Documento di ePolicy

I.C. ALIGHIERI-KENNEDY - TORINO

VIA PACCHIOTTI 102 - 10146 - TORINO
Torino (TO) - Piemonte
Data di approvazione: 23/04/2026 - 09:35

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'Istituto Comprensivo Alighieri-Kennedy adotta la presente ePolicy come documento strategico per assicurare un ambiente digitale sicuro, responsabile e inclusivo, in continuità con la Legge 70/2024 e con le Linee di Orientamento 2021.

La nostra scuola ha maturato un'esperienza consolidata nella promozione della cittadinanza digitale, grazie a:

- l'utilizzo integrato di Google Workspace for Education per didattica, comunicazione e gestione documentale;
- le attività continuative del Team Antibullismo e dell'Animatore Digitale, che lavorano in sinergia nella prevenzione e gestione degli incidenti digitali;
- la partecipazione del personale alle formazioni del Safer Internet Centre, della Piattaforma ELISA e ai percorsi ministeriali sulla sicurezza online;
- progettualità interne che valorizzano un uso positivo delle tecnologie (Patentino digitale del SIC, podcast di Istituto, web radio, laboratori di media education, educazione civica digitale).

Nel nostro contesto l'ePolicy rappresenta un impegno condiviso che richiede:

- un approccio integrato tra competenze digitali, benessere online e educazione alle relazioni;
- una governance stabile composta dal Dirigente Scolastico, dal Referente per Bullismo/Cyberbullismo, dal Team Antibullismo, dall'Animatore Digitale e dal Team digitale;
- procedure chiare per l'uso degli strumenti digitali e per la gestione delle segnalazioni, in coerenza con il Regolamento d'Istituto e con il Patto di Corresponsabilità.

La presente ePolicy diventa pertanto il riferimento condiviso per tutte le azioni di cittadinanza digitale dell'Istituto e per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo, garantendo un percorso uniforme e riconoscibile a tutta la comunità scolastica.

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

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

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

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

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

IL DIRIGENTE SCOLASTICO

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

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

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

L'animatore digitale e il Team per l'Innovazione digitale sono co-responsabili, con il referente ePolicy, dell'attuazione dei

piani di azione in particolare in riferimento alla formazione dei docenti. Sono inoltre responsabili del controllo all'accesso da parte degli studenti delle Tic

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

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

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

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

Il Team ha il compito di:

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

I/LE DOCENTI

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

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

RESPONSABILE DELLA PROTEZIONE DEI DATI

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

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

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

GLI STUDENTI E LE STUDENTESSE

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

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

I GENITORI/ADULTI DI RIFERIMENTO

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

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

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

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

L'Istituto Comprensivo Alighieri–Kennedy conferma e rafforza la governance interna dedicata alla prevenzione del bullismo e del cyberbullismo e alla promozione della cittadinanza digitale.

È attivo un Team Antibullismo e per l'emergenza composto da Dirigente Scolastico, Referente e Commissione bullismo e cyberbullismo. Il Team opera in raccordo con i referenti di plesso, le Funzioni Strumentali, l'Animatore Digitale assicurando coerenza tra interventi educativi, monitoraggio dei fenomeni e gestione dei casi.

In attuazione della Legge 70/2024, l'Istituto prevede la progressiva istituzione di un Tavolo Interno di Monitoraggio Permanente, con la partecipazione di rappresentanti dei genitori e, per la scuola secondaria, degli studenti. Il Tavolo avrà funzione consultiva e di supporto nella valutazione delle azioni previste dall'ePolicy.

Tutta la comunità educante è coinvolta nella realizzazione dell'ePolicy:

- i docenti integrano nelle discipline i temi della cittadinanza digitale;
- il personale ATA supporta l'attuazione delle misure organizzative e di segnalazione;
- le famiglie collaborano attivamente nei percorsi formativi e nei processi di corresponsabilità educativa;
- gli studenti partecipano alle attività di sensibilizzazione, secondo età e grado di autonomia.

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.

L'ePolicy viene integrata nel Regolamento d'Istituto, nel Patto di Corresponsabilità e nel PTOF, con particolare riferimento alle norme sull'uso delle tecnologie digitali, alla prevenzione dei comportamenti a rischio online e all'educazione alla cittadinanza digitale.

Le versioni sintetiche della ePolicy, per studenti e famiglie, sono diffuse tramite:

- sito istituzionale;
- colloqui scuola–famiglia;
- attività di Educazione Civica;
- eventi di plesso e momenti informativi dedicati.

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

1. il curricolo 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.

L'I.C. Alighieri-Kennedy integra il presente documento nella propria organizzazione valorizzando competenze, pratiche e strumenti già consolidati nel corso degli ultimi anni. L'Istituto dispone di un Team Antibullismo attivo, composto da referente, Animatore digitale, Team Digitale e personale formato tramite Piattaforma ELISA, e opera in continuità con il percorso triennale di ePolicy Generazioni Connesse, già adottata e in corso di aggiornamento.

L'Istituto utilizza in modo sistematico la Google Workspace for Education come piattaforma digitale di riferimento, elemento che rende particolarmente rilevante l'allineamento tra ePolicy, regolamento d'Istituto e procedure interne sulla gestione degli account, dei dispositivi e della sicurezza digitale.

La scuola ha inoltre sviluppato negli anni un approccio integrato basato su:

- progetti continuativi di educazione digitale, podcast, web radio, attività laboratoriali e percorsi didattici mirati alla cittadinanza digitale;
- un curricolo verticale che già comprende attività di educazione civica digitale (DigComp 2.2) dall'infanzia alla secondaria;
- una rete territoriale consolidata con Polizia Municipale – Nucleo di Prossimità, ASL, associazioni locali ed enti del terzo settore, coinvolti annualmente in percorsi di prevenzione e sensibilizzazione;
- l'utilizzo sistematico del Kit Didattico Generazioni Connesse e di percorsi di supporto alle famiglie (incontri informativi, materiali digitali, attività nel Patto di Corresponsabilità).

L'ePolicy viene inoltre integrata:

- nel Regolamento d'Istituto, che sarà aggiornato con un'apposita sezione dedicata alla prevenzione del bullismo e cyberbullismo ai sensi della L. 70/2024;
- nel Patto di corresponsabilità, con richiami espliciti all'uso corretto degli strumenti digitali e alla collaborazione scuola-famiglia;
- nel PTOF, quale riferimento per la progettazione delle azioni di cittadinanza digitale e dei percorsi formativi docenti-studenti-famiglie.

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 dell 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

Per il nostro Istituto Comprensivo, i Piani di Azione vengono declinati valorizzando l'esperienza maturata negli anni precedenti nei progetti regionali e nazionali sul bullismo e cyberbullismo, nonché l'integrazione strutturale tra il Team Antibullismo, il Team Digitale e l'Animatore Digitale.

In particolare:

- la rilevazione dei bisogni formativi si fonda sui dati già raccolti negli anni precedenti attraverso i monitoraggi interni, la piattaforma ELISA e gli esiti dei progetti finanziati dalla Regione Piemonte, che costituiscono una base comparabile per il triennio;

- le azioni informative e formative verranno integrate con le attività già in essere nel PTOF (Patentino digitale per lo smartphone, progetto "Connessioni che costruiscono", formazione Google Workspace, percorsi per la cittadinanza digitale), così da evitare duplicazioni e potenziare la continuità educativa dalla primaria alla secondaria;

- la formazione dei docenti coinvolgerà congiuntamente il Referente Bullismo e l'Animatore Digitale, favorendo un approccio unitario alla gestione dei rischi online e all'uso consapevole delle tecnologie;

- la formazione degli studenti sarà integrata nei percorsi di educazione civica già attivi nei vari plessi, con attenzione alle specificità dei diversi ordini di scuola e alla continuità verticale;

- la comunicazione alle famiglie si innesterà su pratiche consolidate del nostro Istituto (incontri informativi annuali, sezioni dedicate sul sito, materiali brevi diffusi tramite registro elettronico);

- il monitoraggio delle azioni sarà svolto dal Team Antibullismo in collaborazione con il Team Digitale, con revisione annuale e con un report sintetico inserito nel RAV, nella sezione dedicata al benessere digitale degli studenti.

Le azioni triennali saranno sviluppate tenendo conto delle progettualità già avviate e delle collaborazioni territoriali consolidate (Polizia di Stato – Nucleo Prossimità, associazioni educative, enti locali), al fine di garantire coerenza, continuità e sostenibilità dell'intero percorso.

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

Nel nostro Istituto Comprensivo, le risorse di Generazioni Connesse rappresentano un riferimento stabile per la progettazione delle attività di educazione civica digitale. In continuità con le pratiche già avviate negli anni precedenti, il Team Antibullismo, l'Animatore e Team Digitale promuovono l'utilizzo periodico del Kit Didattico e dei contenuti multimediali del Safer Internet Centre per supportare attività in classe, incontri con le famiglie e momenti formativi rivolti al personale scolastico.

Particolare attenzione è dedicata alla selezione di materiali adatti alle diverse fasce d'età (primaria e secondaria di I grado), così da garantire un accesso guidato, coerente con i traguardi di competenza previsti dal curricolo digitale d'Istituto.
Le risorse online (webinar, video, percorsi formativi) vengono inoltre integrate all'interno delle unità di apprendimento dedicate all'Educazione alla Cittadinanza Digitale e sono condivise attraverso i canali istituzionali della scuola, favorendo una partecipazione informata e consapevole di studenti, famiglie e comunità educante.

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.

Nel nostro Istituto Comprensivo, le azioni di sensibilizzazione e prevenzione sono integrate stabilmente nella progettazione educativa e nella vita scolastica dei tre ordini di scuola, con un approccio progressivo e calibrato sull'età degli studenti.

In particolare, l'Istituto:

- integra sistematicamente i temi della cittadinanza digitale nella programmazione annuale, attraverso attività curricolari ed extracurricolari che utilizzano il Kit Didattico di Generazioni Connesse come riferimento metodologico comune;
- rafforza il raccordo tra Team Antibullismo e Team Digitale, garantendo che le attività di prevenzione online e offline siano coerenti e coordinate, nel rispetto della L.71/2017 e della L.70/2024;
- promuove percorsi di formazione verticale rivolti a docenti, studenti e famiglie, con particolare attenzione agli aspetti di benessere digitale, gestione responsabile dei dispositivi, uso consapevole dei social e prevenzione delle condotte a rischio;
- coinvolge le famiglie attraverso incontri tematici, materiali informativi sintetici e momenti di confronto all'interno del Patto di corresponsabilità educativa, affinché scuola e genitori condividano criteri educativi comuni;
- utilizza strumenti di monitoraggio e osservazione (questionari, analisi degli episodi, rilevazioni interne) per individuare precocemente segnali di disagio o comportamenti problematici e orientare azioni educative mirate;
- valorizza momenti istituzionali come il Safer Internet Day e le Giornate sulla Legalità per promuovere una riflessione condivisa sulla sicurezza digitale e sulle responsabilità nella comunità online.

Le strategie adottate mirano a sviluppare negli studenti una competenza digitale solida, rispettosa dei diritti propri e altrui, e capace di tradursi in comportamenti responsabili nella vita quotidiana connessa.

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 curricolo di educazione alla Cittadinanza Digitale previsto dalla L. 92/2019. Il curricolo prende forma attorno all'ePolicy e le attività didattiche sono legate al documento ed alle scelte dell'Istituto al suo interno.

Nel curricolo 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.

Nel nostro Istituto Comprensivo il curricolo digitale è sviluppato in modo verticale, dalla scuola dell'infanzia alla scuola secondaria di primo grado, garantendo coerenza e continuità nelle competenze previste dal DigComp 2.2 e dalla L. 92/2019. Le attività curricolari si integrano stabilmente con i progetti già attivi, tra cui l'aggiornamento dell'ePolicy, il percorso "Patentino Smartphone", le iniziative del Team Antibullismo, i progetti del Safer Internet Centre e le attività di educazione al pensiero critico realizzate tramite l'Animatore e Team Digitale.

Particolare attenzione è dedicata all'utilizzo consapevole degli strumenti digitali, alla sicurezza online e al contrasto di bullismo e cyberbullismo, con moduli didattici specifici in ciascun ordine di scuola e con l'impiego del Kit Didattico di Generazioni Connesse. Le competenze digitali vengono inoltre sviluppate attraverso attività laboratoriali, coding, robotica educativa, utilizzo delle piattaforme collaborative e azioni di cittadinanza digitale collegate al PTOF e all'ePolicy.

2.3 - Il Kit Didattico

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

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

Il nostro Istituto utilizza il Kit Didattico come strumento operativo per integrare attività mirate all'interno delle programmazioni. In particolare:

- nella scuola primaria, i moduli del Kit vengono utilizzati per introdurre, in maniera ludica e situata, temi quali l'identità digitale, il rispetto online e l'uso corretto dei dispositivi;

- nella secondaria di I grado, il Kit viene selezionato in base agli obiettivi disciplinari e spesso integrato con attività prodotte dall'Istituto (podcast tematici, simulazioni di casi, lavori collaborativi in Classroom).

Docenti formati tramite Generazioni Connesse supportano i colleghi nella scelta dei materiali più adatti alle classi, assicurando un utilizzo coerente e graduale delle risorse.
L'Istituto valorizza inoltre il Kit nelle collaborazioni con enti esterni, utilizzando i suoi contenuti come base comune di riferimento nei percorsi di sensibilizzazione rivolti a studenti e famiglie.

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.

Nel nostro Istituto Comprensivo la tutela dei dati personali è garantita attraverso un insieme coordinato di misure tecniche e organizzative finalizzate ad assicurare la protezione delle informazioni trattate in ambito scolastico.

L'Istituto si avvale di Google Workspace for Education, piattaforma adottata come ambiente digitale ufficiale, configurata in modalità protetta e conforme alla normativa vigente. La gestione degli account istituzionali, la definizione delle policy d'uso e le procedure di conservazione ed eliminazione dei dati avvengono secondo criteri uniformi e trasparenti comunicati a famiglie, studenti e personale.

Il Responsabile della Protezione dei Dati (RPD/DPO) collabora stabilmente con il Dirigente Scolastico, l'Animatore Digitale e il Referente Privacy nella valutazione dei rischi, nella verifica delle misure di sicurezza e nell'analisi delle richieste relative all'uso di applicazioni e servizi digitali.

Particolare attenzione è dedicata alla protezione dei dati dei minori:

- le comunicazioni online avvengono esclusivamente tramite gli account istituzionali;
- gli studenti accedono a servizi limitati e configurati per ridurre l'esposizione a rischi e contatti esterni;
- i materiali contenenti dati sensibili sono archiviati negli appositi Drive condivisi protetti, con accesso regolato dal principio di minimizzazione.

L'Istituto ha inoltre definito procedure interne per:

- la gestione dei data breach, in coordinamento con il DPO;
- l'uso controllato di applicazioni di terze parti, previa verifica congiunta di sicurezza, privacy e adeguatezza didattica;
- l'informazione puntuale a famiglie e personale attraverso informative aggiornate e disponibili sul sito istituzionale.

La cultura della protezione dei dati è promossa attraverso attività periodiche di sensibilizzazione rivolte a docenti, studenti e famiglie, con l'obiettivo di favorire comportamenti digitali consapevoli e rispettosi della normativa e del ruolo educativo della scuola.

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.

L'Istituto Comprensivo garantisce l'accesso alla rete a tutti i membri della comunità scolastica attraverso un'infrastruttura stabile, protetta e conforme alla normativa vigente. La connessione in fibra ottica è distribuita su tutti i plessi tramite rete cablata ed è protetta da un sistema firewall gestito da ditta esterna specializzata. Gli uffici della segreteria, del DSGA e del Dirigente Scolastico operano su una rete LAN dedicata, collegata a un server indipendente situato in un locale tecnico attrezzato e sincronizzato con un server esterno per assicurare elevati standard di continuità operativa e sicurezza dei dati.

L'Istituto adotta per tutto il personale scolastico e per gli studenti Google Workspace for Education come piattaforma istituzionale per la comunicazione, la collaborazione e la gestione dei contenuti digitali. Tutti gli account sono assegnati esclusivamente per finalità scolastiche e didattiche, nel rispetto del GDPR, e rimangono attivi per la sola durata del rapporto con la scuola.

Gli account degli studenti vengono eliminati il 1° agosto dell'anno in cui concludono il percorso di studi; quelli del personale scolastico a tempo determinato, in mobilità o in cessazione del servizio vengono disattivati nel periodo dal 1° agosto al 20 agosto dell'ultimo anno in cui prestano servizio. La disattivazione comporta la cancellazione definitiva dei contenuti: gli studenti possono esportare i propri file manualmente, scaricandoli dal Drive personale; il personale scolastico può esportare i propri dati tramite Google Takeout, funzione integrata nella piattaforma d'Istituto.

Per una corretta protezione degli account istituzionali, la scuola raccomanda l'utilizzo di password robuste,di custodirle con cura, di non conservarle nei dispositivi scolastici e di non condividerle con terzi, così da garantire la massima protezione

dell'account personale.

Gli account degli studenti e il loro Drive sono configurati per comunicare esclusivamente con utenti interni al dominio scolastico, riducendo la possibilità di interazioni improprie. La scuola mette in atto tutte le misure tecniche e organizzative possibili per tutelare gli alunni durante l'accesso alle tecnologie digitali; tuttavia, come previsto dal Patto di Corresponsabilità, non può essere escluso un rischio residuo legato alla navigazione in rete. È pertanto fondamentale una collaborazione attiva tra studenti, docenti, famiglie e personale ATA.

Servizi digitali messi a disposizione

Gli studenti accedono, tramite account istituzionale, ai seguenti strumenti:

- Gmail per l'invio e la ricezione di messaggi email;
- Google Documenti, Fogli, Presentazioni, Moduli, Keep, Vids per la produzione e la condivisione di contenuti digitali, anche in modalità di lavoro collaborativo;
- Google Drive per l'archiviazione e la condivisione di file;
- Google Meet per videocomunicazioni (per gli studenti è permessa solo la partecipazione e non la creazione);
- Google Sites per la creazione di siti didattici protetti;
- Google Chat per la messaggistica interna;
- Google Classroom come classe virtuale e ambiente di apprendimento digitale.

Il personale scolastico accede,oltre ai servizi disponibili per gli studenti, ha accesso a ulteriori applicazioni Google e ai servizi aggiuntivi della piattaforma.
In particolare, può usufruire di un ulteriore archivio denominato Drive condiviso, di proprietà della scuola. Questo spazio è destinato esclusivamente al lavoro collaborativo dei diversi team scolastici. Può essere usato per conservare la documentazione relativa ad attività d'interesse istituzionale (ad esempio la documentazione delle diverse commissioni e/o vari gruppi di lavoro), che deve rimanere a disposizione nel tempo indipendentemente dalla composizione dei membri del gruppo. Nel Drive condiviso devono essere archiviati documenti contenenti dati sensibili o altri materiali dei Consigli di classe e delle Interclassi, ai quali è possibile applicare livelli di protezione più elevati. I documenti caricati nel Drive condiviso diventano automaticamente proprietà dell'Istituto.
I materiali didattici e scolastici dei docenti devono essere conservati esclusivamente nel proprio spazio personale denominato"Il mio Drive".

La piattaforma offre inoltre strumenti di intelligenza artificiale: Notebook LM e Gemini, integrati in Workspace e conformi alle prescrizioni del GDPR, in quanto le conversazioni non alimentano modelli esterni.
Notebook LM è progettato in modo specifico per la didattica e per supportare il lavoro del docente, mentre Gemini offre diverse funzionalità anch'esse orientate all'uso educativo. L'Istituto predisporrà entro agosto 2026 un Regolamento per l'uso dell'Intelligenza Artificiale in coerenza con le Linee guida ministeriali.
L'adozione di applicazioni di terze parti è consentita solo previa verifica congiunta dell'Animatore Digitale, del referente privacy e del DPO. L'autorizzazione è subordinata a due requisiti imprescindibili: l'accertata valenza didattica dell'applicazione e la sua capacità di creare un ambiente virtuale controllato o una classe gestita direttamente dal docente.

Infine, l'accesso agli studenti sarà consentito esclusivamente tramite l'utilizzo di indirizzi email alternativi (alias), privi di dati personali identificativi, al fine di garantire la pseudonimizzazione degli allievi e la piena tutela della loro privacy.

REGOLE DI UTILIZZO DELLA RETE E DEI DISPOSITIVI

Gli studenti si impegnano a:

- Navigare in rete in modo sicuro e rispettoso, tutelando la propria privacy e quella altrui ed evitando la condivisione di dati personali, immagini o informazioni sensibili.
- Utilizzare la rete e i servizi digitali esclusivamente per scopi didattici e per le attività assegnate dagli insegnanti, evitando qualsiasi uso personale dei dispositivi, come l'accesso a siti di intrattenimento, social network o giochi online non pertinenti alle attività scolastiche.
- Rispettare le norme sul copyright e sulla proprietà intellettuale, citando correttamente le fonti e impiegando solo materiali di libero utilizzo (musica, foto e video).
- Usare i dispositivi messi a disposizione dall'Istituto solo per attività scolastiche e sempre sotto la supervisione dell'insegnante, attenendosi alle regole previste per il loro corretto impiego.
- Non prelevare i dispositivi dai luoghi di custodia né a utilizzarli senza la presenza e la supervisione dell'insegnante.
- Accedere sempre con il proprio account scolastico (evitando la sessione ospite) e disconnettersi sempre al termine della sessione di lavoro, eliminando il profilo memorizzato nel dispositivo.
- Avere cura dei dispositivi, evitando danneggiamenti e modifiche non necessarie, segnalando immediatamente eventuali malfunzionamenti.
- Lavorare preferibilmente in cloud, evitando il salvataggio locale dei file; in caso di download, salvare i file sul proprio Drive e cancellarli dal dispositivo.
- Non utilizzare chiavette USB o altri supporti esterni senza il permesso del docente.
- Usare un dispositivo personale (tablet o PC) solo se autorizzato dalla scuola per specifiche esigenze didattiche, seguendo le regole previste per i dispositivi della scuola.
- Comunicare con i compagni utilizzando Gmail e Google Chat, strumenti sicuri e protetti ed evitare di utilizzare app di messaggistica non istituzionali (es. WhatsApp, Telegram), non idonee per gli studenti di età inferiore ai 14 anni.
- Tenere il cellulare spento e riposto in un luogo sicuro durante la permanenza a scuola e non utilizzarlo per messaggi, foto, video o registrazioni negli ambienti scolastici.

I docenti si impegnano a:

- Formarsi nell'ambito dei temi della cittadinanza digitale e della didattica innovativa digitale promossa e sostenuta dal MIM.

- Promuovere l'uso consapevole e responsabile della rete internet e dei dispositivi negli studenti, provvedendo a garantire un ambiente digitale protetto, conforme alle norme sulla privacy e sul diritto d'autore.

- Essere responsabili dei dispositivi scolastici messi a disposizione dell'Istituto e responsabilizzare gli alunni sul loro uso corretto, sulla cura e sulla prevenzione di qualsiasi danno o manomissione volontaria, al fine di garantirne l'integrità e la conservazione nel tempo.

- Prenotare le risorse digitali secondo le procedure del plesso e occuparsi personalmente del loro spostamento dai luoghi di custodia alla classe.

- Supervisionare la consegna e il ritiro dei dispositivi, verificandone lo stato e assicurandone la corretta sistemazione e ricarica.

- Gestire il materiale audiovisivo di eventi e gite scolastiche caricandolo in una cartella Drive dedicata e condividendola su Classroom, garantendo che l'accesso sia riservato esclusivamente agli account istituzionali degli alunni, per assicurare la riservatezza e la protezione dei dati.

- Utilizzare i dispositivi scolastici esclusivamente per attività didattiche o legate al proprio ruolo professionale. Disconnettersi dal proprio account al termine dell'utilizzo e mantenere i dispositivi aggiornati quando possibile.

- Utilizzare la piattaforma digitale scolastica e il cloud unicamente per la creazione e l'archiviazione di materiali didattici, con divieto di uso per scopi personali o estranei alla funzione di docenza.

- Conoscere e utilizzare correttamente le funzionalità delle app di terze parti adottate e verificarne la corretta procedura di registrazione per gli studenti.

- Tutelare la privacy degli studenti in ottemperanza alla normativa vigente con particolare riferimento alla pubblicazione di contenuti sui social istituzionali

- Segnalare tempestivamente guasti o malfunzionamenti al Team Digitale.

I genitori si impegnano a:

- Custodire con cura le credenziali dell'alunno/a e non condividerle con terzi.

- Segnalare tempestivamente ai docenti eventuali problemi di accesso o il sospetto di utilizzo improprio da parte di altri.

- Non consentire l'uso della piattaforma a persone diverse dallo studente.

- Rispettare la riservatezza delle informazioni apprese tramite la piattaforma.
- Evitare la diffusione tramite social (WhatsApp, Telegram, ecc.) dei materiali didattici presenti su Classroom.
- Garantire che lo studente utilizzi l'account scolastico in modo corretto, assumendosi piena responsabilità per i contenuti creati, inviati o condivisi attraverso la piattaforma.
- Rispettare il presente regolamento, pena la sospensione dell'account da parte dell'Istituto.

Il personale ATA si impegna a:

- Rispettare la riservatezza dei dati trattati tramite strumenti digitali.
- Segnalare tempestivamente guasti o anomalie al Team Digitale o al DSGA.

BUONE PRATICHE D'UTILIZZO DEI DISPOSITIVI SCOLASTICI

Al fine di garantire la corretta gestione, conservazione e funzionalità dei dispositivi scolastici e relativi accessori, si riportano le seguenti buone pratiche:

Gestione degli account e della sicurezza:

- Disconnettersi sempre dal proprio account al termine della sessione di lavoro ed eliminare il profilo memorizzato nel dispositivo in caso di utilizzo dei Chromebook.
- Segnalare immediatamente eventuali accessi non autorizzati o comportamenti sospetti.

Uso corretto dei dispositivi:

- Maneggiare i dispositivi con cura, evitando urti, cadute o esposizione a liquidi.
- Posizionare i dispositivi su superfici stabili e lontano da bordi o zone di passaggio.
- Non sovrapporre oggetti pesanti sui dispositivi, in particolare quando sono chiusi o riposti.
- Evitare di consumare cibi o bevande in prossimità dei dispositivi per prevenire danneggiamenti accidentali.

Gestione dei cavi e degli accessori:

- Inserire ed estrarre con estrema delicatezza i cavi HDMI e USB nelle porte dei PC e dei pannelli interattivi, senza forzare o piegare i connettori.
- Conservare i cavi in modo adeguato, senza avvolgerli strettamente o annodarli, per evitare rotture interne.

- Riporre i caricatori dei dispositivi nella scatola originale del dispositivo stesso, lasciando il cavo elettrico libero e non compresso.
- Raccogliere i cavi HDMI dopo l'uso, inserendoli nella maniglia laterale del pannello o sul gancio apposito, senza abbandonarli a terra dove potrebbero essere calpestati o danneggiati.
- Riporre gli accessori del pannello (penna e/o altro) in un luogo sicuro dell'aula per evitare smarrimenti o furti.
- Verificare che tutti gli accessori (cavi, caricatori, mouse, tastiere) siano restituiti insieme al dispositivo.

Manutenzione e aggiornamenti:

- Effettuare gli aggiornamenti richiesti dal sistema operativo quando richiesto, per garantire la sicurezza e prestazioni ottimali.
- Mantenere pulito il dispositivo, utilizzando panni morbidi e asciutti, senza ricorrere a prodotti chimici aggressivi.
- Segnalare tempestivamente al referente del Team dell'Innovazione di plesso eventuali guasti, malfunzionamenti o anomalie riscontrate.

Gestione dei file e archiviazione:

- Lavorare preferibilmente in cloud, salvando i file su Google Drive.
- Non scaricare file nella memoria locale del dispositivo; se necessario per l'attività didattica, cancellarli immediatamente dopo l'utilizzo.
- Non modificare le impostazioni del dispositivo senza autorizzazione; in caso di particolari esigenze, rivolgersi al personale preposto (Animatore digitale, Team dell'Innovazione).

Configurazione e assegnazione:

- I nuovi dispositivi devono essere configurati esclusivamente con account scolastici istituzionali creati appositamente per la configurazione. In caso di nuovi acquisti affidare la procedura di configurazione al Team dell'Innovazione (Animatore digitale o referente del Team di plesso).
- È vietato configurare i dispositivi di proprietà della scuola con account personali, anche se scolastico.
- L'assegnazione dei pc ai docenti per l'uso in classe avviene su richiesta del docente secondo le modalità previste dal referente del Team dell'innovazione di plesso.
- I dispositivi scolastici assegnati ai docenti possono essere utilizzati solo da loro; per la tutela della privacy è vietato

farli utilizzare dagli alunni durante le lezioni.

- Per le attività digitali degli alunni devono essere utilizzati esclusivamente i dispositivi dedicati specificamente a loro (Chromebook o PC esplicitamente dedicati).

- Il docente è tenuto a conoscere le principali funzionalità dei dispositivi utilizzati in classe, così da garantirne l'uso corretto, prevenire danneggiamenti e gestire eventuali piccoli malfunzionamenti, anche dovuti a manomissioni degli studenti.

Custodia e trasporto:

- Prenotare le risorse digitali secondo le procedure del plesso.

- Il docente deve occuparsi personalmente del trasporto dei dispositivi dai luoghi di custodia alla classe e viceversa. In caso di necessità, può richiedere il supporto di un collaboratore scolastico; è in ogni caso vietato affidare tale compito agli alunni.

- Riporre i dispositivi negli armadi dedicati o nei carrelli, assicurandosi che siano correttamente sistemati negli slot del carrello mobile e collegati alla ricarica.

- Non lasciare i dispositivi incustoditi in aula o in altri spazi comuni.

Responsabilità e verifiche:

- Il docente ha il compito di supervisionare la consegna e il ritiro dei dispositivi agli alunni, verificandone lo stato prima e dopo l'utilizzo, assicurandosi che vengano riconsegnati integri e senza danni o modifiche alla configurazione iniziale.

- Il docente assegna i dispositivi agli alunni nel rispetto delle eventuali regole di distribuzione previste dal plesso di riferimento.

- Il docente deve assicurarsi che ogni alunno si sia disconnesso dal proprio account al termine della sessione di lavoro.

- In caso di danneggiamenti dei pc assegnati ai docenti o del pannello interattivo della propria classe, riconducibili alla mancata osservanza delle indicazioni del presente regolamento e delle buone pratiche d'utilizzo, la scuola può chiedere il risarcimento del danno al docente responsabile, qualora sia compromessa la funzionalità del dispositivo. Inoltre il docente è responsabile della supervisione e della corretta gestione dei dispositivi utilizzati dagli alunni durante le attività didattiche. In presenza di danni ai dispositivi utilizzati dagli alunni, derivanti da reiterata inosservanza del docente delle disposizioni del presente Regolamento e delle buone pratiche d'utilizzo, il Dirigente Scolastico potrà adottare provvedimenti secondo quanto previsto dal Regolamento d'Istituto e dalle normative vigenti.

- In caso di danneggiamento volontario o dovuto a scarsa cura da parte degli alunni, la scuola provvederà a sanzionare gli allievi secondo quanto disposto dal regolamento di disciplina dell'Istituto (sanzioni previste dal Regolamento di

disciplina, sezione Gruppo 3). Qualora il danno causi un malfunzionamento del dispositivo o l'impossibilità di utilizzo, la scuola può chiedere il risarcimento del danno ai genitori dell'allievo che lo ha procurato (sanzioni previste dal Regolamento di disciplina, sezione Gruppo 4).

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.

All'interno dell'Istituto Comprensivo Alighieri-Kennedy l'uso di dispositivi personali è consentito solo all'interno di attività didattiche strutturate e previa autorizzazione del docente e del Team Digitale, nel rispetto delle indicazioni ministeriali ("Dieci punti per l'uso dei dispositivi mobili a scuola").
L'Istituto ha scelto un approccio prudente e progressivo, limitando il BYOD a situazioni circostanziate — attività didattiche specifiche, alunni con bisogni speciali — al fine di garantire:

- un ambiente di apprendimento controllato, con accesso alle sole risorse indicate dal docente;
- la tutela della privacy degli studenti tramite l'utilizzo esclusivo dell'account istituzionale o, quando necessario, di alias pseudonimizzati;
- la riduzione dei rischi legati alla sicurezza delle reti e alla gestione dei dati.

Per tutte le attività BYOD, gli studenti devono:

- utilizzare il dispositivo esclusivamente per le attività previste;
- connettersi solo alla rete scolastica protetta;
- rispettare la Politica d'Uso Accettabile (PUA) e le indicazioni dei docenti.

Le famiglie sono informate sulle modalità di utilizzo dei dispositivi personali tramite il Patto di Corresponsabilità e le comunicazioni dedicate.
Il Regolamento BYOD di Istituto, attualmente in fase di revisione, sarà armonizzato con la presente ePolicy e pubblicato sul sito istituzionale al termine dei lavori del Team Digitale.

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/lle 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.

Nel nostro Istituto Comprensivo, le procedure di segnalazione si integrano con l'organizzazione interna già attiva per la prevenzione e il contrasto del bullismo e del cyberbullismo. In particolare:

- il Team Antibullismo, il Referente di Istituto e l'Animatore Digitale collaborano in modo coordinato per l'analisi preliminare delle segnalazioni che riguardano comportamenti online a rischio, assicurando un intervento tempestivo e proporzionato;
- tutte le segnalazioni provenienti da docenti, studenti, famiglie o personale ATA vengono prese in carico attraverso le procedure indicate negli allegati, garantendo riservatezza, rapidità di risposta e continuità nel monitoraggio;
- particolare attenzione è riservata ai casi che coinvolgono l'uso degli strumenti digitali dell'Istituto (Google Workspace, BYOD), per i quali si attiva un'analisi tecnica preliminare;
- la scuola mantiene un dialogo costante con i soggetti territoriali competenti (Forze dell'Ordine, servizi sociali, consultori, enti del Terzo Settore già partner di progetti d'Istituto), attivandoli solo quando il caso supera le possibilità di gestione interna;
- tutta la comunità scolastica è periodicamente informata sulle modalità di segnalazione attraverso incontri, circolari, materiali informativi e sezioni dedicate del sito web.

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 minorenne.

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

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

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

discriminare tra vittime, testimoni e/o autori.

Prevedere possibili incontri di mediazione tra i minori coinvolti vanno ponderati con la consapevolezza del loro stato emotivo, anche e in base agli elementi raccolti in merito del fatto/episodio avvenuto (elementi che si dovrebbero valutare di caso in caso). Importante è prevedere il coinvolgimento dei genitori sia della vittima che del bullo (ove possibile).

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

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

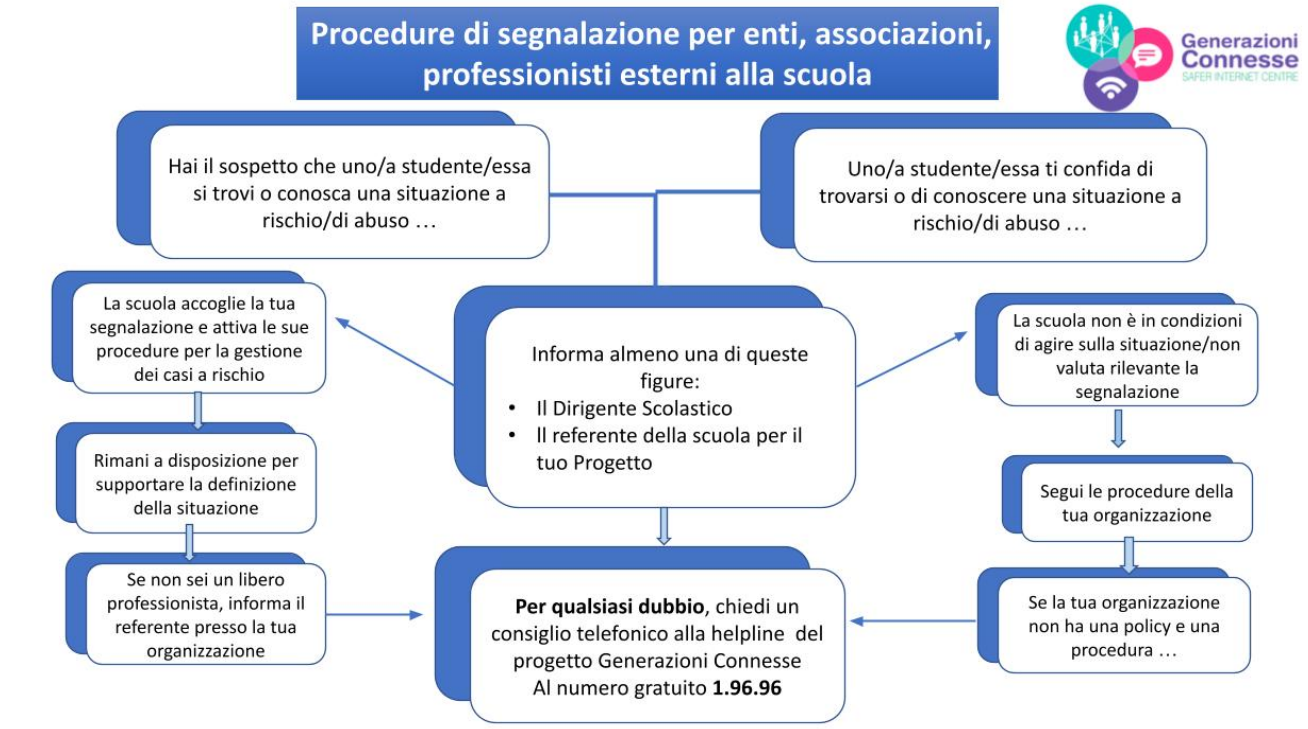
Strumenti a disposizione di studenti/esse

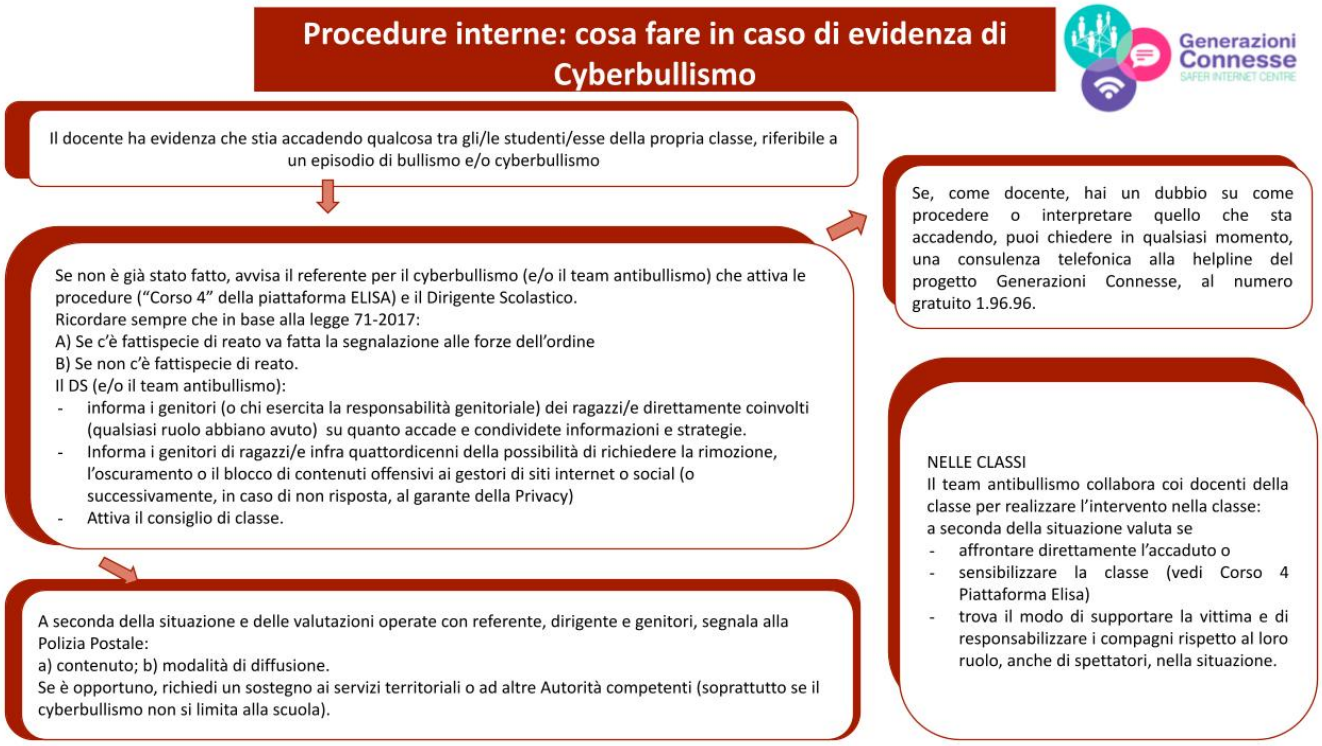
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

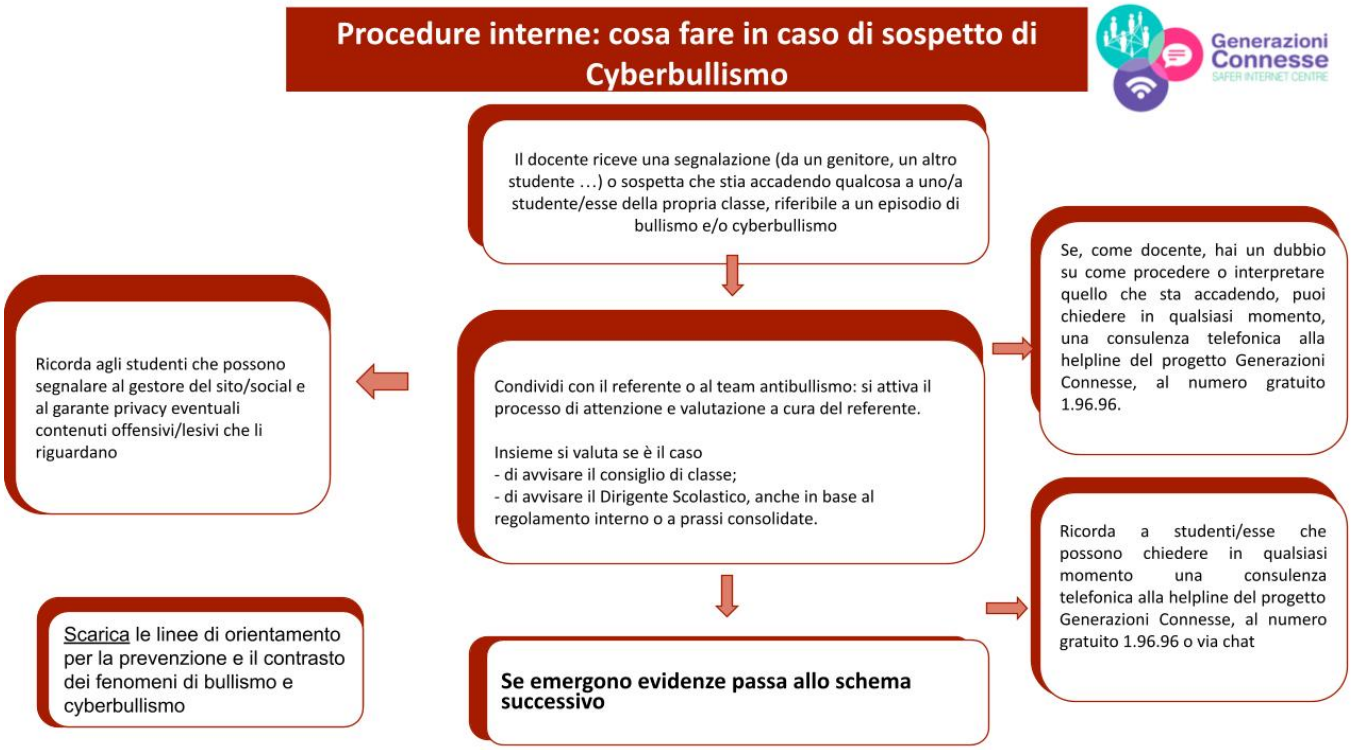
In particolare, sarebbe utile che la scuola attivi un sistema di segnalazione utile anche al monitoraggio dei fenomeni dal quale partire per integrare azioni didattiche preventive e giornate di sensibilizzazione, insieme agli Enti/Servizi presenti sul territorio di riferimento. Importante, altresì, immaginare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

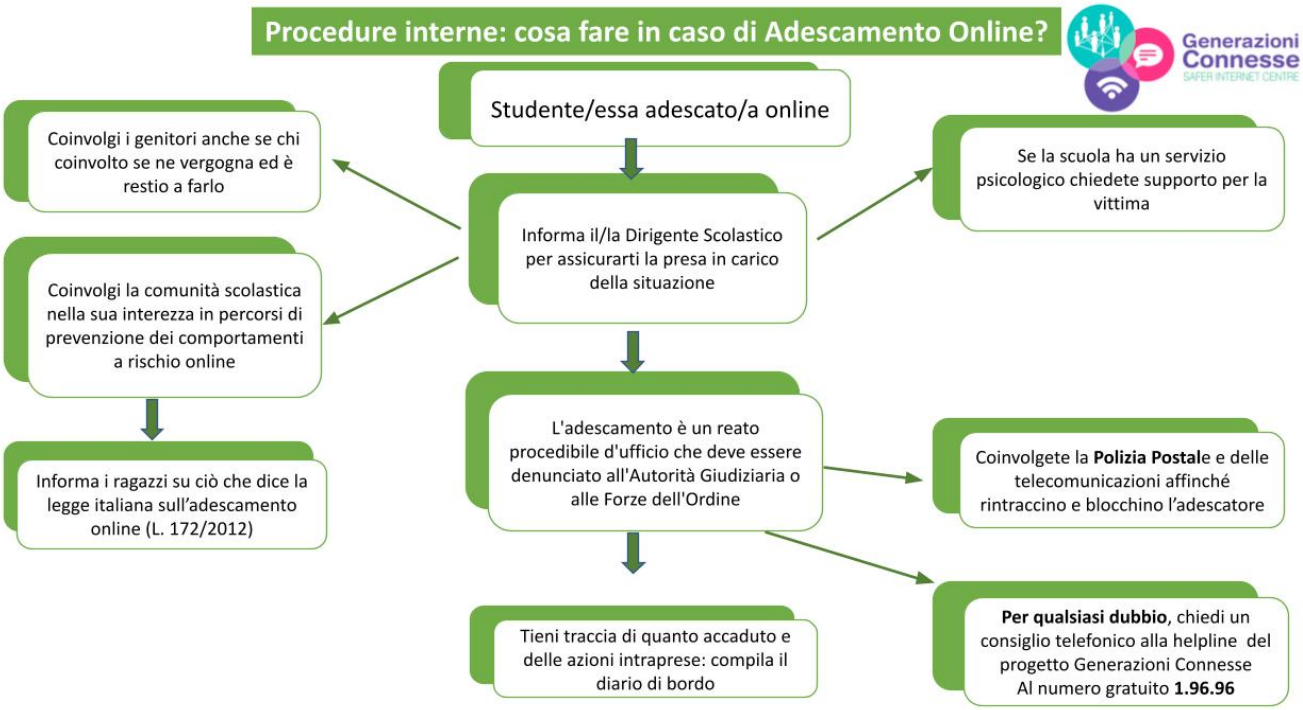
Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle Linee di Orientamento per la prevenzione e il contrasto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

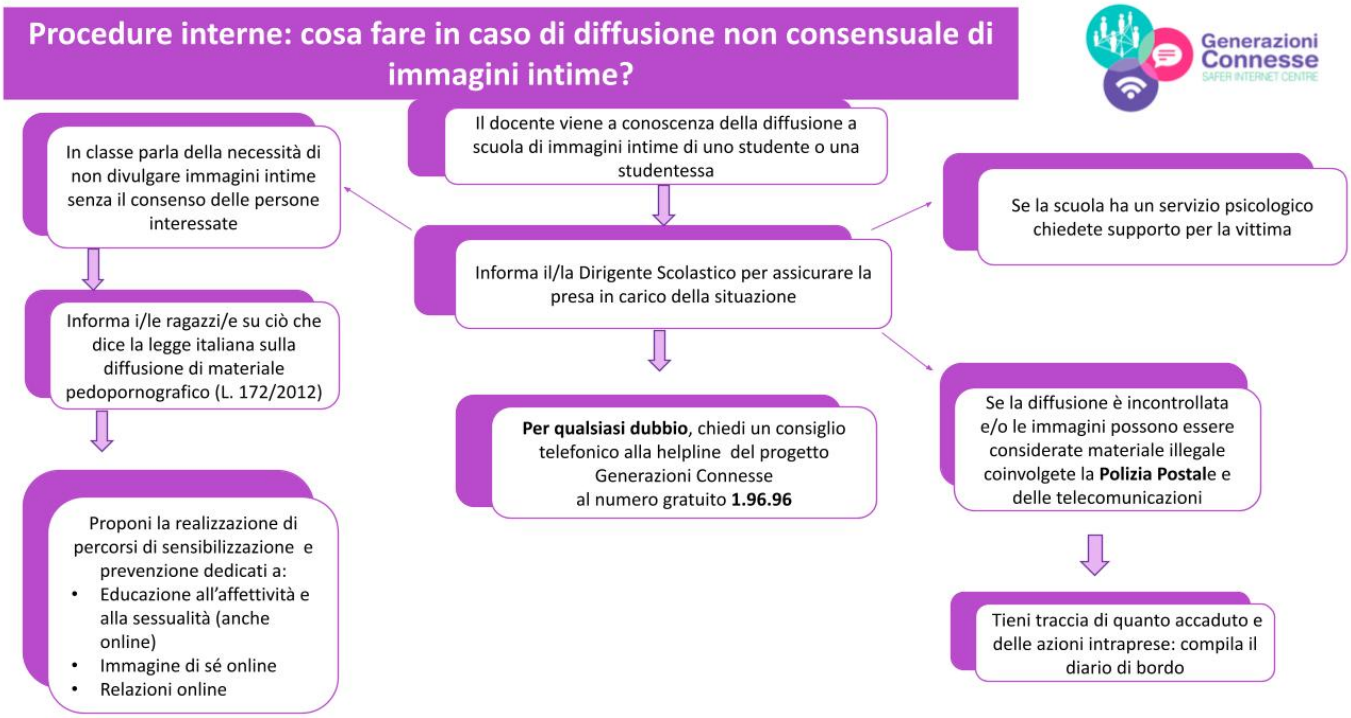
Procedure


Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola
Generazioni Connesse
Hai il sospetto che uno/a studente/essa si trovi o conosca una situazione a rischio/di abuso …
Uno/a studente/essa ti confida di trovarsi o di conoscere una situazione a rischio/di abuso …
La scuola accoglie la tua segnalazione e attiva le sue procedure per la gestione dei casi a rischio
Rimani a disposizione per supportare la definizione della situazione
Se non sei un libero professionista, informa il referente presso la tua organizzazione
Informa almeno una di queste figure:
• Il Dirigente Scolastico
• Il referente della scuola per il tuo Progetto
La scuola non è in condizioni di agire sulla situazione/non valuta rilevante la segnalazione
Segui le procedure della tua organizzazione
Se la tua organizzazione non ha una policy e una procedura …
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse Al numero gratuito 1.96.96


Procedure interne: cosa fare in caso di evidenza di Cyberbullismo
Generazioni Connesse
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 condividete 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.
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).
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.


Procedure interne: cosa fare in caso di sospetto di Cyberbullismo
Generazioni Connesse
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
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.
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.
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano
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
Scarica le linee di orientamento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo
Se emergono evidenze passa allo schema successivo


Procedure interne: cosa fare in caso di Adescamento Online?
Generazioni Connesse
Studente/essa adescato/a online
Coinvolgi i genitori anche se chi coinvolto se ne vergogna ed è restio a farlo
Se la scuola ha un servizio psicologico chiedete supporto per la vittima
Informa il/la Dirigente Scolastico per assicurarti la presa in carico della situazione
Coinvolgi la comunità scolastica nella sua interezza in percorsi di prevenzione dei comportamenti a rischio online
Informa i ragazzi su ciò che dice la legge italiana sull'adescamento online (L. 172/2012)
L'adescamento è un reato procedibile d'ufficio che deve essere denunciato all'Autorità Giudiziaria o alle Forze dell'Ordine
Coinvolgete la Polizia Postale e delle telecomunicazioni affinché rintraccino e blocchino l'adescatore
Tieni traccia di quanto accaduto e delle azioni intraprese: compila il diario di bordo
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse Al numero gratuito 1.96.96



Nel nostro Istituto Comprensivo, le procedure indicate nella sezione standard sono integrate da strumenti operativi e canali già attivi, pensati per agevolare una segnalazione tempestiva e chiara e garantire un'efficace presa in carico dei casi.

Strumenti di segnalazione attivi nell'Istituto

- Casella email dedicata aiutobullismo@alighierikennedy.it per le segnalazioni di bullismo e cyberbullismo, gestita dal Referente e dal Team antibullismo.
- Modulo di segnalazione interno, disponibile per docenti, studenti e famiglie, con procedure uniformi per comunicazioni in forma scritta.
- Sportello d'ascolto psicologico, potenziato annualmente, a disposizione degli studenti e delle famiglie per la prima presa in carico emotiva e per l'orientamento ai servizi territoriali.
- Altri sportelli di ascolto, quali ad esempio quello relativo alla gestione dei conflitti del progetto Sotto l'albero, attivo da due anni nel nostro istituto.

Figure interne coinvolte

- Dirigente scolastico, garante della procedura e dell'attivazione dei protocolli previsti.
- Referente bullismo e cyberbullismo, responsabile della valutazione preliminare delle segnalazioni e del coordinamento degli interventi.

- Animatore Digitale e Team Innovazione, coinvolti nelle situazioni che richiedono analisi tecnica o riferimenti alla sicurezza digitale.
- Consigli di Classe/Interclasse, chiamati a supportare la gestione educativa dei casi.

Collaborazioni territoriali

In base alla gravità e alla tipologia della segnalazione, il Team antibullismo collabora con:

- Polizia Locale – Nucleo di Prossimità,
- Forze dell'Ordine,
- ASL di competenza,
- Servizi Sociali del Comune,
- Associazioni ed enti specializzati già partner dell'Istituto in progetti di prevenzione.

Coinvolgimento delle famiglie

Le famiglie vengono coinvolte tempestivamente, nel rispetto delle procedure e della riservatezza, e ricevono indicazioni sui passi successivi, sul supporto psicologico disponibile e sui riferimenti utili per eventuali segnalazioni esterne.

Monitoraggio interno

Le segnalazioni raccolte – nel rispetto della tutela dei dati personali – confluiscono in un registro interno di monitoraggio, gestito dal Team antibullismo, che permette di:

- individuare tempestivamente eventuali ricorrenze o pattern di rischio,
- orientare interventi educativi mirati,
- programmare attività preventive nel PTOF e nel curricolo di Educazione Civica.