



Documento di ePolicy GIANCARLO VALLAURI

VIALE SALVO D'ACQUISTO 43 - 00049 - VELLETRI

Roma (RM) - Lazio

Data di approvazione: 17/02/2026 - 16:50

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 I.T.I.S. "G. Vallauri" punta a promuovere l'uso consapevole e critico delle tecnologie digitali (TIC) e di Internet da parte degli studenti e degli adulti coinvolti nella comunità educante e di far acquisire procedure e competenze "tecniche". Diffonde, altresì, l'applicazione di corrette norme comportamentali, quali prevenire ovvero rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso delle tecnologie digitali. Gli utenti, siano essi maggiorenni o minorenni, devono essere pienamente consapevoli dei rischi a cui si espongono, pertanto, in tale contesto, gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta da utilizzare a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose. La nuova Strategia Europea per un Internet migliore per i minori "Better Internet For Kids 2022-2030" garantisce che i minori siano protetti, rispettati e responsabilizzati on line in linea con i principi digitali europei: creare ambienti online più sicuri; promuovere contenuti per un uso positivo della rete; dare voce e promuovere l'Empowerment di ragazzi/e; contrastare la produzione e la diffusione di contenuti pedopornografici.

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

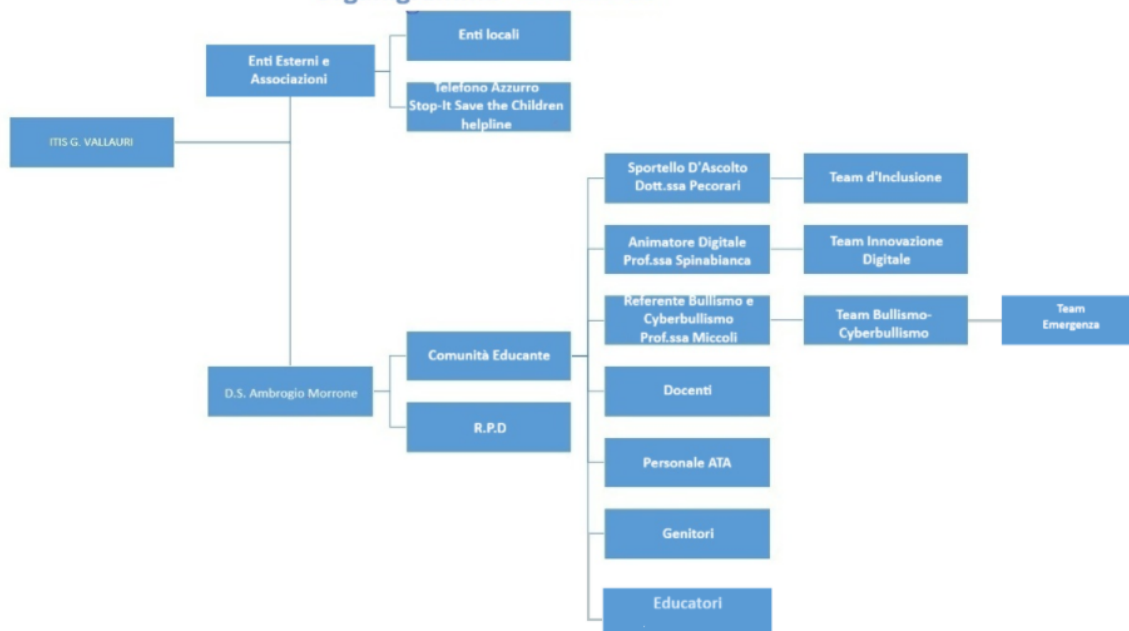
I Genitori, in continuità con l'Istituto scolastico, sono attori partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile degli strumenti personali (pc, smartphone, etc). Come parte della comunità educante sono tenuti a relazionarsi 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.

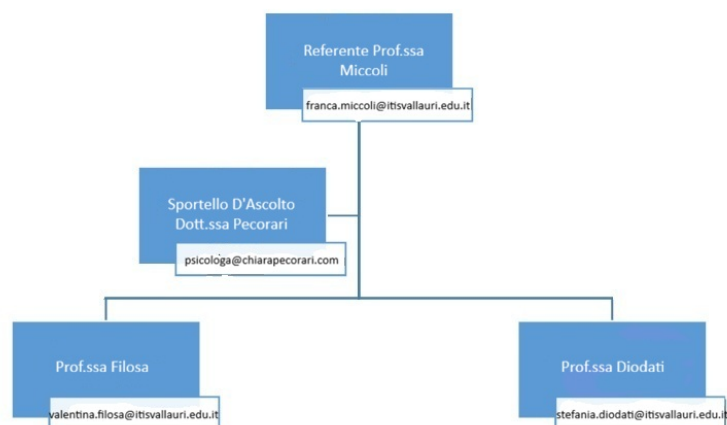
GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

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.

Istituto Tecnico Tecnologico e Liceo Scientifico Scienze Applicate
I.T.I.S Giancarlo Vallauri - Velletri
Cyberbullismo e E-safety
Organigramma - a.s.2025-26



Istituto Tecnico Tecnologico e Liceo Scientifico Scienze Applicate
I.T.I.S Giancarlo Vallauri - Velletri
Cyberbullismo e E-safety
Organigramma a.s.2025-26



Orario di ricevimento referente bullismo
martedì dalle ore 11:00 alle ore 12:00
venerdì dalle ore 10:00 alle ore 11:00

Orario di ricevimento sportello di ascolto
martedì dalle ore 08:30 alle ore 13:40
venerdì dalle ore 11:00 alle ore 13:40

1.3 Integrazione ePolicy nei documenti scolastici

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

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

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

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

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

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

Il presente documento va integrato con gli obiettivi e i contenuti dei seguenti documenti che disciplinano il funzionamento dell'istituto scolastico e specificano il contesto di un uso efficace e consapevole del digitale nella didattica:

- Piano Triennale dell'Offerta Formativa (PTOF);
- Regolamento interno d'Istituto;
- Patto di corresponsabilità educativa tra scuola e famiglia;
- Rapporto di Auto-Valutazione (R.A.V.);
- Regolamento per l'utilizzo dei laboratori.

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

1. il curriculum sulle competenze digitali per la comunità educante (il DigComp2.2);
2. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative;

3. Come comunicare e condividere l'ePolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

1. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative;

L'efficacia dell'ePolicy è direttamente proporzionale a livello di conoscenza e diffusione all'interno della comunità scolastica ivi comprese le famiglie. Il documento rappresenta il canale interno privilegiato per informare, responsabilizzare e collaborare sui temi della rete e delle tecnologie a scuola con l'intera comunità scolastica.

In tal senso, il documento è accompagnato da versioni, allegate e sintetiche, all'interno delle quali sono individuati gli elementi principali del documento; una versione è diretta agli studenti ed una è diretta alle famiglie con un linguaggio e una presentazione dei contenuti adeguata, flessibile e chiara. La versione sintetica rivolta agli studenti è inserita all'interno delle attività didattiche dell'educazione alla cittadinanza mentre la versione per le famiglie è consegnata nel corso dei colloqui scuola-famiglia.

Il documento è altresì pubblicato sul sito della scuola ed inserito nel Patto di corresponsabilità.

2. Come comunicare e condividere l'ePolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

La presenza dell'ePolicy nell'Istituto scolastico è garanzia, per il territorio, della presenza di un presidio informato, sensibile e attento sulla rete e le tecnologie in relazione con i più giovani.

In questo senso l'Istituto può rappresentare per le Istituzioni del territorio, le aziende, e le realtà del Terzo Settore un luogo di confronto privilegiato e di sperimentazione per tutti coloro che intendono costruire progetti di cittadinanza digitale rivolte ai più giovani.

A tal fine l'adozione dell'ePolicy è comunicata all'USR di riferimento e al Municipio (servizi istruzione e servizi sociali) attraverso gli allegati sintetici progettati che indicano gli elementi del documento e le prospettive per la comunità.

1) Condivisione e comunicazione della Policy al personale:

La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di Internet sarà discussa e deliberata negli organi collegiali maggiori e comunicata formalmente a tutto il personale con il documento di ePolicy. Tale documento, con gli eventuali aggiornamenti, sarà pubblicato sul sito istituzionale della scuola dopo l'approvazione da parte del Dirigente Scolastico.

2) Condividere e comunicare la politica di e-safety agli alunni:

- Gli studenti, in particolare ad inizio di ogni anno scolastico, saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione.
- Sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili (ad esempio l'utilizzo dei social media).
- Il percorso formativo proposto da Generazioni Connesse è inserito e valevole come credito scolastico per

gli studenti che decideranno di seguirlo.

3) Condividere e comunicare la politica di e-safety ai genitori:

L'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà attirata nelle news o in altre aree del sito web della scuola; sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet aggiornando il patto di corresponsabilità che le famiglie firmano all'atto dell'iscrizione e promuovendo eventuali incontri per i genitori all'utilizzo critico e consapevole degli studenti delle nuove tecnologie e dei social media.

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

La prima fase del cronoprogramma ha come orizzonte il primo anno dalla stesura del documento di ePolicy; in questo periodo la scuola si impegna a diffondere il documento all'interno della comunità scolastica e, inoltre, intraprende tutte quelle azioni che integrano dal punto di vista amministrativo il documento dell'ePolicy all'interno degli altri documenti della scuola.

Dopo la diffusione dell'ePolicy svolta nel primo anno del cronoprogramma, si apre la seconda fase che diventa condivisione dei contenuti dell'ePolicy con la famiglia e con gli studenti promuovendo una loro partecipazione attiva su questi temi.

Cronoprogramma dei Piani di Azione scolastica per la diffusione del documento:

- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si

- evidenzia la necessità di regolamentare azioni e comportamenti;
- Organizzare eventi di presentazione e conoscenza dell'ePolicy rivolto ai docenti;
- Integrazione del documento dell'ePolicy all'interno dei documenti amministrativi.

Cronoprogramma seconda fase dalla definizione dell'ePolicy:

- Organizzare eventi di presentazione e conoscenza dell'ePolicy rivolto agli studenti;
- Organizzare eventi di presentazione e conoscenza dell'ePolicy rivolto ai genitori;
- Attività programmate al fine di aumentare il coinvolgimento e le informazioni per l'utilizzo corretto delle tecnologie informatiche di tutta la comunità educante.

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

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

L'Istituto cercherà di divulgare a tutta la comunità educante le risorse che Generazioni Connesse propone per il mondo della scuola, delle famiglie e degli studenti. Le risorse possono essere utilizzate per condividere l'ePolicy e le scelte definite dalla scuola e per promuovere una Cittadinanza Digitale attiva all'interno dell'intera comunità scolastica. Il progetto Generazione Connesse prevede, a supporto del lavoro dell'ePolicy, un nuovo kit Didattico che contiene materiali per le lezioni e per il proprio aggiornamento. Può essere usato nella sua interezza oppure selezionato sulla base delle scelte discrezionali del docente.

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.

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme studenti e studentesse verso un uso responsabile e critico delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto sostiene un'informazione diffusa alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento di tutti i documenti scolastici coinvolti e preposti. Il Team Regolamenti si occuperà di aggiornare il Patto di Corresponsabilità educativa tra scuola e famiglia con il documento di e-Policy. Inoltre, la scuola darà ampia diffusione, anche tramite pubblicazione sul sito, del presente documento di ePolicy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e favorire un'attiva collaborazione sui temi della prevenzione dei rischi connessi ad un uso inappropriato del 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.

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. Il piano di studi, programmato nei tre indirizzi dell'I.T.I.S. "G. Vallauri", già dal biennio, prevede due ore di Tecnologie Informatiche, nelle quali si sviluppino competenze di base comuni, competenze trasversali e competenze specifiche per ogni indirizzo (liceo scientifico delle scienze applicate; istituto tecnico ad indirizzo elettronico ed informatico). Il Curriculum Digitale ha lo scopo di programmare ed implementare percorsi didattici di facile replicabilità, uso e applicazione che siano "innovativi, strutturati, aperti e in grado di coinvolgere la comunità scolastica allargata" sul tema del digitale e delle tecnologie digitali. In questo modo, si può rendere quanto più possibile integrato e consapevole l'utilizzo dei dispositivi digitali così come anche esplicitato nel DigComp Edu secondo cui lo sviluppo delle competenze digitali degli studenti significa aiutarli "ad utilizzare in modo creativo e responsabile le tecnologie digitali per attività riguardanti l'informazione, la comunicazione, la creazione di contenuti, il benessere personale e la risoluzione dei problemi". Tutte le Istituzioni scolastiche, attraverso il curriculum digitale, sono tenute a promuovere in ciascun insegnamento le competenze digitali degli studenti e delle studentesse tramite attività, lezioni specifiche, laboratori e workshop (sia in presenza sia a distanza) tesi a massimizzare il protagonismo di tutta la comunità scolastica (ivi inclusi i docenti, dell'animatore digitale e di tutti i professionisti che, nella scuola, svolgono funzioni formative ed educative) e la comunità di riferimento ("i percorsi potranno prevedere il coinvolgimento di partner esterni al mondo scolastico nella produzione dei materiali didattici - centri di ricerca, università, istituzioni locali, associazioni, imprese e dovranno incoraggiare, attraverso le loro attività, il rapporto con il territorio" Allegato 1 - Curricoli Digitali). In questi anni l'Istituto ha intrapreso un progressivo percorso di innovazione sia in termini di pratiche didattiche e relativa formazione del personale, sia in termini di realizzazione di spazi di apprendimento maggiormente rispondenti agli attuali bisogni formativi degli studenti. Questa tendenza si inserisce pienamente nella prospettiva di valorizzazione dei diversi stili di apprendimento e di personalizzazione dell'intervento formativo. In linea con la propria identità di Istituto che avvalorava l'applicazione dei saperi e con quanto previsto nella Missione 4 "Istruzione e Ricerca" del PNRR, i principali elementi di innovazione hanno riguardato i seguenti ambiti:

- corsi di formazione finalizzati al miglioramento delle competenze del corpo docente in servizio, a partire dal suo reclutamento (nuove metodologie di insegnamento mediante l'utilizzo delle nuove tecnologie, competenze linguistiche e digitali, etc.;

- integrazione e rinnovo degli strumenti digitali (PC, laptop, lavagne interattive multimediali, Smart-TV, Digital Board,

etc.) presenti nelle aule;

- rinnovo e/o realizzazione ex-novo di ambienti laboratoriali all'avanguardia, anche attraverso l'acquisizione di nuove strumentazioni.

L'istituto percorre lo sviluppo delle seguenti competenze:

1. Competenza 1: Alfabetizzazione informatica

- Descrizione: Acquisizione di abilità fondamentali nell'uso di dispositivi digitali e software applicativi.
- Competenze:
 - Utilizzo dei principali sistemi operativi.
 - Gestione file e cartelle, creazione di documenti digitali.
 - Utilizzo di browser per la navigazione web sicura e ricerca di informazioni online.
 - Abilità nell'utilizzo di software di produttività e collaborazione.

2. Competenza 2: Comunicazione digitale

- Descrizione: Capacità di utilizzare strumenti digitali per la comunicazione e collaborazione.
- Competenze:
 - Utilizzo di e-mail e piattaforme di messaggistica.
 - Gestione di comunicazioni via videochiamata.
 - Creazione di contenuti per la comunicazione digitale.
 - Collaborazione in ambienti virtuali.

3. Competenza 3: Produzione di contenuti digitali

- Descrizione: Abilità nella creazione e modifica di contenuti digitali.
- Competenze:
 - Creazione e modifica di documenti di testo, fogli di calcolo e presentazioni.
 - Utilizzo di software di grafica e editing video.
 - Progettazione di siti web e applicazioni (HTML, CSS, JavaScript).
 - Utilizzo di piattaforme per la gestione di contenuti multimediali.

4. Competenza 4: Sicurezza digitale

- Descrizione: Conoscenze riguardanti la protezione dei dati, la privacy online e la sicurezza delle informazioni.
- Competenze:
 - Gestione delle password e l'utilizzo di strumenti di autenticazione sicura.
 - Conoscenza di pratiche sicure online per evitare phishing, malware e altre minacce.
 - Comprensione dei concetti di privacy e protezione dei dati personali (GDPR).
 - Gestione sicura dei dispositivi digitali (antivirus, firewall, aggiornamenti).

5. Competenza 5: Risoluzione di problemi tecnologici

- Descrizione: Capacità di identificare e risolvere problemi tecnici utilizzando strumenti digitali.
- Competenze:
 - Risoluzione di problemi informatici di base (malfunzionamenti hardware, software).
 - Diagnosi e riparazione di circuiti elettronici e dispositivi (per l'indirizzo elettronico).
 - Sviluppo di soluzioni software per risolvere problemi di automazione e gestione (per l'indirizzo informatico).
 - Utilizzo di strumenti di diagnostica per l'indirizzo elettronico.

6. Competenza 6: Programmazione e sviluppo

- Descrizione: Abilità nello sviluppo di software e applicazioni digitali.
- Competenze:
 - Programmazione in linguaggi come Python, C++, Java.
 - Sviluppo di applicazioni web (front-end, back-end).
 - Utilizzo di ambienti di sviluppo integrati (IDE) per la scrittura di codice.
 - Conoscenza dei principi di base dell'intelligenza artificiale e della machine learning (per l'indirizzo informatico).

7. Competenza 7: Innovazione e creatività digitale

- Descrizione: Sviluppo di soluzioni innovative tramite l'uso di tecnologie digitali.
- Competenze:
 - Creazione di prototipi digitali (per l'indirizzo elettronico e informatico).
 - Utilizzo di software di modellazione 3D e simulazioni (per elettronica e scienze applicate).
 - Sviluppo di progetti innovativi di automazione e robotica (per l'indirizzo elettronico).
 - Progettazione e sperimentazione con tecnologie emergenti (IoT, AI).

Moduli Aggiuntivi per Ogni Indirizzo

Indirizzo Informatico

- Competenze Avanzate: Conoscenza avanzata di reti e sicurezza informatica, gestione di database, sviluppo di software complessi.
- Progetti Rilevanti: Creazione di applicazioni web e mobile, progettazione di database, amministrazione di server.

Indirizzo Elettronico

- Competenze Avanzate: Progettazione e manutenzione di circuiti elettronici, utilizzo di strumenti di misurazione elettronica (oscilloscopi, multimetri).
- Progetti Rilevanti: Creazione di dispositivi elettronici, sistemi di automazione e controllo.

Liceo Scientifico opzione Scienze Applicate

- Competenze Avanzate: Analisi dei dati scientifici con strumenti digitali, modellazione e simulazione di fenomeni fisici e biologici.
- Progetti Rilevanti: Progetti di ricerca scientifica, analisi di dati complessi tramite software di statistica e simulazione.

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.

Strumento fondamentale per poter sensibilizzare e prevenire è il kit didattico.

Il Kit Didattico utilizza la metodologia EAS - Episodi di apprendimento situato - sviluppata dal CREMIT in grado di offrire al docente un quadro metodologico efficace ed operativo per costruire una lezione che comprenda al suo interno le diverse dimensioni utili all'apprendimento: *problem setting, learning by doing e learning by reflecting*. Le schede didattiche del kit sono, quindi, proposte attraverso la prospettiva metodologica EAS ed in questo modo il docente è guidato nelle diverse fasi di sviluppo della lezione a partire da uno stimolo iniziale (es. un video) un lavoro di gruppo che "produce" un artefatto e una successiva riflessione della classe.

Il Kit Didattico è disegnato sul framework europeo di riferimento per le competenze digitali DigComp 2.2 ed in questo modo il docente, nello svolgimento della singola lezione, è in grado di connettere l'attività con il cv verticale del proprio Istituto e con le indicazioni sull'educazione civica digitale che utilizzano lo stesso riferimento.

Il Kit Didattico propone anche contenuti dedicati ai docenti di sostegno progettati sulla base degli indicatori ICF (classificazione internazionale del funzionamento, della disabilità e della salute è un sistema di classificazione della disabilità sviluppata dall'Organizzazione mondiale della Sanità) e collegando questi ultimi agli indicatori di competenza di ciascuna attività. In questo modo il docente di sostegno può realizzare le attività personalizzandole sull'allievo e proponendo strategie di apprendimento funzionali anche alla partecipazione, con la classe, alle attività.

Il KIT didattico è strutturato nelle 5 aree del syllabo dell'Educazione Civica digitale (Educare ai media, Internet e il cambiamento in corso, Creatività e cultura digitale, Quantificazione e computazione, Educazione all'informazione).

È composto di 40 pillole teoriche e 32 schede didattiche che affrontano tematiche come il cyberbullismo, il sexting, la web reputation e molte altre.

Le schede didattiche si basano sul DigComp 2.2, fornendo ai docenti i riferimenti utili a individuare le dimensioni della competenza digitale che si vuole sviluppare e il livello per poter scegliere attività calibrate al proprio gruppo classe.

Le schede didattiche sono corredate dei riferimenti per i docenti di sostegno per adattare le attività a specifiche esigenze.

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.

La protezione dei dati personali delle persone fisiche costituisce un diritto fondamentale.

Le principali normative di riferimento sono il Regolamento Generale sulla Protezione dei Dati 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati) noto anche come GDPR (General Data Protection Regulation), e il Dlgs 196/2003 conosciuto come Codice della Privacy. Quest'ultimo è stato profondamente modificato e integrato dal D.Lgs. 101/2018 per adeguarsi al GDPR.

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. Pertanto, anche le scuole oggi hanno l'obbligo di adeguarsi al cosiddetto GDPR e al D.Lgs. 10 agosto 2018, n. 101.

Difatti, 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) che ha una conoscenza approfondita della normativa privacy; funge da punto di contatto tra la scuola e il Garante Privacy, organizza attività formative e di aggiornamento del personale.

I principali obblighi in materia di protezione dei dati personali del DPO consistono nell'informare e fornire consulenza all'istituto scolastico ed ai suoi dipendenti in merito agli adempimenti privacy.

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il "corretto trattamento dei dati personali" a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni.

Il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza. Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi.

Va specificato, altresì, che la scuola non è tenuta a richiedere il consenso alle famiglie laddove il trattamento dei dati personali venga effettuato per perseguire delle finalità di natura istituzionale, in quanto ciò è previsto dalla legge. Tuttavia, il consenso privacy diventa necessario laddove la scuola intenda effettuare un

trattamento di dati personali finalizzato ad attività che non rientrano tra quelle istituzionali o didattiche, come ad esempio, l'organizzazione di corsi di musica, utilizzo di foto e video sui social della scuola, di corsi teatrali o comunque attività che non rientrano in quello che è il curriculum scolastico.

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.

Il diritto di accesso a Internet è presente nell'ordinamento italiano ed europeo e la scuola viene intesa come il luogo dove tale diritto è garantito. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola". Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola. Ogni Istituto scolastico è tenuto ad adottare la P.U.A. (Politica d'Uso Accettabile), ovvero un documento che detta regole precise riguardanti l'utilizzo della rete a scuola e a casa da parte di studenti e di tutto il personale anche in base a quanto previsto dal decalogo ministeriale per l'uso dei dispositivi mobili a scuola. L'utilizzo dei dispositivi informatici in dotazione all'istituto, nello specifico, deve avvenire in maniera responsabile ed avendo cura sia degli apparati fisici che dell'integrità dei software in essi installati. Sulla base di tali presupposti e per motivi di sicurezza, agli utenti è vietato:

- utilizzare i dispositivi per finalità personali o comunque non correlati con attività didattiche o di studio;
- collegare dispositivi esterni (memorie USB, hard disk, ecc.);
- installare e disinstallare i programmi o modificarne le impostazioni;
- copiare, caricare o scaricare musica, film, programmi e qualsiasi altro materiale non legato alla didattica o vincolato da copyright o comunque in conflitto con le norme dei codici civile e penale riguardanti il diritto d'autore, la privacy, la divulgazione di materiale offensivo, pedo-pornografico etc. Nel caso in cui i dispositivi in dotazione all'istituto abbiano accesso alla rete WiFi, sarà necessario dotarli di credenziali per l'accesso alla rete. Tali credenziali devono essere gestite con la massima cautela e riservatezza. L'accesso alle piattaforme didattiche dell'istituto deve essere consentito esclusivamente previa autenticazione

informatica. A ciascun utente devono essere fornite credenziali univoche che devono essere custodite con la dovuta diligenza. L'accesso al registro elettronico viene abilitato per docenti, genitori e studenti tramite credenziali di accesso da custodire con la dovuta diligenza. Il registro elettronico deve essere utilizzato esclusivamente per le finalità istituzionali predeterminate dall'istituto (es. assenze, caricamento e lettura voti, comunicazioni, avvisi, ecc.).

- Responsabilità

È fondamentale che gli utenti siano pienamente consapevoli dei rischi a cui si espongono durante l'utilizzo dei dispositivi dell'istituto. I docenti sono responsabili dell'utilizzo dei dispositivi informatici e hanno l'obbligo di sorvegliare e responsabilizzare gli studenti e le studentesse rispetto ad un uso consapevole e sicuro. Gli utenti non devono lasciare incustoditi i dispositivi informatici e devono provvedere alla disconnessione del proprio account al termine dell'utilizzo. Attualmente, nel nostro Istituto, I.T.I.S. "G. Vallauri" l'accesso ad Internet è possibile in tutte le aule, dotate di Lavagna Interattiva Multimediale, di Smart TV o di Digital Board, con relativo computer portatile contenuto in un cassetto ben custodito. Per gli insegnanti, inoltre, l'accesso ad Internet è possibile anche in due postazioni a loro riservate nella sala docenti, i quali hanno piena autonomia nel collegamento ai siti web in tali postazioni. Per gli studenti l'accesso ad Internet è consentito per la didattica nei laboratori presenti a scuola per le materie tecniche d'indirizzo (informatica, elettronica, sistemi informatici ed elettronici, robotica e aula multimediale). Nelle aule e negli stessi laboratori sono attivi filtri per la navigazione sicura, tramite gestione di blacklist ed è prevista l'attivazione di software per la gestione e il controllo delle postazioni.

L'Animatore digitale definisce le impostazioni, nonché i responsabili di laboratorio e i tecnici, mentre ogni docente è tenuto a segnalare eventuali malfunzionamenti e/o disservizi. Inoltre, sia gli studenti che i docenti hanno un account Gmail istituzionale controllato dalla scuola, utilizzabile per la didattica. Gli indirizzi di posta elettronica degli allievi sono sottoposti a blocco rispetto alla ricezione e all'invio di mail da soggetti esterni all'istituto. I docenti comunicano con gli alunni anche attraverso la mail istituzionale, la classroom dedicata alla propria disciplina e tramite il registro elettronico.

L'Animatore digitale gestisce la Suite di Google dall'a.s. 2025/2026 unitamente al Dirigente scolastico, i quali provvederanno alla creazione di un altro account per i docenti consentendo l'accesso riservato per questi ultimi finalizzato alla presa visione delle comunicazioni interne, mentre le comunicazioni generali verranno pubblicate regolarmente sul sito della scuola I.T.I.S. "G. Vallauri".

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.

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/le studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando

il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

Risulta 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.

Per quanto riguarda la gestione degli strumenti personali (cellulari, tablet, ecc.) per gli studenti: in ottemperanza a quanto disposto dal Ministero dell'Istruzione e del Merito con la Circolare n. 3392 del 16 giugno 2025, a partire dall'anno scolastico 2025/2026 è esteso a tutte le scuole secondarie di secondo grado il divieto di utilizzo degli Smartphone, inclusi i momenti di lezione e di pausa. Pertanto, non è consentito l'uso di strumenti elettronici personali da parte della componente studentesca. Sono autorizzati all'utilizzo di tablet, cellulari (senza connessione Internet), gli alunni con DSA e con L. 104/92, se previsto dal PDP e dal PEI. Tutti gli studenti, inoltre, saranno autorizzati all'utilizzo dei computer portatili personali durante le ore di laboratorio delle materie tecniche (ad esempio, informatica) e si impegnano a tenere custoditi i telefoni cellulari nello zaino. In caso di urgenza per comunicazioni tra gli studenti e le famiglie, su autorizzazione dei docenti e sotto il diretto controllo dei collaboratori scolastici, i primi possono comunicare con le famiglie tramite gli apparecchi telefonici della scuola.

Invece, per quanto concerne la gestione degli strumenti personali (cellulari, tablet, ecc.) per i docenti, durante le ore di servizio non è consentito l'utilizzo del cellulare, mentre è consentito l'uso di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili e attività funzionali all'insegnamento.

mento di ePolicy - GIANCARLO VALLAURI - 11/01/2025 - 16:07 Pagina: 21/30

Cap 4 - Segnalazione e gestione dei casi

4.1 - Cosa Segnalare

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire). Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Queste, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola.

Nelle procedure sono indicate le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso, nonché le modalità di coinvolgimento del Dirigente Scolastico e del Referente per il contrasto al bullismo e al cyberbullismo. Inoltre, la scuola individua le figure che costituiranno un team preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica. La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

A seguire, le problematiche a cui fanno riferimento le procedure allegate:

Cyberbullismo: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/le studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).

Adescamento online: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

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.

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. Esse, 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. La scuola, difatti, si avvale di un team specializzato che include il Dirigente scolastico, la Referente per il contrasto del bullismo e del cyberbullismo, i servizi e gli enti del territorio.

Questi ultimi vengono coinvolti nel momento in cui la segnalazione fa riferimento a un caso di particolare gravità.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica.

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

La condivisione avverrà attraverso assemblee scolastiche, collegio docenti, eventuali incontri mirati che coinvolgano i genitori, gli studenti, le studentesse e il personale della scuola, attraverso news nel sito della scuola e/o circolari specifiche. L'obiettivo è che tutta la comunità scolastica sia informata di queste procedure che identificano quali possano essere i "casi" da segnalare, laddove per "casi" si intendono tutti quei comportamenti online a rischio di studenti e studentesse, ovvero:

Cyberbullismo: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica.

Quindi, bisogna verificare se il comportamento sia posto in essere alla presenza di un pubblico, tra coetanei, in modo ripetuto, con intenzionalità, al cospetto di una disparità di forze e potere tra i soggetti coinvolti e l'isolamento della vittima. È necessario, inoltre, capire il grado di disagio vissuto dallo studente o dalla studentessa, difatti, in caso di particolari gravità, si possono coinvolgere servizi esterni deputati ad offrire un supporto psicologico e di mediazione adatto al caso di specie considerato. L'attuale normativa mira, infatti, a proteggere i minori contro il cyberbullismo con misure educative e rieducative.

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 danneggiata. Inoltre, è importante non sostituirsi al minore e/o all'adolescente, evitando, quindi, di rispondere all'adescatore al suo posto. È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono.

La legge n. 172/2012, ispirata al principio generale di protezione dei diritti del minore, ha introdotto la possibilità per il minorenne coinvolto come vittima o nella qualità di testimone in alcune tipologie di reati, tra cui il "grooming", di essere ascoltato in sede di raccolta di informazioni durante le indagini preliminari con l'ausilio di una persona esperta in psicologia o psichiatria infantile, nominato dal Pubblico Ministero.

GROOMING: trattasi di un adescamento on line tramite chat e social network in cui un cyber predatore individua una giovane vittima, instaura con lei dapprima una relazione dapprima amicale poi confidenziale ed intima al fine di sfruttarla per fini sessuali. È un lento processo interattivo attraverso cui il cyber predatore si "prende" cura del mondo psicologico della vittima.

Sexting: scambio di contenuti sessualmente espliciti viene considerato alla stregua di un atto sessuale e richiede il consenso di tutte le parti coinvolte. Questo deve avvenire all'interno di una relazione consensuale con particolare attenzione all'età e alla capacità di autodeterminazione dei minori.

Pertanto, la divulgazione di tali materiali, ovvero immagini e/o video, senza consenso, soprattutto, se riguardano minori può costituire un reato indipendentemente dall'età del minore coinvolto. In tal caso, è opportuno adottare sistemi di segnalazione direttamente alla piattaforma con l'obiettivo primario di tutelare il minore e ottenere la rimozione o il blocco del materiale diffuso in rete lesivo.

In tal caso, 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 ventiquattro 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.

Per farlo bisogna compilare il modello che si trova sul sito www.garanteprivacy.it

I servizi esterni o enti del territorio che possono offrire supporto in caso di comportamenti online a rischio sono: l'Helpline del Telefono Azzurro, una linea telefonica gratuita attiva 24 ore su 24 per tutto l'anno alla quale rispondono operatori esperti che offrono consulenza psicopedagogica non solo ai minori, ma anche adulti, a docenti o persone che ne richiedono aiuto.

Questa linea è raggiungibile anche attraverso una chat accessibile sul sito del telefono azzurro. Esistono oltre all'Helpline anche altri due strumenti di segnalazione di materiale pedopornografico online.

Questi servizi di segnalazione esterni sono "click e segnala di telefono azzurro", "Stop it di Save the Children", che servono appunto per segnalare contenuti pedopornografici online attraverso la compilazione di un form presente sui diversi siti.

Entrambi i servizi provvederanno alla segnalazione di questo materiale e alla condivisione con il Centro Nazionale per il Contrasto della Pedopornografia Internet, il quale provvederà all'analisi di questo punto materiale ed eventualmente in caso necessario alla segnalazione alle realtà del territorio.

Segnalare la presenza di materiale pedopornografico online.

Può capitare che uno studente manifesti un'insofferenza nei confronti di un compagno o, al contrario, che un altro si senta escluso o emarginato dai coetanei. In alcuni casi sono gli studenti stessi a rivolgersi ai docenti in cerca di aiuto, anche quando i fatti siano accaduti fuori dall'ambiente e dall'orario scolastico.

La diffusione capillare dei social network tra gli adolescenti li espone sempre più spesso al rischio di inviare o condividere senza alcuna protezione materiali personali o riservati. Discutendo in classe dei rischi del web e confrontandosi sulle esperienze personali o dei propri coetanei, emergono, spesso, fatti che "allarmano" l'insegnante. Tuttavia, mentre quest'ultimo ha la possibilità, anzi il dovere, di intervenire sui dispositivi digitali in uso a scuola, non può intervenire direttamente sui telefoni cellulari degli allievi senza un'esplicita autorizzazione delle famiglie.

Tra i contenuti andranno opportunamente segnalati:

dati sensibili o riservati (foto, immagini, video personali, informazioni private proprie o di amici; l'indirizzo di casa o il telefono, ecc.);

contenuti che possano considerarsi in qualche modo lesivi dell'immagine altrui (commenti offensivi, minacce, osservazioni diffamatorie o discriminatorie, foto o video denigratori, videogiochi che contengano un'istigazione alla violenza, ecc.);

contenuti riconducibili alla sfera sessuale: messaggi, immagini o video a sfondo sessuale, come foto di nudo o semi-nudo, ecc.

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.

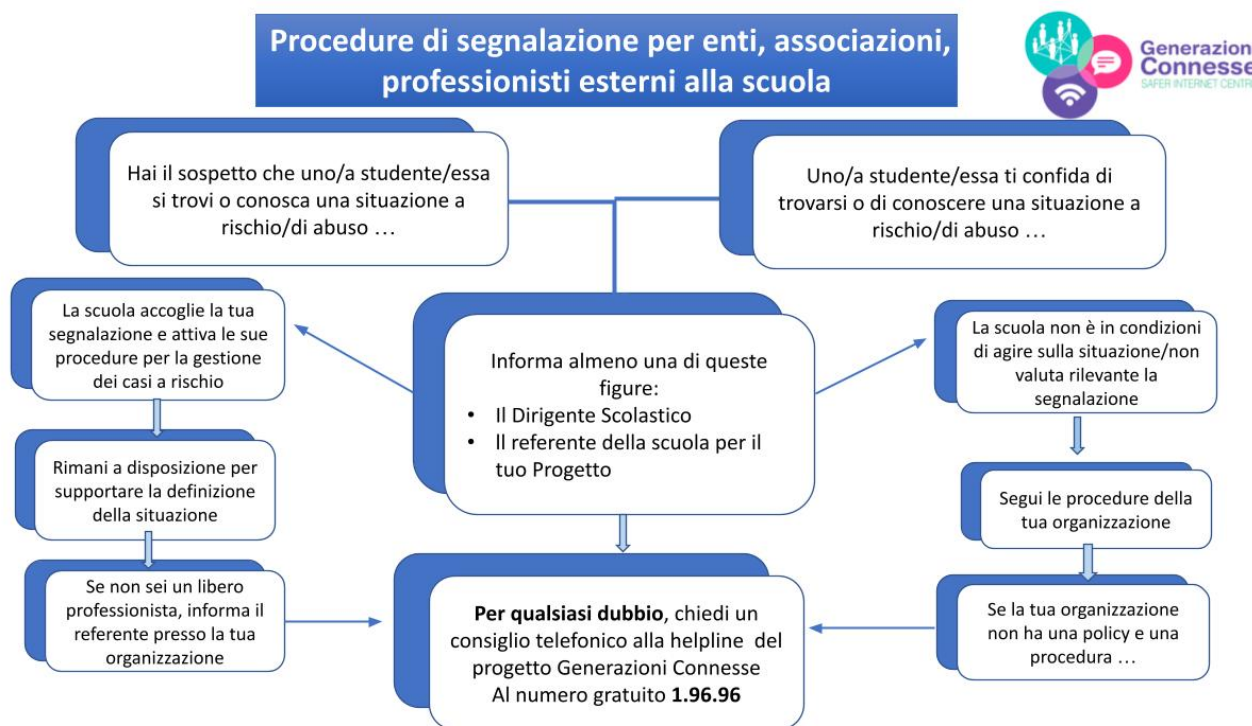
Strumenti a disposizione di studenti/esse

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.

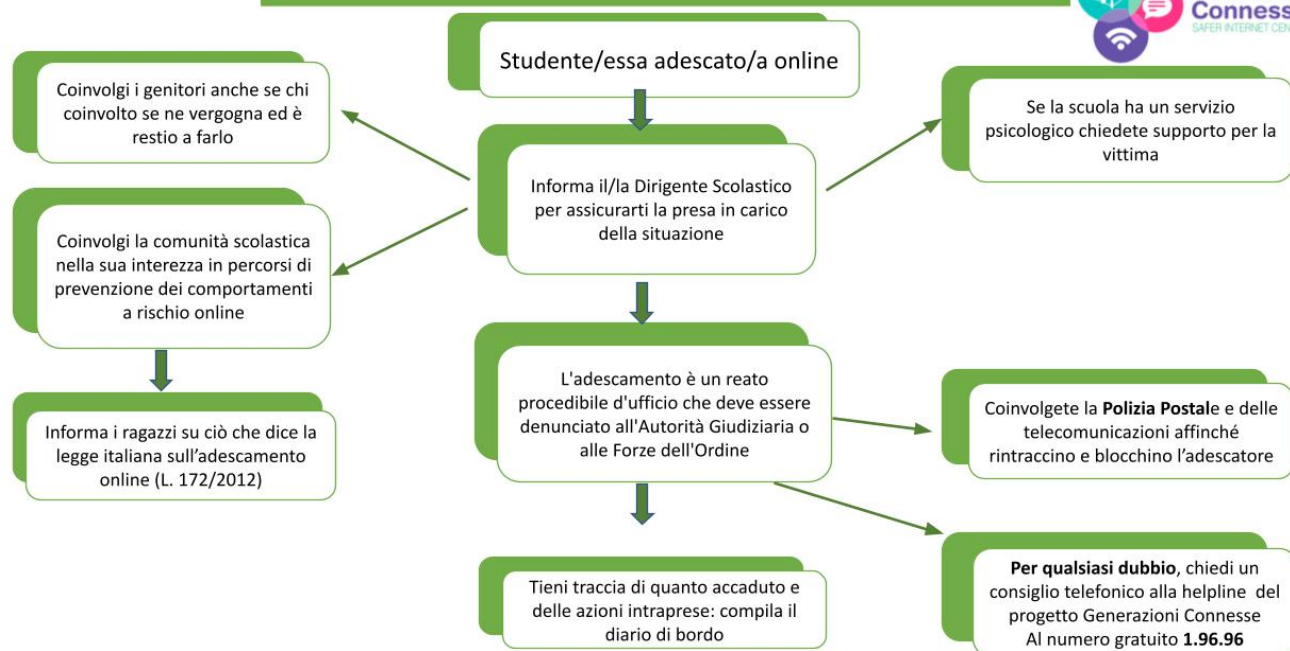
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

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

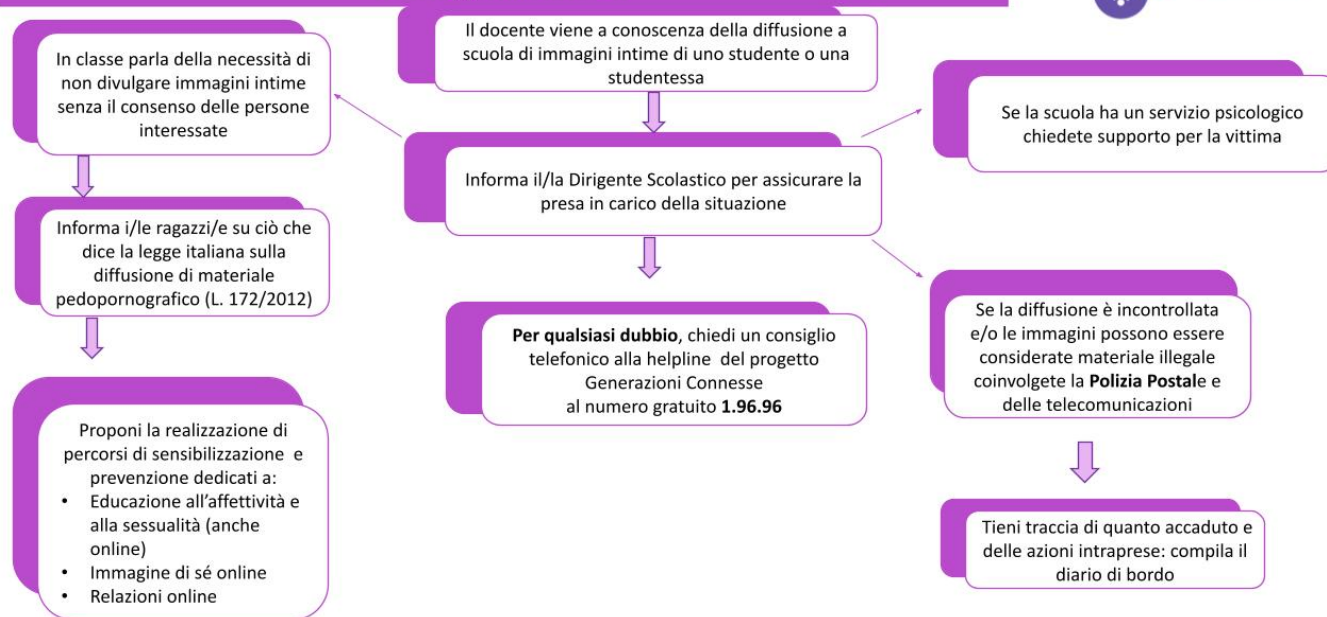
Se emergono evidenze passa allo schema successivo

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?



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:

segnalazioni.teambullismo@itisvallauri.edu.it;

- 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 interne (referente per il contrasto al bullismo/cyberbullismo).

Il personale della scuola, anche con l'ausilio del personale di assistenza tecnica, dovrà provvedere a conservare le eventuali tracce di una navigazione non consentita su Internet o del passaggio di materiali inidonei sui pc della scuola; la data e l'ora consentiranno di condurre più approfondite indagini; nel caso di messaggi, si cercherà di risalire al mittente attraverso i dati del suo profilo.

Sia nel caso di chat che di messaggi di posta elettronica, la vittima dovrà fornire prove documentali (stampe, screenshot, ecc.) per fornire le eventuali prove dell'indagine sugli abusi commessi.

Tali prove saranno utili anche ad informare la famiglia dello studente vittima di abuso, il Dirigente scolastico e, ove si configurino reati, la Polizia Postale.

In ogni caso, sarà opportuna una tempestiva informazione delle famiglie in merito all'accaduto, anche per consentire ulteriori indagini e, in assenza di prove oggettive, di raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico ed, eventualmente, alla Polizia Postale.

Qualora siano coinvolti più alunni, in qualità di vittime o di responsabili della condotta scorretta, le famiglie degli alunni in questione saranno informate tempestivamente per un confronto.

In base all'entità dei fatti si provvederà:

1. ad una comunicazione scritta alle famiglie;
2. a nota disciplinare sul registro elettronico;
3. a convocazione formale dei genitori degli alunni, tramite segreteria, da parte del Dirigente scolastico.

Per i reati più gravi la scuola si rivolgerà direttamente agli organi di polizia competenti.

AMBROGIO
MORRONE
18.03.2026
15:43:16
GMT+01:00

