati).
- Promuovere la partecipazione del corpo docente ad attività formative. Sensibilizzare la Comunità Scolastica al problema dei rischi legati ad un uso non responsabile di internet e dei social.
- Organizzare eventi/attività volte ad incrementare la partecipazione e lo scambio tra studenti, genitori, insegnanti. Programmare progetti di peer education sui temi della sicurezza on line.
- Promuovere incontri e laboratori dedicati alla Cittadinanza Digitale.

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.

I ragazzi usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali".

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

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

Ciò avverrà attraverso la progettazione e implementazione di un curriculum digitale. La formazione del curriculum digitale non può non tener conto di quanto disposto dall'art. 5 della legge 20 agosto 2019 n. 92 (Introduzione dell'insegnamento

scolastico dell'educazione civica) interamente dedicato alla "cittadinanza digitale" intesa come capacità di un individuo di avvalersi consapevolmente e responsabilmente dei mezzi di comunicazione virtuali.

L'Istituto Comprensivo Arzachena 1 si è dotato nell'anno scolastico 2023-24 di un nuovo curriculum trasversale di educazione civica per competenze in cui è contemplata la competenza digitale.

La scuola, per implementare le competenze digitali degli studenti e dei docenti, adotta la piattaforma **Google Workspace for Education** secondo le modalità specificate nel capitolo 3 del presente documento.

L'Istituto, inoltre, coinvolge gli studenti nella sperimentazione del coding attraverso il progetto di Istituto "Dal Coding alla Robotica", integrando così le competenze digitali già previste dalle Indicazioni Nazionali, attraverso la promozione dello sviluppo del "pensiero computazionale" negli alunni.

Tenendo conto del Piano Scuola Digitale (PNSD), in particolar modo il paragrafo 4.2. su "Competenze e contenuti", il [Sillabo sull'Educazione Civica Digitale](#) e la Raccomandazione del Consiglio europeo relativa alle competenze chiave per l'apprendimento permanente (2018/C 189/01, p.9), l'istituto individua cinque aree di competenza digitale da sviluppare così come declinate all'interno del [quadro di riferimento DIGCOMP 2.2](#) (Quadro comune di riferimento europeo per le competenze digitali) e che sono incluse nel curriculum dello studente:

Area 1. INFORMAZIONE: identificare, localizzare, recuperare, conservare, organizzare e analizzare le informazioni digitali, giudicare la loro importanza e lo scopo;

Area 2. COMUNICAZIONE: comunicare in ambienti digitali, condividere risorse attraverso strumenti on-line, collegarsi con gli altri e collaborare attraverso strumenti digitali, interagire e partecipare alle comunità e alle reti;

Area 3. CREAZIONE DI CONTENUTI: creare e modificare nuovi contenuti (da elaborazione testi a immagini e video); integrare e rielaborare le conoscenze ed i contenuti; produrre espressioni creative, contenuti media e programmare; conoscere e applicare i diritti di proprietà intellettuale e le licenze;

Area 4. SICUREZZA: protezione personale, protezione dei dati, protezione dell'identità digitale, misure di sicurezza, uso sicuro e sostenibile;

Area 5. PROBLEM-SOLVING: identificare i bisogni e le risorse digitali, valutare appropriati strumenti digitali secondo lo scopo o necessità, risolvere problemi concettuali attraverso i mezzi digitali, utilizzare creativamente le tecnologie, risolvere problemi tecnici, aggiornare la propria competenza e quella altrui.

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.

Di seguito vengono indicate le misure che il nostro Istituto intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori e riferimento all'uso delle tecnologie digitali,. A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali.

La scuola ha l'obbligo di informare, tramite apposita informativa, gli interessati delle caratteristiche e delle modalità del trattamento dei loro dati, indicando i responsabili del trattamento. Gli interessati sono gli studenti, le famiglie e gli stessi insegnanti . E' importante verificare i trattamenti effettuati e controllare che non vi siano dati eccedenti rispetto alle finalità perseguite.

All'inizio dell'anno i genitori del nostro Istituto sottoscrivono un'[informativa sulla privacy](#) in ottemperanza all'ex art. 13 e 14 del D.Lgs 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali). L'accesso ai dati riportati nel registro elettronico (ritardi, assenze, note e valutazioni) è riservato ai genitori dell'Istituto, tramite l'invio di una password di accesso strettamente personale.

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.

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.

L'**AZIONE #6** del PNSD "Politiche attive per il BYOD (Bring your own device)" prevede che la scuola riconosca agli alunni la possibilità di una formazione digitale che parta dal saper utilizzare i propri dispositivi in modo consapevole.

Si legge testualmente nel Piano Nazionale: "La scuola digitale, in collaborazione con le famiglie e gli enti locali, deve aprirsi al cosiddetto BYOD (Bring Your Own Device), ossia a politiche per cui l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficientemente integrato".

Un ulteriore obiettivo di suddetta azione è quello di formare gli alunni ad una corretta gestione dei rischi e dei pericoli della Rete. ([DECALOGO BYOD MIUR 2018](#))

Il seguente Regolamento scolastico per l'attività Byod integra la sezione del [Regolamento di Istituto](#) dedicata all'uso dello smartphone e dei dispositivi mobili (artt. 30, 31, 33).

La tecnologia, se utilizzata in modo responsabile e corretto, fornisce agli studenti opportunità innovative per incrementare la loro cultura, in linea con quanto specificato nel PNSD.

Per questo motivo, l'Istituto vuole favorire tale processo garantendone la sicurezza attraverso una modalità di interazione che contribuisca al miglioramento dell'ambiente educativo e di apprendimento.

Pertanto, al di fuori di questo contesto, l'uso improprio dei dispositivi digitali mobili a scuola non è ammesso e viene sanzionato in misura della gravità in base a quanto stabilito dal Regolamento di Istituto e dal regolamento sull'uso dei cellulari, che rimane in vigore per tutto quanto non concerne la sperimentazione BYOD.

In particolare:

1. Sono ammessi a scuola i seguenti dispositivi: computer portatile, tablet, e-reader.
2. Non sono ammessi smartphone e dispositivi per videogiochi, quali console portatili. L'alunno è tenuto a conservare il proprio smartphone spento (non in modalità offline) nello zaino fino al termine delle lezioni. Lo stesso potrà essere riacceso soltanto dopo aver abbandonato l'edificio scolastico.
3. I dispositivi ammessi devono essere portati a scuola ed usati per SOLI scopi didattici, in momenti ben definiti, **ESCLUSIVAMENTE SU INDICAZIONE DEL DOCENTE**, e solo dopo autorizzazione esplicita dell'insegnante. Agli studenti non è permesso usare i dispositivi mobili per giochi, online e offline, durante le ore scolastiche.

4. È vietato agli alunni usare dispositivi di registrazione audio, videocamere o fotocamere per registrare video o fare foto in classe senza il permesso dell'insegnante e senza il consenso della persona che viene registrata o ripresa.
 5. Agli alunni non è permesso usare i propri dispositivi al di fuori dall'orario di lezione come ad esempio pause, ricreazione, uscite didattiche, visite guidate, viaggi d'istruzione, attività facoltative extracurricolari, manifestazioni sportive, spettacoli teatrali ecc., se non con l'esplicita autorizzazione del docente responsabile della classe.
 6. Gli alunni sono responsabili personalmente dei dispositivi portati a scuola e devono custodirli con cura e attenzione.
 7. La scuola non è responsabile della custodia dei dispositivi, di eventuali furti o smarrimenti e di eventuali danni ad essi cagionati dal proprietario o da altri.
 8. È in capo agli alunni la responsabilità di riportare a casa il dispositivo al termine delle lezioni. La scuola non assume la responsabilità per la custodia di nessun dispositivo lasciato a scuola.
 9. Agli alunni è vietato:
 - a. usare Internet per scopi diversi da quelli didattici;
 - b. scaricare musica, video e programmi da Internet o qualsiasi file senza il consenso dell'insegnante;
 - c. utilizzare i social network per fini diversi da quelli didattici e senza la supervisione del docente;
 - d. giocare sul computer, in rete o offline (a meno che il gioco non faccia parte di una lezione e sia supervisionato dall'insegnante).
 10. Utilizzare la Rete e i social network per deridere, offendere, denigrare compagni, docenti, personale scolastico, parenti/amici dei compagni; si ricorda che il cyberbullismo è un reato e qualsiasi atto degli studenti che dovesse configurarsi come reato verrà denunciato d'ufficio alle autorità competenti forze dell'ordine.
- Si suggerisce la sperimentazione in classe di una serie di [applicazioni e strumenti didattici](#) per poter sfruttare le potenzialità dei dispositivi con il metodo BYOD.

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.

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

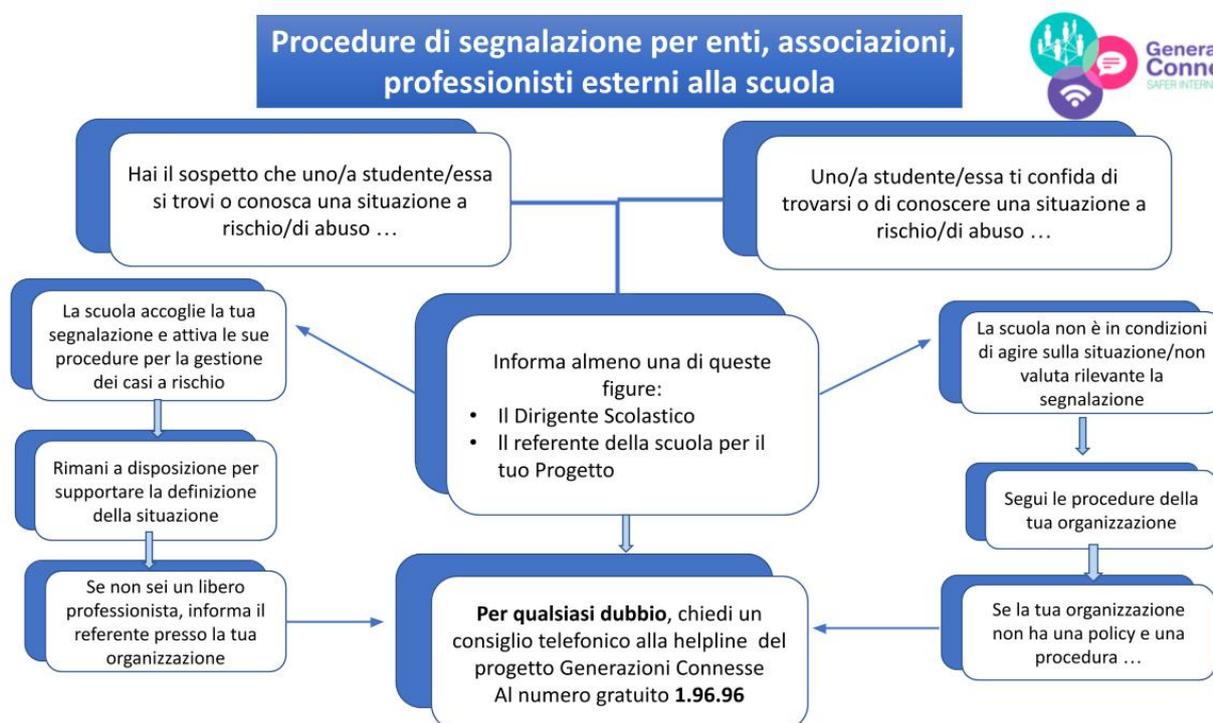
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

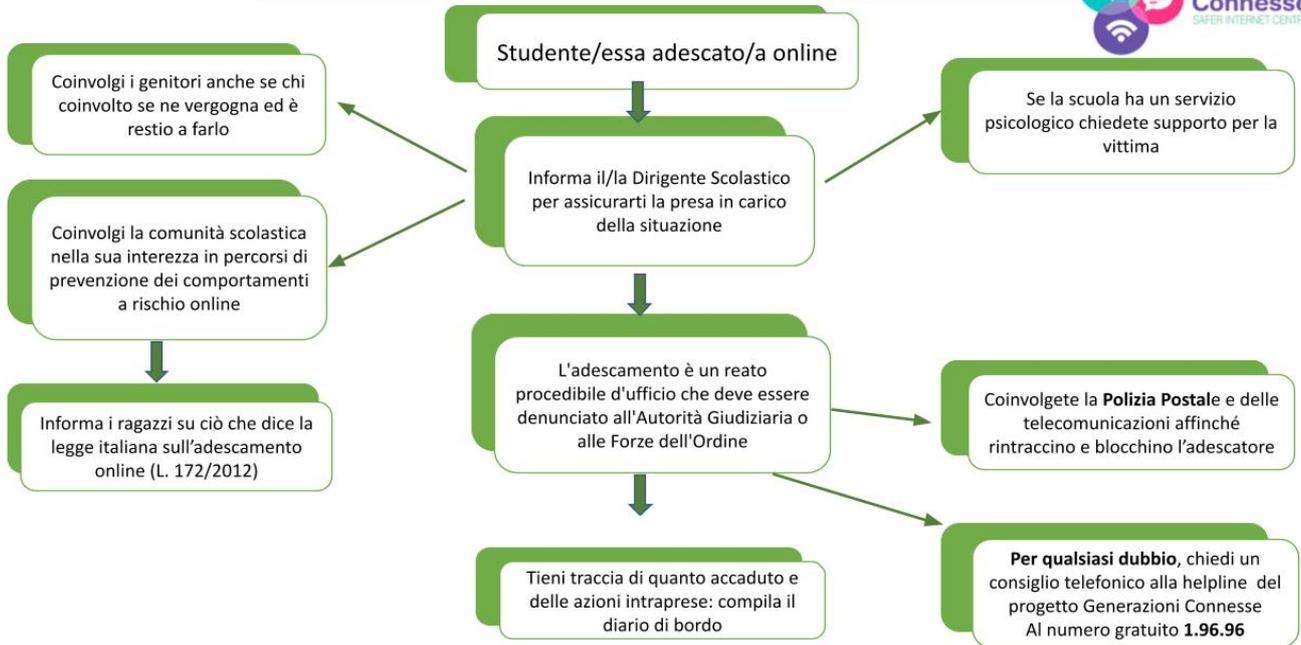
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

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?

