Documento di ePolicy

ISTITUTO COMPRENSIVO L. MONTINI

VIA GIOVANNITTI SNC - 86100 - CAMPOBASSO

Campobasso (CB) - Molise

Data di approvazione: 09/09/2024 - 14:11

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.

Il documento ha lo scopo di individuare e descrivere la linea di condotta dell'Istituto relativamente all'utilizzo delle TIC nella didattica, educare e sensibilizzare bambini/ragazzi, genitori, docenti e personale tutto della scuola all'uso consapevole di Internet; far acquisire norme comportamentali per prevenire le problematiche che derivano da un utilizzo non responsabile delle tecnologie digitali.

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.

In particolare le figure professionali summenzionate devono:

L'animatore digitale e il team per l'innovazione digitale

- diffondere la E-Policy attraverso schede semplificative;
- garantire la tutela di tutti i dati relativi agli alunni pubblicati sul sito della scuola e/o altri siti;
- supportare il personale scolastico sia dal punto di vista tecnico-informatico, sia in riferimento ai rischi online, alla protezione e gestione dei dati personali;
- promuovere percorsi di formazione interna all'istituto negli ambiti di sviluppo della "scuola digitale";
- monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle TIC a scuola;
- controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione);
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale";
- svolgere funzioni di supporto al D.S. e al DSGA (di cui ai punti precedenti), Dirigente scolastico e Responsabili della sicurezza on-line (DSGA e docente su nomina del DS)).

Il referente per il bullismo e cyberbullismo

- coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo;
- coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori;
- coordinare attività e collaborare con le autorità locali e le altre agenzie competenti (Forze di polizia, associazioni e centri di aggregazione giovanile, ...);
- controllare probabili azioni di cyberbullismo e/o altri rischi on-line;
- supportare il personale nell'adozione delle procedure da seguire in caso di incidente nella sicurezza on-line.

Il personale amministrativo, tecnico e ausiliario

- promuovere la consapevolezza e l'impegno per la salvaguardia on-line in tutta la comunità scolastica;
- garantire che tutto il personale conosca le procedure da seguire in caso di incidente nella sicurezza on-line;
- garantire la tenuta di un registro sugli incidenti di sicurezza on-line;
- controllare la condivisione di dati personali;
- controllare l'accesso a materiali inadeguati/illegali;
- assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;
- garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

Studenti e studentesse

- leggere, comprendere ed accettare la E-Policy;
- utilizzare correttamente le tecnologie digitali;
- partecipare a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete;
- possedere capacità di ricerca e rispettare la normativa sul diritto d'autore;
- segnalare abusi o l'uso improprio delle tecnologie digitali o l'accesso a materiali inappropriati da parte dei compagni;
- tutelare e rispettare i propri compagni;
- conoscere ed applicare le norme sulla sicurezza;
- conoscere la politica scolastica relativa all'uso di telefoni cellulari, fotocamere digitali e dispositivi portatili;
- conoscere la politica scolastica sull'uso di immagini e sul cyberbullismo;
- adottare buone pratiche di sicurezza on-line dentro e fuori dalla scuola.

Genitori/adulti di riferimento

- leggere, comprendere, accettare e condividere la E-Policy d'Istituto;
- sostenere la scuola nella promozione della sicurezza on-line, anche partecipando a iniziative di sensibilizzazione e formazione organizzate dall'Istituto;
- comunicare ai docenti problemi rilevati, relativi all'uso non responsabile delle tecnologie digitali o Internet da parte dei propri figli;
- seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllando l'utilizzo del pc e di internet;

- accedere al sito web della scuola ed al registro elettronico in conformità con quanto stabilito dalla scuola medesima;
- collaborare con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite.

Tutti gli **attori esterni** sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

I soggetti esterni, pertanto, sono tenuti a:

- avere consapevolezza dei problemi di sicurezza on-line connessi all'uso di telefoni cellulari, fotocamere e dispositivi portatili;
- prendere visione del regolamento d'Istituto relativamente all'uso di telefoni cellulari, fotocamere digitali, dispositivi portatili;
- contribuire nella promozione di politiche scolastiche sulla sicurezza on-line;
- monitorare l'uso di dispositivi tecnologici;
- segnalare qualsiasi abuso sospetto ai responsabili della sicurezza on-line;
- raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo e cyberbullismo;
- adottare comportamenti sicuri, responsabili e professionali nell'uso delle tecnologie;
- conoscere ed applicare le norme sulla sicurezza;
- conoscere ed applicare le procedure di segnalazione;
- conoscere i provvedimenti adottabili in caso di omessa segnalazione o di comportamenti adottati in violazione del codice di comportamento.

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 in vigore nel nostro Istituto, il Patto di Corresponsabilità Educativa e il PTOF, incluso il piano per l'attuazione del PNSD, si integrano pienamente -per obiettivi e contenuti – con la presente ePolicy.

L'Istituto, secondo quanto disposto dall'art. 5 - comma 2 - della legge 29 maggio 2017 n, 71, ha integrato il Regolamento d'Istituto e il Patto di Corresponsabilità Educativa con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti, al fine di meglio regolamentare l'insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione al fenomeno.

Il Patto di corresponsabilità ((DPR 24 giugno 1998, n. 249, modificato dal DPR n. 235 del 21 novembre 2007-art. 5-bis) è aggiornato secondo le Linee di indirizzo "Partecipazione dei genitori e corresponsabilità educativa" al fine di informare e rendere partecipi le famiglie sul percorso intrapreso con il documento e-policy e il piano d'azione.

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.

La scuola utilizza diversi strumenti di comunicazione sia per valorizzare e promuovere le attività portate avanti dall'Istituto, sia per far circolare al suo interno informazioni di servizio o contenuti importanti tra i diversi attori scolastici (docenti, studenti, genitori, ...).

Tra gli strumenti di comunicazione esterna c'è in primis il sito web, tramite il quale l'Istituto trasmette la sua identità, i suoi valori, le sue azioni, i progetti e l'idea di educazione che porta avanti.

Tra gli strumenti di comunicazione interna, invece, ci sono l'e-mail istituzionale, una piattaforma web professionale di comunicazione, le piattaforme di lavoro condiviso e collaborativo come classroom, google doc con gli strumenti di google workspace e, non ultimo, il registro elettronico – che permette di gestire la comunicazione con le famiglie in merito all'andamento scolastico, ai risultati scolastici, a comunicazioni varie.

Relativamente alla condivisione e comunicazione della ePolicy, nel nostro Istituto vengono applicate le seguenti modalità:

Condivisione e comunicazione della ePolicy agli alunni e alle alunne

All'avvio dell'anno scolastico, ogni team docente e consiglio di classe illustra la presente e-policy agli alunni, insieme ai regolamenti correlati e al patto di corresponsabilità. Tutti gli alunni sono, quindi, informati delle modalità di utilizzo di internet, di ogni dispositivo digitale all'interno del contesto scolastico e delle buone norme da tenere relativamente all'uso delle TIC.

E' data particolare attenzione - nell'educazione sulla sicurezza - agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili, con specifico riferimento al contrasto di ogni forma di bullismo/cyberbullismo, mediante azioni mirate che coinvolgono il più possibile gli alunni e le alunne al fine di prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e.

Condivisione e comunicazione della ePolicy al personale scolastico

Copia integrale o sintetica del documento ePolicy viene inviato, tramite segreteria cloud, al personale scolastico il quale è, altresì, consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri

professionali è sanzionabile.

Condivisione e comunicazione della ePolicy ai genitori

È auspicabile una forte collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet. Gli incontri scuola-famiglia assembleari, collegiali e individuali rappresentano un'occasione utile per sensibilizzare le famiglie sui temi dell'uso delle TIC. Sono organizzati incontri informativi per presentare e condividere la presente e-policy, nonché eventuali percorsi formativi online rivolti alle famiglie sul tema del bullismo e del cyberbullismo.

L'informazione tramite il sito di istituto e tramite il Registro elettronico è la modalità prioritaria per comunicare alle famiglie le iniziative attuate dall'istituto.

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

In riferimento ai moduli delle attività con lePolicy (Piano d'Azioni) si precisa quanto segue:

1° ANNO DI ATTIVITA'

MODULO I

L'Istituto Comprensivo "L. Montini" ha elaborato la prima policy di E-SAFETY, nell'anno scolastico 2017/2018, ottenendo il primo attestato di "Scuola virtuosa" sui temi relativi all'uso sicuro e positivo delle tecnologie digitali il 30 giugno 2018. Negli anni a seguire ha provveduto ad aggiornare il documento ed a ottenere altri due attestati, rispettivamente il 29 giugno 2020 e il 01 ottobre 2022.
Il documento, quindi, è stato presentato in occasione della sua approvazione a tutto il Collegio dei docenti ed ai rappresentanti dei genitori in seno al Consiglio d'Istituto, nella versione originale ed in quelle aggiornate. Altresì, ai singoli docenti è stata inviata una sintesi dello stesso in formato Power Point, mentre i genitori sono stati informati nel corso delle assemblee tenute all'inizio di ciascun anno

scolastico e gli allievi nei primi giorni di scuola quando, nelle giornate dedicate all'accoglienza, tra le altre attività sono state rivisitate anche le regole d'Istituto. Non da ultimo, le famiglie annualmente hanno firmato il Patto di Corresponsabilità in cui sono riportati principi e regole presenti nel documento ePolicy e nel Regolamento d'Istituto.

L'Istituto, per il futuro, presenterà l'ePolicy con le stesse modalità adottate in precedenza e s'impegna a diffonderla negli ambienti scolastici mediante affissione di sintesi e/o schede semplificative - a cura dell'animatore e del team digitale - nelle bacheche dei singoli plessi.

MODULO II

L'Istituto effettuerà una rilevazione del fabbisogno formativo dei docenti sui temi dell'educazione civica digitale e una rilevazione di interessi, bisogni e comportamenti delle famiglie sull' uso positivo del digitale mediante questionari predisposti dal team digitale e/o dal referente per il bullismo e cyberbullismo.

MODULO III

L'Istituto ha integrato l'ePolicy nei propri documenti fin dall'anno scolastico 2019/2020, a seguito della prima elaborazione della medesima ePolicy.

MODULO IV

Per aiutare gli alunni/e a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, nella scuola è già presente lo sportello di ascolto con la figura di una psicologa.

Per il futuro prevede di inserire una casella/box per la raccolta di segnalazioni anonime in uno spazio accessibile e ben visibile di ciascun plesso della scuola.

Inoltre, gli alunni e le alunne potranno rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Il Referente per la prevenzione e il contrasto del Bullismo e del Cyberbullismo provvederà a raccogliere in modo sistematico e continuativo le segnalazioni in merito a fatti di bullismo.

Delle segnalazioni e degli esiti sarà tenuta traccia mediante il diario di bordo.

2° ANNO DI ATTIVITA'

MODULO I

Nell'Istituto sono già presenti docenti formati attraverso la Piattaforma Generazioni Connesse, la Piattaforma Elisa, Formazione Erasmus – eTwinning ed attraverso corsi in presenza presso l'U.S.R. Molise.

La scuola intensificherà la formazione rivolta ai docenti attraverso il supporto di esperti/associazioni esterne o avvalendosi del percorso disponibile sul sito di Generazioni Connesse, fino a coprire almeno il 60% del corpo docente.

MODULO II

Nel corso di questi anni la nostra scuola ha realizzato numerose attività sul tema dell'educazione digitale, coinvolgendo studenti, studentesse e famiglie:

ü ha predisposto ed organizzato il Progetto d'Istituto "Generazioni Connesse: Bullismo e Cyberbullismo", incluso nel PTOF

della scuola;

- ü celebra annualmente la Giornata Nazionale contro il Bullismo e Cyberbullismo con l'evento streaming **#cuoriconnessi** di UNIEURO e POLIZIA DI STATO;
- ü ha realizzato un evento teatrale dal titolo **"Scherzo o non scherzo!?"**;
- ü ha partecipato ad eventi di educazione alla legalità dal titolo "**#StopCyberbullismo**";
- ü ha partecipato al progetto proposto dalla Prefettura di Campobasso ***#STOPCYBERBULLISMO*** ed al successivo concorso ***"Uno spot contro il Cyberbullismo"*** **di cui è** risultata vincitrice ed è stata premiata alla presenza del Ministro degli Interni, Luciana Lamorgese;
- ü ha realizzato il progetto **"PILLOLE DI CYBERBULLISMO"** (Legge n. 234/2021);
- ü ha organizzato numerosi incontri tra ragazzi e ragazze, famiglie e Polizia Postale;
- ü ha partecipato, con alcune classi, alla diretta streaming del 21 settembre 2023 tenuta presso il Ministero dell'Istruzione e del Merito, allo scopo di promuovere e aggiornare l'attivazione delle ePolicy;
- ü ha organizzato presso la Scuola Allievi Carabinieri di Campobasso un **convegno** dal titolo **"NON BULLI…AMO"**, in cui sono intervenuti il Procuratore della Repubblica presso il Tribunale per i Minorenni di Campobasso, la Presidente dell'Ordine degli Psicologi della Regione Molise, il Commissario Capo Responsabile Sezione Operativa per la Sicurezza Cibernetica, l'Ispettore Responsabile I Settore P.G. di Campobasso, il Comandante Scuola Allievi Carabinieri di Campobasso;
- ü dall'anno scolastico 2022/23 realizza il Progetto "**Una patente smartphone … per la sicurezza!"**;
- ü dal 2021 ha partecipato al monitoraggio ministeriale della Piattaforma Elisa sul bullismo e cyberbullismo.

L'Istituto, pertanto, si impegna a proseguire con l'organizzazione/realizzazione delle attività summenzionate, integrandole con l'utilizzo del kit didattico e la formazione rivolta a famiglie, studenti e studentesse attraverso il percorso previsto sulla piattaforma di Generazioni Connesse.

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

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

Cap 2 - Sensibilizzazione e prevenzione

2.1 - Sensibilizzazione e prevenzione

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

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

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

La nostra scuola già da qualche anno attua interventi di sensibilizzazione e prevenzione universale mediante il progetto d'Istituto "GENERAZIONI CONNESSE: Bullismo e Cyberbullismo" che integra l'offerta formativa. Per suo tramite essa forma e consolida le competenze educative di base necessarie per poter gestire le situazioni di vita che i ragazzi sperimentano online: li informa sui vari rischi online cui possono incorrere e su quali sono i comportamenti più corretti da adottare. In particolare il progetto vuole rendere i ragazzi consapevoli circa un determinato problema che potrebbe presentarsi nel gruppo, incoraggiarli ad adottare comportamenti più funzionali, favorire la diffusione di informazioni utili alla collettività. Nel contempo promuove competenze digitali al fine di ridurre i rischi per la loro sicurezza.

Non sono previsti ancora interventi di prevenzione selettiva e prevenzione indicata poiché, al momento, non risultano gruppi di studenti in cui è presente il rischio on-line o casi specifici.

Il nostro istituto, inoltre, in questi ultimi anni ha organizzato incontri con soggetti esterni, come la Polizia Postale – Psicologi - Procuratore della Repubblica presso il Tribunale per i minorenni, per sensibilizzare docenti, alunni e genitori sui temi della sicurezza online.

Per i prossimi anni prevede ulteriori incontri con esperti esterni (polizia, associazioni, ...) e l'organizzazione di percorsi di sensibilizzazione e formazione su un uso responsabile e costruttivo della Rete in famiglia e a scuola, anche mediante la piattaforma Generazioni Connesse.

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'alfabetizzazione informatica è presente nel Piano dell'Offerta Formativa del nostro Istituto come principale obiettivo da raggiungere nel percorso formativo.

La scuola, pertanto, è impegnata a sviluppare, a seconda del grado di maturità degli alunni, le competenze digitali previste dal quadro di riferimento DigComp 2.2. Le aree tematiche in esso riportate vengono affrontate anche trasversalmente con la disciplina "Educazione Civica".

2.3 - Il Kit Didattico

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

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

Il Kit Didattico diventa, dunque, parte integrante del materiale a disposizione dei docenti indispensabile per implementare le competenze digitali degli alunni, come previsto dai Piani di Azione illustrati nei paragrafi precedenti.

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.

Il nostro Istituto, avvalendosi anche della figura del Responsabile della protezione dei dati (R.P.D./D.P.O.), redige l'Informativa Generale sul trattamento dei dati personali ai sensi degli Artt. 13 e 14 del Regolamento UE 2016/679 (GDPR) e fornisce a ciascun utente informazioni relative alle modalità con le quali vengono trattati i dati e quali diritti può esercitare l'interessato rispetto ad ogni trattamento.

Ciascuna Informativa Generale viene integrata, caso per caso, da altre Informative Specifiche.

I dati personali vengono trattati ispirandosi ai seguenti principi generali: necessità, finalità, liceità, minimizzazione, correttezza, trasparenza e lealtà, sicurezza e protezione.

A garanzia della riservatezza dei dati sono applicate misure adeguate di sicurezza organizzativa ed informatica evidenziate nel "Documento delle misure a tutela dei dati delle persone" elaborato dall'Istituto Scolastico con riferimento esplicito alle regole tecniche in materia di conservazione digitale degli atti, definite dall'Agenzia per l'Italia Digitale (Ag.I.D.).

Tra i punti da soddisfare per rendere compliant ogni Istituto Scolastico al Regolamento UE 2016/679, la nostra scuola:

- redige un registro dei trattamenti dei dati, deposto in segreteria (il registro è depositato in cloud con accessi limitati al personale autorizzato), sia per il titolare che per il responsabile dei trattamenti,
- predispone una lettera di incarico per il trattamento dei dati al personale ATA, ai collaboratori scolastici (tutto il personale ATA -Assistenti e Collaboratori) e ai docenti all'inizio del rapporto di lavoro con aggiornamenti ad inizio del nuovo a.s.,
- adotta misure tecniche ed organizzative per garantire la sicurezza dei trattamenti:

- ha effettuato la migrazione del sito da suffissi gov.it a suffissi edu.it
- utilizza il protocollo HTTPS per la comunicazione su Internet
- possiede un sistema di backup e un piano di disaster recovery
- ha realizzato un sito web secondo i protocolli di privacy by default e by design.

Relativamente alla sicurezza della intranet scolastica, l'Istituto si avvale di un gestore della rete, AFA System, che si occupa - attraverso il proprio sistema Majornet – di controllare il traffico con sistemi di controllo e limitazioni di accesso alla rete tramite una blacklist, firewall e registro dei log di accesso.

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.

Per garantire il diritto di accesso a Internet in tutte le sezioni e classi, dalla scuola dell'infanzia alla scuola secondaria di primo grado, il nostro Istituto è provvisto di una rete Wi-fi adeguata al numero di studenti e in grado di supportare il traffico dati generato dal numero di utenti. Dispone, inoltre, di fibra ottica a banda larga, soluzioni cloud e cablaggio LAN.

La scuola, per le attività da svolgere nel contesto extra-scolastico, mette anche a disposizione degli alunni della scuola primaria e secondaria di primo grado, che ne avessero reali necessità, tablet e notebook per la didattica a distanza in regime di comodato d'uso gratuito.

In riferimento alla sicurezza dell'ambiente digitale ed alla manutenzione del sistema di accesso, si avvale di un gestore della rete, AFA System, che si occupa - attraverso il proprio sistema Majornet - di controllare il traffico con sistemi di controllo e limitazioni di accesso alla rete tramite una blacklist, firewall e registro dei log di accesso; relativamente agli aspetti legali, in relazione prevalentemente alla privacy, si avvale della figura del Responsabile della protezione dei dati (R.P.D./D.P.O.)

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.

Il nostro Regolamento d’Istituto, aggiornato e consultabile nella sezione “Amministrazione Trasparente del sito ufficiale https:/icmontinicb.edu.it, non consente l’uso del cellulare all’interno della scuola e disciplina i provvedimenti da adottare in caso di violazione. Altri strumenti possono essere utilizzati solo ed esclusivamente per uso didattico/scolastico.

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.

Il nostro Istituto ha provveduto dall'anno scolastico 2017/18 alla nomina del Referente per le iniziative di prevenzione e contrasto al bullismo e cyberbullismo, a munirsi di un documento e-policy, ad integrare il Regolamento d'Istituto ed il Patto di Corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari.

La tematica del **cyberbullismo** è ampiamente trattata mediante il progetto d'Istituto "GENERAZIONI CONNESSE: Bullismo e Cyberbullismo" che si prefigge di rendere gli alunni consapevoli in merito a cos'è il cyberbullismo, le sue caratteristiche, la suddivisione nei due grandi gruppi, come riconoscerlo, le responsabilità civili e penali di chi compie atti di bullismo e cyberbullismo, le responsabilità che ricadono su ragazzi e ragazze, genitori e docenti. Destinatari del progetto sono gli alunni di tutte le classi della scuola primaria e secondaria di primo grado, con declinazione diversa delle priorità tra i diversi cicli. Gli obiettivi del progetto vengono raggiunti mediante una serie di attività/azioni che vanno dalla semplice conversazione, alla visione e analisi di filmati – compresi i video di Generazioni Connesse, alla lettura di testi, a giochi di ruolo, agli incontri con la Polizia Postale.

Al fine di rendere i ragazzi più sicuri e pronti ad affrontare eventuali situazioni a rischio, quali **adescamento online e sexting**, la nostra scuola si prefigge di accompagnarli in due percorsi paralleli: da un lato un percorso di educazione all'affettività e alla sessualità affinché imparino a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri; dall'altro un percorso di educazione digitale che comprenda lo sviluppo di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online. Importante è il ruolo degli adulti – genitori e/o insegnanti – che devono essere un punto di riferimento, ispirare fiducia, affinché i ragazzi si sentano ascoltati, compresi, non giudicati.

Trattandosi di una problematica molto delicata da gestire e con possibili ripercussioni psicologiche significative, l'esistenza di casi reali comporterebbe l'intervento della Polizia Postale e di un Servizio territoriale.

La prevenzione dell'**hate speech** è legata indissolubilmente all'educazione e alla sensibilizzazione alla diversità, da attuarsi all'interno della comunità educante.

Il PTOF della nostra scuola, tra le altre, prevede anche l'Educazione alle pari opportunità e prevenzione della violenza di genere. In particolare, l'Istituto si propone di potenziare la cultura dell'inclusione per rispondere in modo efficace alle necessità di ogni alunno, di ridurre le barriere che limitano l'apprendimento e la partecipazione sociale, di far acquisire non solo gli obiettivi didattici ma soprattutto abilità che migliorino, in modo reale, le azioni quotidiane e la qualità della vita attraverso un costante utilizzo di ecosistemi relazionali. Per questo privilegia attività formative che favoriscono l'acquisizione della conoscenza di sé, la costruzione di una propria identità e rapporti relazionali positivi.

Azioni di prevenzione alla **dipendenza da Internet e gioco online** sono promosse mediante l'integrazione della tecnologia nella didattica - al fine di evidenziarne il suo utilizzo funzionale e rendere, così, i ragazzi più consapevoli delle proprie abitudini online, momenti di riflessione comune che mettono in risalto la tecnologia come strumento per raggiungere i propri obiettivi e non solo come strumento di distrazione o addirittura di ostacolo, lo sviluppo di conoscenze e competenze riferite al mondo del web e della comprensione dei rischi personali legati al suo utilizzo scorretto.

Il personale docente dell'Istituto, quando ha il sospetto o la certezza che uno/a studente/essa sia vittima o responsabile di

una situazione di cyberbullismo, sexting o adescamento online, ha a disposizione le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (si vedano i paragrafi successivi). Tali procedure saranno 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 e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà.

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

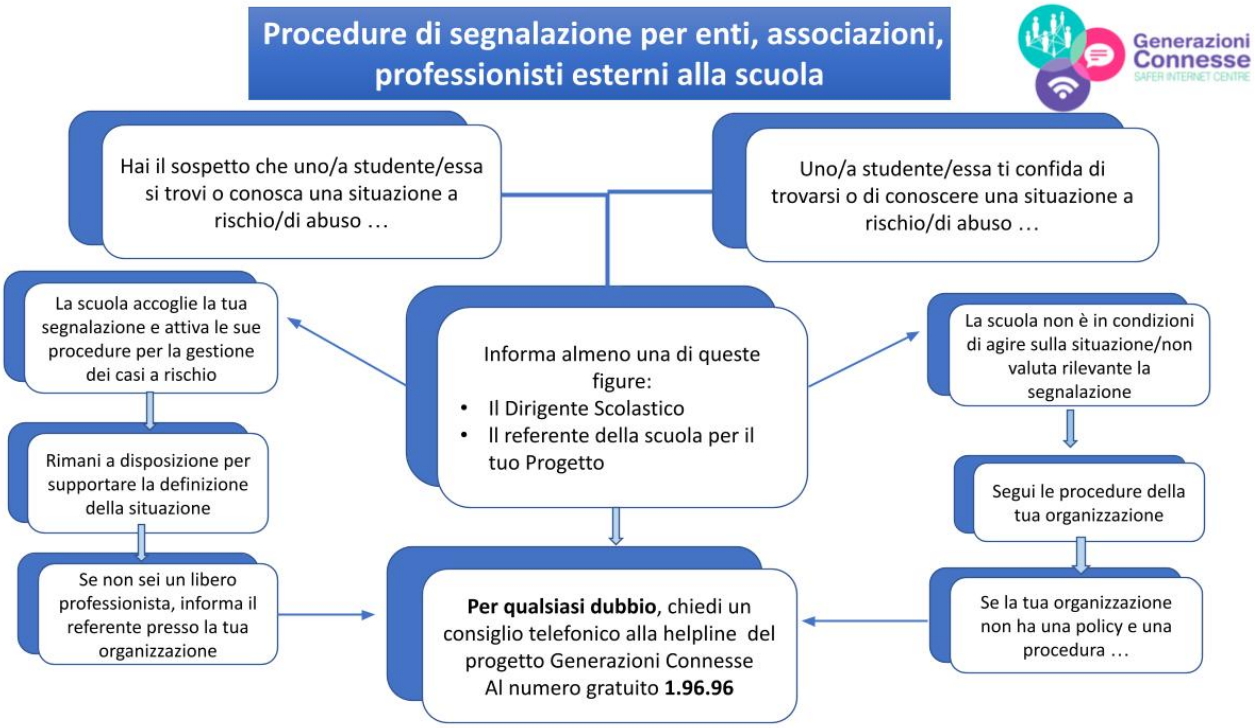
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

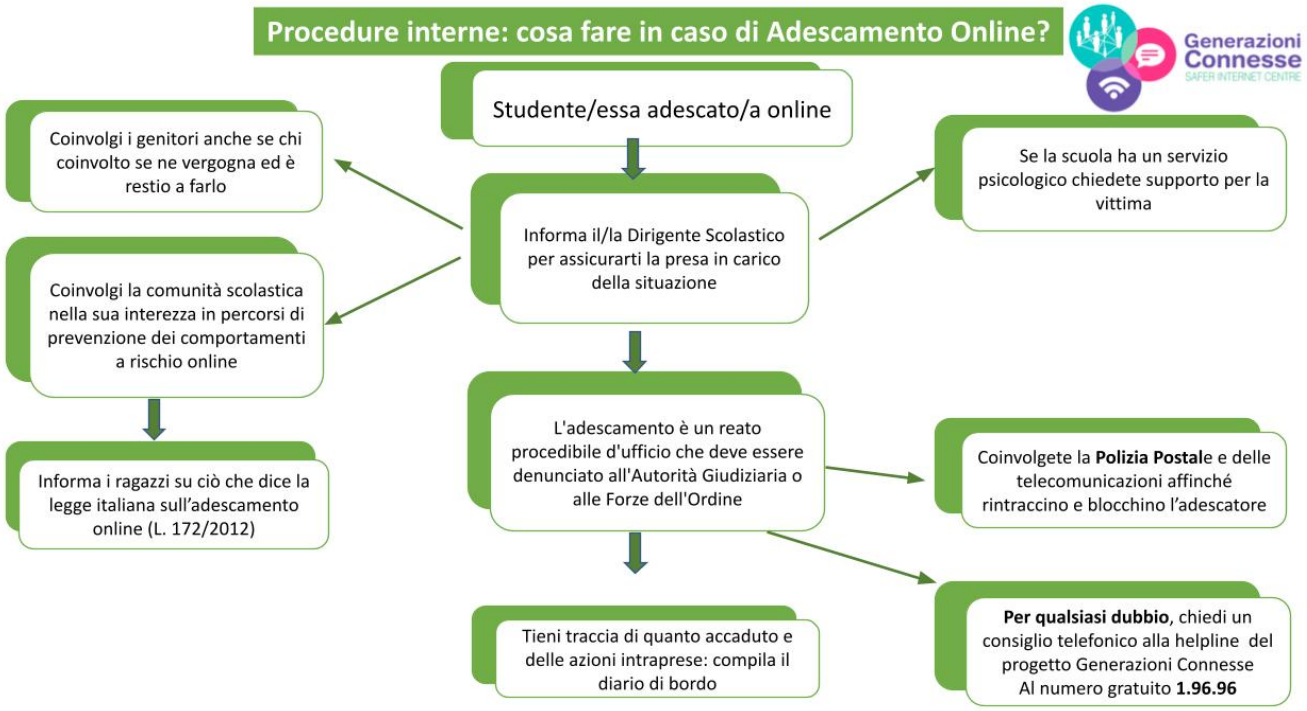
Se emergono evidenze passa allo schema successivo

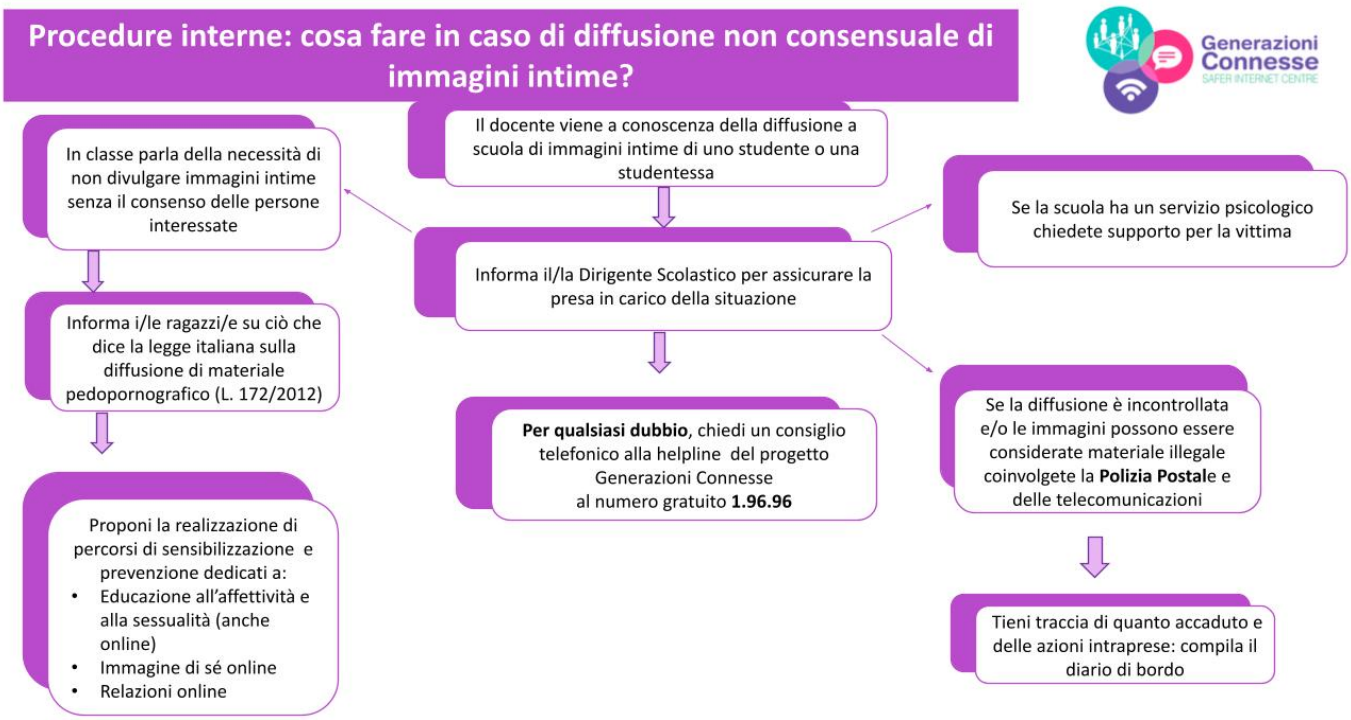
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

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





Per aiutare gli alunni/e a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola prevede - oltre allo sportello di ascolto già presente - una casella/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile di ciascun plesso della scuola.

Il Referente per la prevenzione e il contrasto del Bullismo e del Cyberbullismo provvede a raccogliere in modo sistematico e continuativo le segnalazioni in merito a fatti di bullismo. La gestione dei casi rilevati andrà differenziata a seconda della loro gravità: per tutti è opportuna la condivisione a livello di Consiglio di Classe/Team di Docenti di ogni episodio rilevato.

Delle segnalazioni, gestione dei casi e risoluzione sarà tenuta traccia mediante il diario di bordo.