Documento di ePolicy
I.A.C. "CROCE" - VITULAZIO

VIALE DANTE 17 - 81041 - VITULAZIO
Caserta (CE) - Campania
Data di approvazione: 10/12/2024 - 14:07

Cap 1 - Lo scopo della ePolicy

1.1 Scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

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

Capitolo 2 - Sensibilizzazione e prevenzione

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

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

Capitolo 4 - Segnalazione e gestione dei casi

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

1.1 Scopo dell'ePolicy

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

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

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

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

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

Perché è importante dotarsi di una E-policy?

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

L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

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

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

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

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

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

IL DIRIGENTE SCOLASTICO

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

- promuovere la cultura della sicurezza online e garantirla a tutti i membri della comunità scolastica, in linea con il quadro normativo di riferimento, le indicazioni del MIM, delle sue agenzie e attraverso il documento di ePolicy;
- promuovere la cultura della sicurezza online – anche attraverso il documento di ePolicy - integrandola ed inserendola nelle misure di sicurezza più generali dell'intero Istituto;
- ha la responsabilità di fornire sistemi per un uso sicuro delle TIC, internet, i suoi strumenti ed ambienti e deve

garantire alla popolazione scolastica la sicurezza di navigazione tramite internet utilizzando adeguati sistemi informatici e filtri;
- ha la responsabilità della gestione dei dati e della sicurezza delle informazioni e garantisce che l'Istituto segue le pratiche migliori possibili nella gestione dei dati stessi;
- deve tutelare la scuola e garantire agli utenti la sicurezza di navigazione utilizzando adeguati sistemi informatici e servizi di filtri Internet;
- ha il compito di garantire a tutto il personale una formazione adeguata sulla sicurezza online per essere tutelato nell'esercizio del proprio ruolo educativo e non;
- deve essere a conoscenza delle procedure da seguire in caso di un grave incidente di sicurezza online;
- deve garantire adeguate valutazioni di rischio nell'usare strumenti e TIC, effettuate in modo che comunque quanto programmato possa soddisfare le istanze educative e didattiche dichiarate nel PTOF di Istituto;
- deve garantire l'esistenza di un sistema che assicuri il monitoraggio e il controllo interno della sicurezza online in collaborazione con le figure di sistema;
- deve essere a conoscenza ed attuare le procedure necessarie in caso di grave incidente di sicurezza online.

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

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

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

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

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

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

Il Team ha il compito di:

- coadiuvare il Dirigente scolastico, coordinatore del Team, nella definizione degli interventi di prevenzione del bullismo (per questa funzione partecipano anche il presidente del Consiglio d'Istituto e i Rappresentanti degli studenti).
- Intervenire (come gruppo ristretto, composto da Dirigente e referente o referenti per il bullismo e il cyberbullismo, psicologo o 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.

Affinché l'E-policy 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.

Dirigente scolastico

- Garantisce la sicurezza, anche on-line, di tutti i membri della comunità scolastica.
- Promuove per i docenti la cultura della sicurezza on-line, attivando percorsi di formazione e prevenzione del fenomeno del cyberbullismo.
- Garantisce l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on-line.
- Gestisce ed interviene nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

Referente bullismo e cyberbullismo

- Coordina e promuove iniziative di prevenzione e di contrasto del bullismo cyberbullismo messe in atto dalla scuola.
- Coinvolge, con progetti e percorsi formativi tutti i componenti della comunità scolastica: personale docente e non docente, studenti, genitori.

Docenti

- Diffondono la cultura dell'uso responsabile delle TIC e della Rete.
-Integrano parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo l'uso delle tecnologie digitali nella didattica.
- Supportano gli studenti e le studentesse nelle attività di apprendimento che prevedono l'uso della LIM o altri dispositivi tecnologici che si connettono alla Rete.

Segnalano al dirigente scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

L'animatore digitale

- Supporta il personale scolastico da un punto di vista non solo tecnicoinformatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali.

- Promuove percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale".
- Monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola.
- Coinvolge la comunità scolastica nella partecipazione ad attività e progetti attinenti la "scuola digitale".

Il personale amministrativo, tecnico e ausiliario

- Svolge funzioni di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche in collaborazione con il dirigente scolastico e con il personale docente tutto.
- Controlla che gli utenti autorizzati accedano alla Rete della scuola con apposita password per scopi istituzionali e consentiti.
- Si occupa, ciascuno per la propria funzione, del funzionamento dell'Istituto scolastico che passa anche attraverso lo sviluppo della cultura digitale, dell'organizzazione del tempo scuola e del potenziamento dell'offerta formativa, ma anche le attività di formazione e autoformazione in tema di bullismo e cyberbullismo.
- Segnala al dirigente scolastico comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.
- Collabora nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

Gli studenti e le studentesse

- Utilizzano le tecnologie informatiche e digitali in conformità con quanto richiesto e consentito dai docenti.
- Sono tenuti/e al rispetto delle norme che disciplinano l'utilizzo consapevole delle tecnologie digitali con la finalità di salvaguardare la propria identità e quella altrui.
- Comprendono l'importanza di adottare buone pratiche di sicurezza on-line per non incorrere nei rischi della Rete.
- Partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete.
- Promuovono quanto appreso anche attraverso possibili percorsi di peer education.

I Genitori

- Sostengono la la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'informazione e delle comunicazioni nella didattica.
- Controllano l'utilizzo degli strumenti (pc, tablet, smartphone) e di Internet.
- Concordano con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di Internet.
- Fissano delle regole per l'utilizzo delle tecnologie informatiche e digitali.

GLI ENTI EDUCATIVI ESTERNI E LE ASSOCIAZIONI

- Osservano le politiche interne sull'uso consapevole della Rete e delle TIC.
- Attivano procedure e comportamenti sicuri per la protezione degli studenti e delle studentesse durante le attività che vengono svolte all'interno della scuola.

1.3 Integrazione ePolicy nei documenti scolastici

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

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

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

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

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

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

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.
Il referente del bullismo/cyberbullismo con il suo gruppo di lavoro, in collaborazione con la Commissione POF, in raccordo con il Collegio Docenti, opera al fine di integrare i regolamenti dell'Istituto con il presente documento, apportandone le opportune modifiche da proporre al Consiglio d'Istituto.

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.

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro i discenti e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.
L'E-policy viene condivisa e comunicata al personale, ai discenti, alla comunità scolastica attraverso:
la pubblicazione del documento sul sito istituzionale della scuola;
il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;
Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.
I discenti vengono informati sul fatto che sono monitorati, formati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

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

Nell'ambito delle attività educative relative alla prevenzione del bullismo e all'uso consapevole delle nuove tecnologie, la scuola ha integrato e consolidato il Team Bullismo, con l'integrazione da quest'anno del referente Team e di educazione civica e cittadinanza. L'obiettivo principale è sensibilizzare la comunità scolastica sui benefici e sui rischi legati all'utilizzo delle nuove tecnologie, promuovendo una cultura della responsabilità, del rispetto reciproco e dell'inclusione. Il percorso educativo si sviluppa su più fronti: 1. "Prevenzione e segnalazione del bullismo" È stato aggiornato e pubblicato il regolamento per la segnalazione di casi di bullismo. Inoltre, sono stati predisposti documenti e strumenti specifici per permettere a studenti, insegnanti e famiglie di individuare tempestivamente situazioni di disagio e intervenire con efficacia.
Il Team, nel corso dell'anno intende presentare due progetti fa realizzare in classe sulla piattaforma di Generazioni connesse: progetti neoconnessi kids (primaria) e progetti neoconnessi young (secondaria I grado)

Il **mondo digitale** offre infinite opportunità, ma è fondamentale imparare a navigarlo in modo consapevole e responsabile. Per questo, ***NeoConnessi Kids*** di **WINDTRE** si impegna a creare un ponte tra scuola e famiglia, accompagnando le bambine e i bambini in un **percorso di crescita digitale**. Partendo dal presupposto che la chiave sia fornire gli **strumenti per un utilizzo critico e responsabile della tecnologia**, NeoConnessi promuove il benessere digitale dei più piccoli.

Il **benessere digitale** è un concetto ampio che include:

- **Uso equilibrato della tecnologia**: trovare un sano equilibrio tra vita online e offline;
- **Consapevolezza dei rischi**: conoscere i potenziali pericoli della rete, come il cyberbullismo;
- **Relazione positive**: utilizzare la tecnologia per costruire relazioni sane e significative;
- **Ricerca di informazioni affidabili**: sviluppare un pensiero critico per distinguere le fonti attendibili da quelle false o fuorvianti.

Per l'anno scolastico 2024/2025, ***NeoConnessi Kids*** offre un **kit didattico totalmente rinnovato** e completamente digitale, accessibile tramite l'area riservata di Scuola.net. Stiamo lavorando per rendere l'esperienza in classe ancora **più coinvolgente, digitale ed efficace**.

NeoConnessi Kids offre anche numerose risorse gratuite per **docenti e famiglia** per aiutarli a comprendere le sfide e le opportunità del mondo digitale e a supportare le ragazze e i ragazzi nel loro percorso di crescita:

- Il **corso di formazione gratuito per docenti**, valido per l'assolvimento dell'obbligo formativo, che offre uno sguardo approfondito sui nuovi contenuti digitali per bambine e bambini in un'ottica sempre più crossmediale e un nuovo approfondimento sull'Intelligenza Artificiale per la didattica;
- Il **sito** **NeoConnessi.it** con risorse educative e proposte di attività per stimolare un uso consapevole e sicuro della rete da parte dei più piccoli e per aiutare le famiglie a impostare una educazione digitale;
- Il **corso di formazione sulla genitorialità digitale**, il ***Decalogo NeoConnessi*** per rafforzare il patto tra generazioni e il **gruppo Facebook**, la community con esperti dove trovare le giuste risposte a dubbi e recuperare per educare le bambini e i bambini all'uso corretto e sicuro dei dispositivi digitali della rete.

NeoConnessi Young si focalizza sullo sviluppo delle competenze chiave della cittadinanza digitale, guidando studenti e studentesse verso un **uso consapevole e responsabile della tecnologia**. Il programma mira a fornire alle classi gli strumenti necessari per navigare in sicurezza nel **mondo digitale**, costruendo relazioni sane e positive, e acquisendo

un **pensiero critico** nell'era dell'informazione. In linea con il quadro di riferimento europeo **DigComp**, adottato anche dal **Ministero dell'Istruzione e del Merito**, il programma offre un percorso educativo completo e coinvolgente. Dal 2018, il progetto, realizzato da **WINDTRE** con il supporto di esperti e la collaborazione di istituzioni autorevoli, si è ampliato per includere con NeoConnessi Young anche le **scuole secondarie di primo grado**.

NeoConnessi Young accompagna le classi in un viaggio verso un uso consapevole e responsabile della tecnologia, promuovendo il benessere digitale in un mondo sempre più connesso. Attraverso lo **Skill Game**, un'innovativa piattaforma di gioco basata sul quadro DigComp, gli studenti mettono alla prova e sviluppano le proprie competenze digitali in modo interattivo e divertente. Il percorso culmina con l'erogazione di un **Patentino delle Competenze Digitali**, che certifica il livello raggiunto e valorizza le abilità acquisite.

In occasione della Giornata Nazionale contro il Bullismo e Cyberbullismo, il nostro istituto organizza una manifestazione per sensibillizzare i ragazzi e promuovere i valori del rispetto e della convivenza civile. Le attività proposte saranno differenziate in base alle classi. La manifestazione si terrà il giorno 8 febbraio. Le classi IV e V della scuola Primaria parteciperanno alla manifestazione con laboratori creativi e momenti di riflessioni. Le classi prime della Scuola Secondaria parteciperanno alla manifestazione insieme agli allievi della Scuola Primaria, prendendo parte attiva alle attività di sensibilizzazione.

Le classi Seconde e Terze della Scuola Secondaria svolgeranno un'attività di approfondimento sul tema del Bullismo direttamente in classe, guidati dai loro insegnanti. Questa attività includerà un momento di confronto e discussione, oltre alla realizzazione di progetti creativi per promuovere il rispetto reciproco. Nel corso della giornata, gli allievi avranno anche l'opputunità di partecipare a incontri con esperti della settore: psicologi e specialisti della prevenzione del bullismo, che offriranno spunti di riflessione e risponderanno alle domande dei ragazzi.

L'esperienza riuscita della manifestazione dello scorso anno ha invogliato la scuola a riproporre la stessa esperienza anche per il nuovo anno scolastico.

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

Per risorsa didattica digitale si intende qualsiasi fonte di natura digitale a supporto della didattica. Si va dall'uso dell'immagine digitalizzata ad un percorso didattico completo. In particolar modo, facciamo qui riferimento a strumenti per la progettazione, sviluppo, utilizzazione, gestione e valutazione di processi e risorse per l'insegnamento e l'apprendimento.

Il progetto **Safer Internet Centre – Generazioni Connesse**, è cofinanziato dalla Commissione Europea nell'ambito del programma **Digital Europe**, ed è membro di una rete promossa dalla Commissione Europea che si concretizza nella piattaforma online "Better Internet for Kids" gestita da European Schoolnet, in stretta collaborazione con INSAFE (network che raccoglie tutti i SIC europei) e Inhope (network che raccoglie tutte le hotlines europee).

Il progetto prevede il coinvolgimento di docenti, genitori ed allievi, realizzando la concreta possibilità per docenti e genitori di aggiornarsi e formarsi sulle tematiche di rete.

E' possibile avere una panoramica completa accedendo al seguente indirizzo: http://www.generazioniconnesse.it/site/it/home

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.

CAPITOLO 2- SENSIBILIZZAZIONE E PREVENZIONE

2.1 Sensibilizzazione e prevenzione

L'I.C. "B. Croce di Vitulazio così intende intervenire:

Sensibilizzazione: A partire dalle prime della scuola primaria sino all'intero ciclo della Secondaria, si punta a informare ma soprattutto ad educare alla consapevolezza e alla riflessione sulle seguenti tematiche:
- Uso o abuso di internet
- Quanto sono dipendente dallo smartphone, che uso ne faccio, per quante ore nell'arco della giornata riesco a darmi delle regole?
- Come la rete ha modificato il mio modo di comunicare e di pormi in relazione con l'altro; i gruppi WhatsApp, la messaggistica sostituiscono il linguaggio verbale e non verbale?
- Quanto sono consapevole dei pericoli della rete, cosa penso di sapere, come penso di evitarli.

Prevenzione: Oltre a promuore le competenze previste dal curricolo digitale un accento particolare viene dato:

- alla conoscenza dell'importanza di tutelare la propria privacy e quella degli altri (dati sensibili, password, foto, video) e delle implicazioni legali in caso di trasgressione;
- alla conoscenza delle regole o norme etiche da tenere in mente quando si naviga in rete, quando si pubblica e/o si condivide un contenuto;
- alla riflessione di come sia possibile dietro uno schermo, protetti dall'anonimato infrangere con facilità tali norme, essere vittime o artefici di azioni lesive e offensive della propria e altrui persona.

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.

L'Istituto Comprensivo B. Croce ha elaborato ed approvato un documento che tiene conto del Quadro di riferimento per le competenze digitali dei cittadini aggiornato alla versione 2.2 (DigComp 2.2) ed il Digcomp come riferimenti fondamentali. In esso sono previste le 5 aree di competenza: Area 1 : Alfabetizzazione su informazioni dati. Area 2 : Comunicazione e collaborazione. Area 3: Creazione di contenuti digitali. Area 4: Sicurezza. Area 5: Risolvere problemi. Per ognuna di questa aree sono stati individuati: obiettivi, attività proposte e risorse per i diversi cicli scolastici: Infanzia, Primaria e Secondaria di 1°grado.

Il curricolo digitale scuola dell'Infanzia è organizzato per i bambini da tre a sei anni e si propone, attraverso la presenza di un adulto,favorire l'avvicinamento e la familiarizzazione degli allievi verso le nuove tecnologie sostendo il passaggio dal pensiero concreto a quello simbolico. Si suggeriscono alcune risorse che variano in base alle aree di competenza. Per quanto riguarda l'area 1, che prevede tra gli altri alcuni obiettivi come "Conoscere le principali funzionalità touch per navigare in Internet" e " Eseguire giochi ed esercizi di tipo logico, linguistico e matematico al computer, tablet o tavoli interattivi", si propone un canale video di Google dedicato ai bambini in cui è possibile settare i contenuti visualizzabili in base all'età (You Tube Kids).

Per l'area 2, che si pone obiettivi come "Individuare e riconoscere immagini, foto e video presentati dall'insegnante", oppure "Ascoltare e registrare e inviare un messaggio vocale con la supervisione del docente" si suggerisce ,oltre al canale indicato per l'area 1, anche siti di giochi interattivi proposti dai docenti.

Per area 3 , un obiettivo è " Sperimentare semplici programmi o applicazioni di grafica", si propongono risorse come Pixel Art e Coding; per l' area 4, tra i cui obiettivi è presente "Utilizzare semplici procedure di protezione dei dispositivi". si suggerisce una risorsa come Interland e per l'area 5 App Kids art.

Per la scuola Primaria le risorse si diversificano tenendo conto anche delle classi e delle aree di competenze. Sono previste risorse come Typin gclub o Piattaforma Giada per le classi prime e seconde per l'area 1 che riguarda principalmente "Navigare, ricercare dati, informazioni e contenuti digitali". Per l'area 2 Canale YouTube Kids oppure applicazioni di Google Workspace. Per l'area 3 ovvero sviluppare contenuti digitali si suggerisce una risorsa come Paint . Come traguardo della classe quinta l'alunno deve almeno saper scrivere un testo digitale e conoscere i più comuni motori di ricerca.

Per le classi terze, quarte e quinte sempre della Primaria si suggeriscono risorse come: Animaker, StoryJumper, BookCreator.

Per la Scuola Secondaria di 1 grado le 5 aree sopra elencate vengono distinte per obiettivi, attività e risorse in modo differenziato per le classi prime e successivamente per le seconde e terze. Per le classi prime della secondaria, nell'ambito dell'area 1 , le risorse preferibili sono indicate, tra le altre, Focus Junior e Interland. Per l'area 2 sono indicate Google Workspace, Avatar Maker. Per area di competenze 3, Creazione di contenuti digitali, si suggeriscono diverse risorse, quali: Animaker, StoryJiumper, Ourboox, BookCreator e diversi altri. Per le aree 4 e 5 sono suggeriti diversi canali che aiutano a proteggere i dispositivi, i dati personali, la salute e il benessere. Per le classi seconde e terze , sempre della secondaria 1 grado, per tutte le aree sono suggeriti i diversi motori di ricerca, Clip Champ, che sono utili soprattutto per interagire con gli altri attraverso le tecnologie, oppure Storymap, Bookcreator, Podcast per sviluppare contenuti digitali. Al termine della scuola secondaria l'alunno è in grado di utilizzare materiali digitali per l'apprendimento. Utilizzare il PC, periferiche e programmi applicativi. Utilizzare la rete per scopi di informazione, comunicazione, ricerca e svago e ovviamente sa riconoscere le potenzialità e rischi connessi all'uso delle tecnologie più comuni.

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.

La scuola e la famiglia hanno un ruolo chiave per garantire l'educazione dei più giovani a un uso consapevole e responsabile della tecnologia e della Rete. NeoConnessi è un percorso di responsabilità condivisa che coinvolge tutta la comunità educante – a partire dalla scuola e dalla famiglia – nell'impostazione di un rapporto sano con la Rete e i device.

Oltre ai kit didattici messi a disposizione dalla piattaforma generazioni connesse, l'IAC di Vitulazio ha deciso di aderire al progetti "Neoconnessi kids" e "Neoconnessi young".

I kit didattico digitale di ***NeoConnessi Kids*** contiene:

- **Guida didattica aggiornata**: una guida completa per i docenti, con nuove attività e suggerimenti.
- Il secondo volume di "***Nati Digital***": tante nuove avventure digitali per Auri, Tommi, Nico e i loro amici.
- **6 storie animate**: i personaggi di "Nati Digital" prendono vita in sei coinvolgenti episodi animati.
- **6 video-laboratori interattivi**: video-laboratori digitali per approfondire in modo divertente i temi chiave del benessere digitale, da utilizzare in classe dopo la visione delle storie animate.

Il kit didattico digitale di ***Neoconnessi Young***, sviluppato con il contributo di esperti in ambito psicologico, pedagogico, tecnologico e didattico, e con la collaborazione della Polizia di Stato e la Società Italiana di Pediatria, comprende:

- **Piattaforma Skill Game**: un ambiente di gioco online coinvolgente in cui le e gli studenti possono testare e

sviluppare le proprie competenze digitali attraverso un percorso strutturato e gamificato. Lo skill game consente anche di erogare il Patentino delle Competenze Digitali per una valorizzazione del livello di conoscenza e abilità di ogni singolo alunno.

- **Guida interattiva per i docent**i: un manuale online e interattivo completo di informazioni, schede didattiche e risorse pratiche per integrare l'educazione digitale nella propria attività didattica.

NeoConnessi Young si propone come un valido strumento per accompagnare i ragazzi e le ragazze della scuola secondaria di primo grado nel loro percorso di crescita digitale, promuovendo un uso consapevole, responsabile e sicuro delle tecnologie.

La scuola si propone, attraverso l'attivazione dei percorsi per studenti di arrivare a sensibilizzare anche i genitori degli stessi.

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 scuola ha provveduto all’individuazione del DPO, in italiano è traducibile con Responsabile della Protezione dei dati ed è una figura nuova introdotta dal GDPR. La sua principale mansione è quella di supportare il titolare, ma anche il responsabile del trattamento, nel rispetto del GDPR. In particolare deve assicurarsi che i dati siano conservati in conformità alle previsioni del Regolamento e che siano tenuti al sicuro, gestendo i rischi e imponendo misure di sicurezza conformi alle previsioni del GDPR. La scuola ha, inoltre provveduto all’implementazione della pagina del sito web dedicata alla privacy dove è illustrata agli utenti la normativa sulla privacy e dove è possibile reperire informative e DPIA, acronimo di Data Protection Impact Assessment che è una valutazione preliminare, eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

3.2 - Strumenti di comunicazione online (PUA)

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

sensibili di ciascuno, in particolar modo degli alunni e delle alunne.

La Scuola ha provveduto a stilare un'informativa sull'utilizzo della piattaforma didattica Google workspace e i documenti DPIA per i servizi Microsoft e Google.

In particolare Google Workspace è una suite di strumenti per la produttività e la collaborazione online sviluppata da Google. In precedenza nota come G Suite, questa piattaforma integra applicazioni come **Gmail** (email), **Google Drive** (archiviazione e condivisione di file), **Google Docs, Sheets e Slides** (editor di documenti, fogli di calcolo e presentazioni), **Google Meet** (videoconferenze), e **Google Calendar** (gestione del calendario).

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.

BYOD (Bring Your Own Device), in ambito scolastico, si riferisce alla pratica in cui gli studenti, i docenti e talvolta anche i genitori portano i propri dispositivi elettronici (come smartphone, tablet, laptop) a scuola per utilizzarli come strumenti didattici. L'idea alla base del BYOD è che l'accesso a tecnologie moderne e portatili può favorire un ambiente di apprendimento più interattivo, personalizzato e tecnologicamente avanzato, consentendo agli studenti di utilizzare dispositivi che conoscono e con cui sono familiari per completare attività educative.

A seguito della circolare ministeriale del 2022, firmata dal Ministro dell'Istruzione e del Merito Giuseppe Valditara, contenente le indicazioni sull'utilizza dei telefoni cellulari e di analoghi dispositivi elettronici nelle classi, è stato confermatovil divieto di utilizzare il cellulare durante le lezioni, trattandosi di un elemento di distrazione propria e altrui e di e di una mancanza di rispetto verso i docenti, come già stabilito dallo Statuto delle studentesse e degli studenti del 1998 e della circolare miministeriali n. 30 del 2007.

La scuola, nonostante l'utilizzo positivo dei suddetti device negli anni precedenti, attualmente non è ancora dotata di un regolamento BYOD.

Cap 4 - Segnalazione e gestione dei casi

4.1 - Cosa Segnalare

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

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

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

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

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

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

4.1. - Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che un/a alunno/a possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite alle quali può fare riferimento 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 dei discenti (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 stessa e l'intervento migliore da mettere in atto per aiutare chi è 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: il Dirigente scolastico, il referente per il Bullismo e Cyber-bullismo e il Team Bullismo composto da docenti dei diversi ordini e grado di scuola(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. 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 che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.
La condivisione avverrà anche attraverso la condivisione di informazioni in sede di Consigli di Intersezione, Classe ed Interclasse, che coinvolgono i rappresentanti dei genitori, i discenti,con l'utilizzo di locandine da affiggere a scuola e sul registro elettronico, attraverso news nel sito della scuola e durante i Collegi dei 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 la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via 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.

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

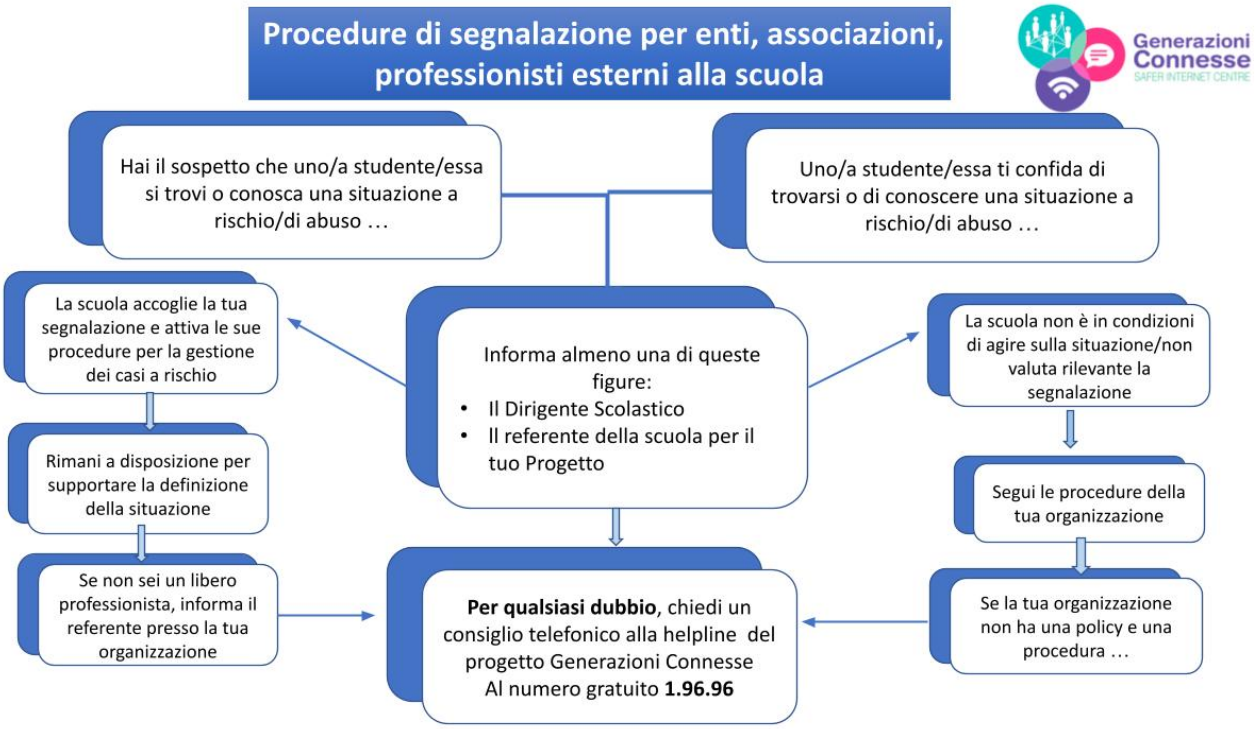
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

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

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.

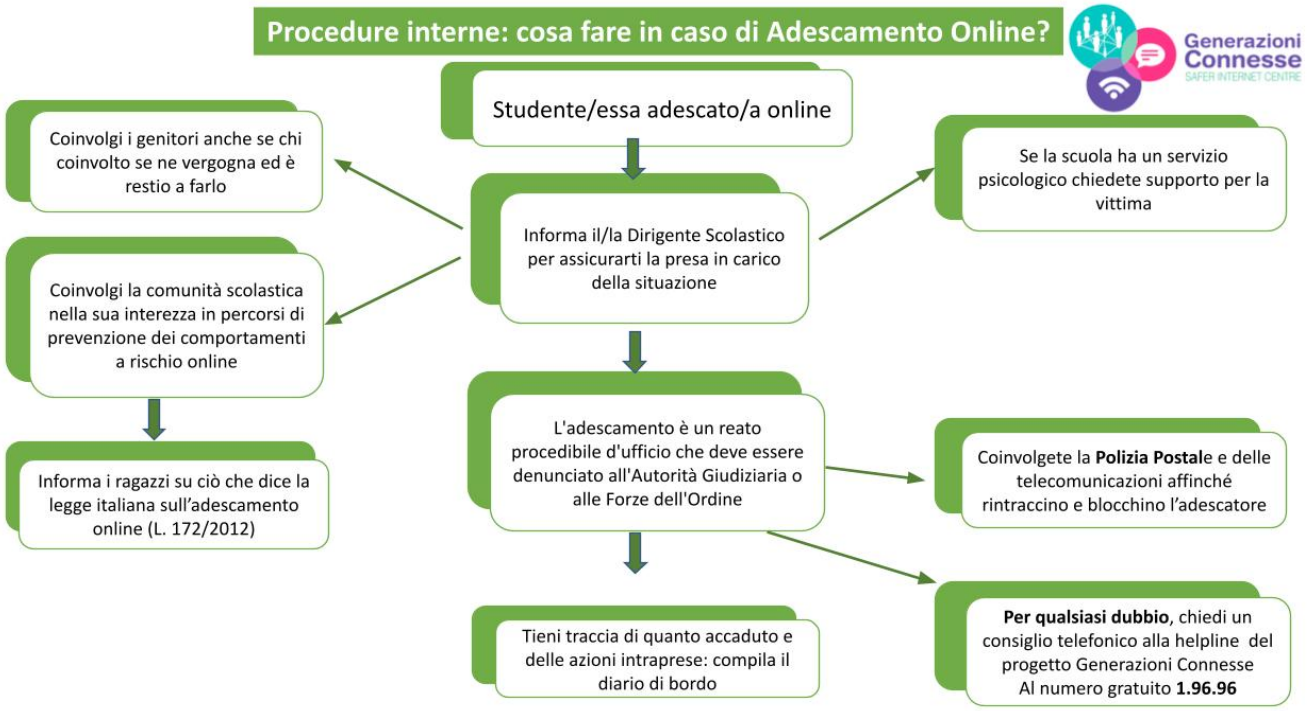
Se emergono evidenze passa allo schema successivo

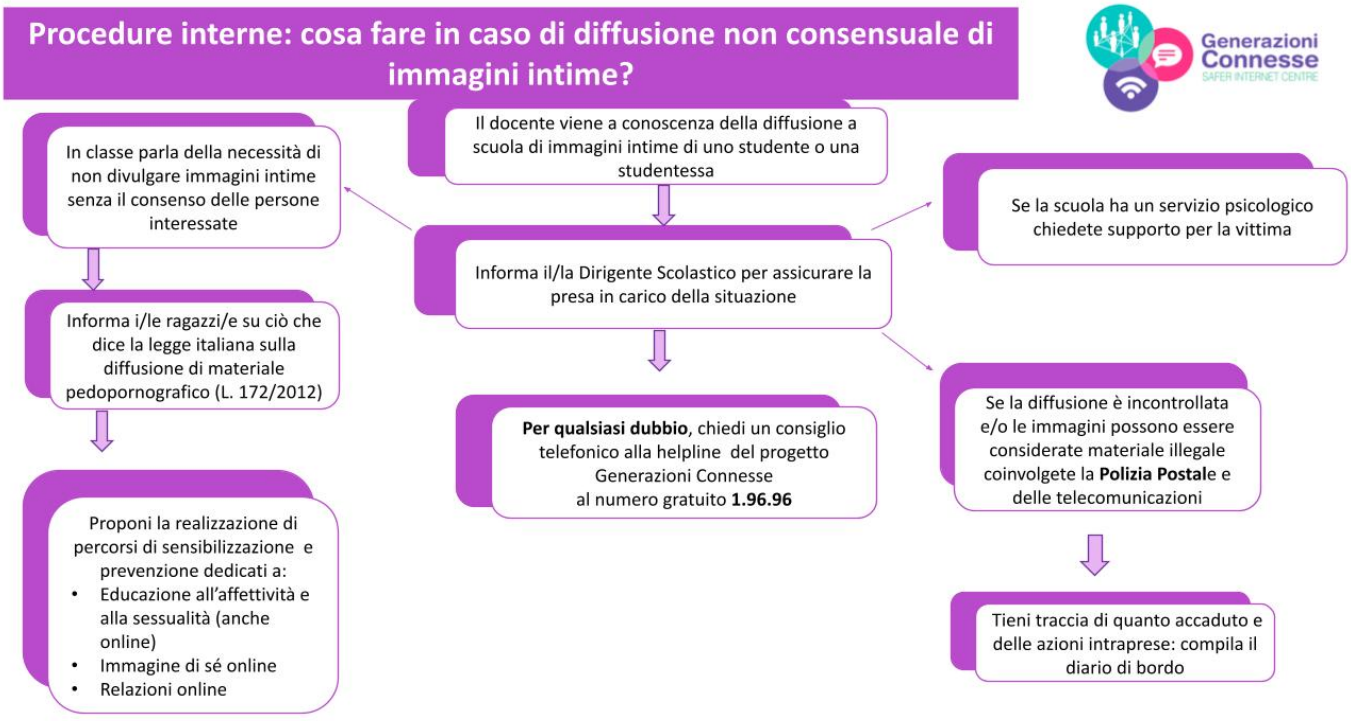
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

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

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





4.2 - Quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale 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

alunni e dalle alunne, ma si estende a tutte le altre attività educative. Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.
Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:
CASO A (SOSPETTO) – Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le alunni/e della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
CASO B (EVIDENZA) – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le alunni/e della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
Per tutti i dettagli fate riferimento agli allegati con le procedure.

Strumenti a disposizione dei discenti
Per aiutare gli alunni e le alunne 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.