I.C. "RACHEL BEHAR"-TRECATE
Prot. 0006891 del 05/06/2025
II (Uscita)

Documento di ePolicy
I. C. "RACHEL BEHAR"

VIA MEZZANO 41 - 28069 - TRECATE
Novara (NO) - Piemonte
Data di approvazione: 05/06/2025 - 15:14

Cap 1 - Lo scopo della ePolicy

1.1 Scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

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

Capitolo 2 - Sensibilizzazione e prevenzione

1. Sensibilizzazione e prevenzione
2. Il Curricolo Digitale
3. IL KIT DIDATTICO

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

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

Capitolo 4 - Segnalazione e gestione dei casi

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

1.1 Scopo dell'ePolicy

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

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

La competenza digitale è una competenza chiave del cittadino europeo come indicato dal Consiglio Europeo

(Raccomandazione del 2018) che permette ad ogni cittadino di esercitare i propri diritti all'interno degli ambienti digitali (ONU - Commento Generale 25: I diritti dei minori negli ambienti digitali).

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

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

Perchè 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, al fine di svilppare , attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

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 ed 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.

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 Dirigente scolastico,in collaborazione con i Referenti bullismo e cyberbullismo, valuterà la necessità di aggiornare periodicamente il Regolamento d'Istituto con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida del Ministero dell'Istruzione e le indicazioni normative generali.

Il Regolamento d'Istituto disciplina in modo dettagliato le tematiche in oggetto, e in particolare:

Nel regolamento di disciplina ai punti:

- PUNTO 3: Utilizzo di cellulari e apparecchi elettronici senza l'autorizzazione dell'insegnante
- PUNTO 4: Registrazione e riprese audio/foto/video non espressamente autorizzate durante le attività scolastiche, anche da remoto. Diffusione di registrazioni delle suddette riprese audio/foto/video non espressamente autorizzate. Partecipazione consapevole a registrazioni e riprese audio/foto/video durante le attività scolastiche
- PUNTO 7: Comportamenti violenti (sia sul piano fisico che su quello psico-emotivo) atti ad intimidire i compagni o a limitarne la libertà personale, reiterati anche tramite l'uso dei social network (BULLISMO e CYBERBULLISMO).

Il personale scolastico si impegna a conoscere e ad applicare il Regolamento d'Istituto e gli eventuali aggiornamenti. A tale scopo partecipa periodicamente ad attività formative inmateria di privacy e di utilizzo corretto dei dispositivi digitali.

Il monitoraggio dell'implementazione della ePolicy avverrà:

· all'inizio dell'anno scolastico, contestualmente alla revisione del PTOF, a cura del Dirigente scolastico, dei Referenti per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo, dell'Animatore digitale e del Team per l'innovazione digitale, della Funzione strumentale PTOF;

· alla fine di ogni anno scolastico ,contestualmente al Rapporto di Autovalutazione e sulla base dei casi problematici riscontrati

---

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.

Attraverso una serie di iniziative dedicate , l'IC Behar si impegna ad assicurare la concreta promozione degli intenti dichiarati nel documento, valorizzando studenti e studentesse ed esplicitando ruoli e prerogative di tutte le figure operanti a vario titolo nella comunità scolastica. In particolare:

- il personale della Scuola riceverà adeguata informazione/formazione sull'uso sicuro e responsabile della Rete;
- agli studenti, ad inizio anno, verrà presentato dai docenti il documento di E-policy, insieme ai regolamenti correlati, al fine di fornire loro spunti di riflessione, regole condivisedi sicurezza per gestire consapevolmente il mondo del Web;
- nel corso dell'anno ciascun Consiglio di Classe dedicherà alcune lezioni alle buone pratiche per un uso sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al Cyberbullismo;
- le famiglie saranno informate in merito alla linea di condotta adottata dalla Scuola per un uso consapevole e sicuro delle tecnologie digitali e di Internet attraverso la condivvisione del presente documento e di materiali informativi specifici sul sito web della Scuola;
- La Scuola organizzerà durante l'anno incontri finalizzati a sensibilizzare/informare le famiglie sul tema della sicurezza informatica e sui comportamenti da monitorare o evitare.

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

Gestione delle infrazioni alla E-policy

La Scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

Eventuali infrazioni alla presente E-policy andranno tempestivamente segnalate al Dirigente Scolastico, che avrà cura di convocare le parti interessate onde valutare possibili azioni da intraprendere.

Le infrazioni a carico degli alunni sono identificabili in:

- Uso social network per pubblicare, condividere o, in genere , postare commenti o giudizi lesivi della dignità altrui;
- condivisione di dati o immagini personali che possano permettere l'identificazione dei soggetti;
- connessioni a siti proibiti o comunque non autorizzati;
- pubblicazione di foto o immagini non autorizzate e/o compromettenti. Gli interventi correttivi previsti ssono rapportati all'età, nonchè alla gravità dell'infrazione commessa, coerentemente con quanto definito nel Regolamento d'Istituto .

Le infrazioni a carico del personale scolastico sono identificabili in:

- utilizzo delle tecnologie e della strumentazione della Scuola non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi.
- diffusione delle password assegnate e custodia non adeguata degli strumenti e degli accessi di cui possano approffittare terzi;
- mancata sorveglianza che possa favorire un utilizzo non autorizzato delle TIC da parte degli alunni;
- mancato pronto intervento dinanzi a palesi o sospetti episodi di infrazione. Le procedure sanzionatorie attivabili sono

quelle previste dalla disciplina contrattuale. Compito dei genitori è supportare gli insegnanti e il personale scolastico nella progettazione di efficaci azioni di riconoscimento e contrasto ai principali rischi rappresentati dalla navigazione internet da parte di utenti giovani e poco accorti. Le azioni e la condotta dei familiari possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a Scuola. In particolare, tra le iniziative familiari meno favorevoli potrebbero rientrare una piena autonomia concessa al proprio figlio nella navigazione sul Web e nell'utilizzo dei devices personali, e, più in generale, il mancato dialogo rispetto alle problematiche in questa sede affrontate. I genitori possono essere convocati a scuola dai docenti dal Dirigente scolastico per concordare misure educative sanzionatorie anche a norma di legge.

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.

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.

Struttura del Curricolo digitale

Il Digicomp 2.2 individua cinque aree di competenze.

AREE	DESCRITTORI
1. Alfabetizzazione su informazioni e dati	1.1 Navigare, ricercare e filtrare dati, informazioni e contenuti digitali
	1.2 Valutare dati, informazioni e contenuti digitali
	1.3 Gestire dati, informazioni e contenuti digitali
2. Comunicazione e collaborazione	2.1 Interagire attraverso le tecnologie digitali
	2.2 Condividere informazioni attraverso le tecnologie digitali
	2.3 Esercitare la cittadinanza attraverso le tecnologie digitali
	2.4 Collaborare attraverso le tecnologie digitali
	2.5 Netiquette
	2.6 Gestire l'identità digitale
3. Creazione di contenuti	3.1 Sviluppare contenuti digitali
	3.2 Integrare e rielaborare contenuti digitali
	3.3 Copyright e licenze
	3.4 Programmazione
4. Sicurezza	4.1 Proteggere i dispositivi
	4.2 Proteggere i dati personali e la privacy
	4.3 Proteggere la salute e il benessere
	4.4 Proteggere l'ambiente
5. Soluzione di problemi	5.1 Risolvere problemi tecnici
	5.2 Individuare i bisogni e le risposte tecnologiche
	5.3 Utilizzare in modo creativo le tecnologie digitali
	5.4 Individuare divari di competenze digitali

SCUOLA DELL' INFANZIA

La Scuola dell'Infanzia si qualifica come luogo di apprendimento e di socializzazione intenzionalmente organizzato per i bambini da tre a sei anni. È in questo contesto che, grazie all'intervento educativo, si avviano processi di simbolizzazione attraverso una pluralità di linguaggi. I bambini, fin da piccolissimi, vengono a contatto diretto con le nuove tecnologie. L'avvicinamento e la familiarizzazione verso queste tecnologie, supportati dalla presenza di un adulto, favoriscono il passaggio dal pensiero concreto a quello simbolico, supportando la maturazione delle capacità di attenzione, riflessione, analisi e creatività, attraverso la progettazione di esperienze significative a livello affettivo, cognitivo, metacognitivo e relazionale.

AREA DI COMPETENZA 1: ALFABETIZZAZIONE SU INFORMAZIONI E DATI			
DESCRITTORE DELLA COMPETENZA	OBIETTIVI	ATTIVITA' PROPOSTE	RISORSE SUGGERITE

1.1 Navigare, ricercare e filtrare dati, informazioni e contenuti digitali 1.3 Gestire dati, informazioni e contenuti digitali	• Conoscere le principali funzionalità touch per navigare in Internet • Conoscere ed individuare su un device le icone dei principali canali di comunicazione e social media per l'infanzia • Ricercare, con la supervisione del docente, informazioni, dati e contenuti in ambienti digitali adottando le strategie più idonee (tasti, pulsanti, icone, comandi vocali) • Eseguire giochi ed esercizi di tipo logico, linguistico, matematico, topologico, al computer, tablet o tavoli interattivi.	• Utilizzo degli strumenti a disposizione • Utilizzo delle icone su un dispositivo • Uso del mouse ed alcuni tasti della tastiera • Uso di applicazioni multimediali, selezionate dal docente, per ricercare informazioni e dati utilizzando i comandi vocali, pulsanti, parole calde, icone	• YouTube Kids canale video di Google dedicato ai bambini, in cui è possibile settare i contenuti visualizzabili in base alle fasce d'età • Siti di giochi interattivi proposti dai docenti

AREA DI COMPETENZA 2: COMUNICAZIONE E COLLABORAZIONE			
DESCRITTORE DELLA COMPETENZA	OBIETTIVI	ATTIVITA' PROPOSTE	RISORSE SUGGERITE
2.1 Interagire con gli altri attraverso le tecnologie 2.4 Collaborare attraverso le tecnologie digitali 2.5 Netiquette	• Individuare e riconoscere immagini, foto e video presentati dall'insegnante. • Ascoltare, registrare e inviare un messaggio vocale, con la supervisione del docente. • Utilizzare emoticon per l'autovalutazione del proprio comportamento nelle interazioni online	• Visionare immagini, brevi filmati e documentari didattici con la presenza dell'insegnante. • Raccontare e descrivere ciò che vede sugli schermi. • Rispettare il proprio turno e lo spazio di attività.	• YouTube Kids canale video di Google dedicato ai bambini, si possono settare i contenuti visualizzabili in base alle fasce d'età. • Siti di giochi interattivi proposti dai docenti • Eseguire percorsi su grandi scacchierepavimento-griglie con robot educativi (Bee-Bot, Blue-Bot) • Codeweek • Schede didattiche e libri digitali

AREA DI COMPETENZA 3: CREAZIONE DI CONTENUTI DIGITALI			
DESCRITTORE DELLA COMPETENZA	OBIETTIVI	ATTIVITA' PROPOSTE	RISORSE SUGGERITE

3.1. Sviluppare contenuti digitali 3.2. Integrare e rielaborare contenuti digitali 3.4 Programmazione	• Individuare e riconoscere immagini, foto e video presentati dall'insegnante. • Ascoltare, registrare e inviare un messaggio vocale, con la supervisione del docente. • Utilizzare emoticon per l'autovalutazione del proprio comportamento nelle interazioni online • Sperimentare semplici programmi o applicazioni di grafica	• Coding unplugged • Attività ludiche di orientamento per muoversi correttamente in: avanti, indietro, a destra e a sinistra su un tappeto a scacchiera • attività pratiche per imparare ad inserire comandi in ordine seguendo algoritmi; • Utilizzo di giochi didattici con drag and drop • Utilizzo di programmi e app di grafica	Coding: • CodyFeet, • CodyColor, • CodyRoby • ScratchJr ● code.org • Wardwall • Learningapps Grafica • Paint • App di disegno

	AREA DI COMPETENZA 4: SICUREZZA		
DESCRITTORE DELLA COMPETENZA	OBIETTIVI	ATTIVITA' PROPOSTE	RISORSE SUGGERITE
4.1 Proteggere i dispositivi 4.3 Proteggere la salute e il benessere; 4.4 Proteggere l'ambiente	• Utilizzare semplici procedure di protezione dei dispositivi precedentemente impostate dai docenti/genitori • Riconoscere le persone a cui fare riferimento in caso di pericolo; • Conoscere basilari norme sulla sicurezza per se stessi e per gli altri.	• Accedere ad un dispositivo mediante segno, impronta digitale, codice numerico • Imparare a distinguere le emozioni del virtuale da quelle del reale. • Riflettere, utilizzando infografiche o video, sui tempi e momenti di utilizzo dei media.	• Protezione e sicurezza su internet per bambini

AREA DI COMPETENZA 5: RISOLVERE PROBLEMI			
DESCRITTORE DELLA COMPETENZA	OBIETTIVI	ATTIVITA' PROPOSTE	RISORSE SUGGERITE

5.1 Risolvere problemi tecnici 5.3 Utilizzare in modo creativo le tecnologie digitali	• Individuare il livello della batteria dei dispositivi in utilizzo; • Regolare il volume e la luminosità; • Accendere e spegnere correttamente un dispositivo • Conoscere semplici software didattici • Conoscere le risorse della rete per la risoluzione dei problemi (visione di tutorial e video, ricerca guidata in rete..)	• Riconoscere su uno schermo le icone di sistema e ne conosce il significato; • Manipolare in modo creativo applicativi e giochi digitali	• Percorsi tecnologici (pavimento interattivo e unplugged)

SCUOLA PRIMARIA

AREA DI COMPETENZA 1: ALFABETIZZAZIONE SU INFORMAZIONI E DATI			
DESCRITTORE DELLA COMPETENZA	OBIETTIVI	ATTIVITA' PROPOSTE	RISORSE SUGGERITE
1.1 Navigare, ricercare e filtrare dati, informazioni e contenuti digitali 1.2 Valutare dati, informazioni e contenuti digitali 1.3 Gestire dati, informazioni e contenuti digitali	• Conoscere ed utilizzare alcune modalità di archiviazione delle informazioni • Trovare dati, informazioni e contenuti attraverso una ricerca guidata in rete • Organizzare, archiviare e recuperare dati e informazioni e contenuti in ambienti digitali • Salvare un documento o file in una cartella. • Avviare la procedura per stampare un documento	• Avviare all'utilizzo di un motore di ricerca • Individuare una specifica cartella sul desktop, aprirlo, visionarne il contenuto • Utilizzare correttamente la procedura per organizzare, salvare e stampare un file	• In rete con la testa • Ricerche maestre • Ti presento Windows • WordWall- Ricerche in rete • Symbaloo • Utilizzo di Drive, Office, Libreoffice

AREA DI COMPETENZA 2: COMUNICAZIONE E COLLABORAZIONE			
DESCRITTORE DELLA COMPETENZA	OBIETTIVI	ATTIVITA' PROPOSTE	RISORSE SUGGERITE

2.1 Interagire con gli altri attraverso le tecnologie 2.2 Condividere attraverso le tecnologie digitali 2.3 Sviluppare le competenze di cittadinanza tramite le tecnologie digitali 2.4 Sviluppare forme di collaborazione tramite le tecnologie digitali 2.5 Netiquette 2.6 Gestire l'identità digitale	• Conoscere la differenza tra diverse forme di comunicazione (telefonata, messaggi di testo, messaggi vocali, mail) • Conoscere diversi tipi di comunicazione (formale e informale) e il tipo di linguaggio da utilizzare. • Conoscere le diverse parti che compongono un messaggio (mittente, destinatario e oggetto) • Comunicare in una mail utilizzando un linguaggio appropriato (netiquette) • Utilizzare correttamente la propria identità digitale	• Consolidare la familiarità con la piattaforma della scuola. • Utilizzare i principali strumenti digitali per la comunicazione in piattaforma • Utilizzare la condivisione di un documento secondo varie modalità • Utilizzare lavagne digitali e raccoglitori multimediali • Applicare la netiquette in contesti comunicativi e di condivisione • Conoscere la propria "impronta digitale" • Creare e gestire un'identità digitale, fornendo solo i dati necessari	• L'impronta digitale • Attività di cittadinanza digitale • Linoit • Padlet • Symbaloo • Excalidraw • Applicazioni di Microsoft Office 365 • Whiteboard

AREA DI COMPETENZA 3: CREAZIONE DI CONTENUTI DIGITALI			
DESCRITTORE DELLA COMPETENZA	OBIETTIVI	ATTIVITA' PROPOSTE	RISORSE SUGGERITE

3.1 Sviluppare contenuti digitali 3.2 Integrare e rielaborare contenuti digitali 3.3 Copyright e licenze 3.4 Programmazione	• Individuare software e applicazioni utili in base al tipo di contenuto da creare • Utilizzare software e applicativi per la creazione di contenuti digitali • Saper gestire le regole di formattazione del testo basilari. • Completare la presentazione multimediale sulla base di un modello dato • Completare/costruire mappe concettuali utilizzando applicativi online • Saper scrivere semplici algoritmi di istruzioni, sia unplugged che digitale. • Conoscere l'esistenza dei diritti d'autore dei materiali reperibili on line (immagini, audio, video...)	• Scrivere in formato digitale un testo • Tradurre un racconto in un fumetto utilizzando applicativi online • Completare una breve presentazione utilizzando le strutture proposte • Partecipare ad attività di Codeweek o Ora del Codice • Codificare e decodificare istruzioni date mediante strumenti e materiali predisposti dal docente. • Riconoscere i simboli del copyright e individuarli in un contenuto online • Elaborare da un testo una mappa concettuale	• Anymaker • StoryJumper • BookCreator - • Canva • Ed Puzzle • Il copyright e il diritto d'autore • CodeWeek • L'ora del codice • CodyFeet, • CodyColor, • CodyRoby • ScratchJr • code.org • Utilizzo Foto e immagini – Il diritto d'autore • Flibook – animazioni online

AREA DI COMPETENZA 4: SICUREZZA			
DESCRITTORE DELLA COMPETENZA	OBIETTIVI	ATTIVITA' PROPOSTE	RISORSE SUGGERITE

4.1 Proteggere i dispositivi 4.2 Proteggere i dati personali e la privacy 4.3 Proteggere la salute e il benessere; 4.4 Proteggere l'ambiente	• Sapere che esistono diversi rischi associati all'uso delle tecnologie • Essere consapevole che molti servizi utilizzano le informazioni personali per filtrare messaggi pubblicitari • Utilizzare con sicurezza l'account scolastico per accedere alla piattaforma • Proteggere il dispositivo in uso e i contenuti digitali • Utilizzare le tecnologie nel rispetto dei miei diritti e di quelli altrui • Conoscere quali dati personali condivido quando accedo ad un servizio online	• Scoprire e saper leggere i termini di utilizzo dei servizi web • conoscere e rispettare i vari regolamenti scolastici sull'uso dei dispositivi e della rete a scuola • Scegliere password sicure • Utilizzare il proprio account scolastico nei device della scuola effettuando il logout al termine • Conoscere i dati personali e saperne preservare la sicurezza • Riconoscere i vari momenti di utilizzo del digitale durante la giornata e saperne limitare la quantità per preservare il proprio benessere e la propria salute. • Saper eliminare il proprio account dopo l'utilizzo su un dispositivo scolastico. • Eliminare le password salvate	• Segui le tracce digitali • Alla scoperta del Web • Cosa è internet • Cosa è Internet (schede didattiche) • Vivi Internet al meglio • Il potere delle Parole • Materiali didattici - Ludoteca • Impronta digitale • Space Shelter (proteggersi online) • Detective per un giorno • I super Errori nel Web • Proteggere i nostri dati

AREA DI COMPETENZA 5: RISOLVERE PROBLEMI			
DESCRITTORE DELLA COMPETENZA	OBIETTIVI	ATTIVITA' PROPOSTE	RISORSE SUGGERITE

5.1 Risolvere problemi tecnici 5.2 Identificare i bisogni e le soluzioni tecnologiche 5.3 Utilizzare in modo creativo le tecnologie digitali	• Riconoscere vari dispositivi e le loro parti fondamentali • Individuare semplici problemi tecnici nell'utilizzo dei dispositivi e delle tecnologie digitali • Utilizzare semplici software didattici di programmazione e coding • Utilizzare le risorse della rete per la risoluzione dei problemi (visione di tutorial e video, ricerca guidata in rete..)	• Denominare e distinguere correttamente le varie parti hardware e software dei dispositivi • Verificare le reti Wi-Fi disponibili e collegarsi alla piattaforma adeguata • Utilizzare piattaforme Cloud	• Il gioco della Rete • Computer: Hardware • Escape Room • Come si apre una cartella • Il device misterioso • Digital storytelling • Esploriamo il Web • Canva

SCUOLA SECONDARIA DI PRIMO GRADO

AREA 1: ALFABETIZZAZIONE SU INFORMAZIONI E DATI			
DESCRITTORE DELLA COMPETENZA	OBIETTIVI	ATTIVITA' PROPOSTE	RISORSE SUGGERITE
1.1 Navigare, ricercare e filtrare dati, informazioni e contenuti digitali 1.2 Valutare dati, informazioni e contenuti digitali 1.3 Gestire dati, informazioni e contenuti digitali	• Riconoscere le proprie esigenze di ricerca • Organizzare autonomamente ricerche di dati, informazioni e contenuti in ambienti digitali. • Effettuare una ricerca utilizzando le principali funzioni del browser • Confrontare e organizzare le informazioni tra due o più siti, selezionando le più pertinenti e vere. • Saper riconoscere i principali elementi hardware e software	• Conoscere ed utilizzare diversi motori di ricerca. • Ricercare le informazioni, utilizzando parole chiave e filtri di ricerca. • Individuare informazioni e riferimenti credibili e affidabili • Organizzare e archiviare contenuti digitali, mediante applicazioni cloud • Organizzare, da solo in modo collaborativo, l'ambiente di lavoro personale • Identificare in siti e blog gli argomenti di interesse. • Utilizzare la sintassi di ricerca avanzata per selezionare uno specifico tipo di file.	• Motori di ricerca • Focus Junior • Come usare Google per trovare informazioni • Fake News • Interland • Linoit • Symbaloo • Scovare le bufale • Principali piattaforme AI

AREA DI COMPETENZA 2: COMUNICAZIONE E COLLABORAZIONE			
DESCRITTORE DELLA COMPETENZA	OBIETTIVI	ATTIVITA' PROPOSTE	RISORSE SUGGERITE
2.1 Interagire con gli altri attraverso le tecnologie 2.2 Condividere attraverso le tecnologie digitali 2.3 Sviluppare le competenze di cittadinanza tramite le tecnologie digitali 2.4 Sviluppare forme di collaborazione tramite le tecnologie digitali 2.5 Netiquette 2.6 Gestire l'identità digitale	• Conoscere e gestire le varie opzioni di condivisione • Presentare in modo efficace i risultati di una ricerca • Utilizzare strumenti digitali per collaborare nella costruzione di risorse e compiti. • Utilizzare la tecnologia per migliorare la capacità critica e la capacità di porsi in modo costruttivo nelle relazioni con gli altri (virtuali e reali)	• Utilizzare correttamente e in modo autonomo l'account scolastico; • Inviare mail utilizzando le opzioni avanzate (mail di gruppo, Cc e Ccn, programmare ora di invio, inserire allegati) • Creare, condividere e lavorare su file (documenti, tabelle, fogli di calcolo, infografiche) • Modificare le impostazioni di condivisione in base al grado di libertà da assegnare. • Creare ed utilizzare form digitali per sottoporre sondaggi ai compagni. • Riconoscere ed applicare le principali regole di comportamento appropriato per la collaborazione online. • conoscere come scuole, banche e comuni organizzano l'accesso online	• Dati personali e altri dati • Clip Champ • Avatar Maker • La Netiquette: regole per scrivere • Consapevoli in rete • Canva • DigiPad • Timelinely • Prezi • Genially • Parole ostili

AREA DI COMPETENZA 3: CREAZIONE DI CONTENUTI DIGITALI			
DESCRITTORE DELLA COMPETENZA	OBIETTIVI	ATTIVITA' PROPOSTE	RISORSE SUGGERITE

3.1 Sviluppare contenuti digitali 3.2 Integrare e rielaborare contenuti digitali 3.3 Copyright e licenze 3.4 Programmazione	• Realizzare prodotti multimediali di vario genere individualmente e in modalità collaborativa. • Impartire ed interpretare istruzioni sulla base di una codifica concordata. • Registrarsi su un sito indicato dal docente per attività didattiche • Conoscere e rispettare i diritti d'autore. • Attribuire le fonti da cui si prende materiale online. • Realizzare semplici istruzioni utilizzando codici di programmazione	• Realizzare contenuti digitali come infografiche e presentazioni con attenzione alla grafica e al contenuto • Realizzare filmati e video con software e app • Realizzare podcast • Sperimentare applicativi e piattaforme di robotica • Conoscere ed utilizzare siti di realtà aumentata • Creare storie e far interagire i personaggi con cambi di scena e sfondi sincronizzati. • Partecipare a manifestazioni di coding e robotica • utilizzare in autonomia interfacce di programmazione • Creare una presentazione digitale, in autonomia o in collaborazione, con diversi contenuti multimediali. • Utilizzare programmi per realizzare costruzioni geometriche complesse (Geogebra)	• storymap • Storyjumper • Book creator • Storyboard That • Podcast • Creazione di poster / giornale / infografica con Canva • Genially • Book Creator - Istruzioni • Infografica sui diritti di autore • Interviste impossibili con Chat Animator ● Stop Motion: • Geogebra • LEGO® Education Professional Development • Piani di lezione con i prodotti LEGO First Lego League Kids Game Jam • Micro:Bit Pagina dei progetti • Pixabay immagini free • Creative Commons • Google Earthù • Realtà aumentata

	AREA DI COMPETENZA 4: SICUREZZA

DESCRITTORE DELLA COMPETENZA	OBIETTIVI	ATTIVITA' PROPOSTE	RISORSE SUGGERITE
4.1 Proteggere i dispositivi 4.2 Proteggere i dati personali e la privacy 4.3 Proteggere la salute e il benessere; 4.4 Proteggere l'ambiente	• Conoscere le regole per il rispetto delle aule e dei laboratori digitali • Conoscere e rispettare i regolamenti dell'Istituto sull'utilizzo del BYOD • Aver cura e rispetto dei propri strumenti digitali e di quelli altrui. • Individuare e saper spiegare modi per proteggere dispositivi e accessi digitali • Distinguere l'ambiente digitale da quello reale • Scegliere semplici modi per proteggere i dati e la privacy (Es: i rischi legati alla pubblicazione di immagini personali) • Riconoscere i rischi legati alla salute psicologica e fisica quando utilizzo il digitale	• Leggere il regolamento d'Istituto". • Conoscere e ricordare le credenziali dei propri o Account • Riflettere e discutere sul manifesto della comunicazione non ostile • Riflettere e identificare semplici modi per evitare rischi legati alla salute fisica (dipendenza da internet, disturbi visivi, disturbi dell'umore), creando prodotti multimediali di sintesi (es: infografica). • Analizzare con la classe e riconoscere i rischi legati ai social o all'uso eccessivo dei videogiochi. • Riflettere e discutere sulle emozioni suscitate durante l'utilizzo di un videogioco • Stabilire delle regole per un uso sano ed equilibrato dei media. • Distinguere contenuti appropriati o meno da condividere sulla piattaforma della scuola in modo da non danneggiare la propria e altrui privacy. • Sapere cosa è e come si crea un'identità digitale	• Come difendersi dal Pishing • Web reputation • Cybersecurity • Be Safe - Kit di Cittadinanza digitale • Usare internet in sicurezza • Sicurezza in rete • Crittografare i nostri dati • Agenda 2030 • Conseguenze climatiche • Polizia Postale – sezione approfondimenti • Generazioni connesse
	• Adottare semplici atteggiamenti sostenibili (usare funzioni di risparmio energetico...)	(Spid e identità sui social) • Comprendere come proteggere il profilo sui social distinguendo tra profilo pubblico e privato • Conoscere le modalità per denunciare eventuali problemi connessi alla rete. • Conoscere i punti salienti della normativa sul Cyberbullismo (L. 71/2017) • Riflettere insieme ai compagni sulle implicazioni di un uso esagerato dei videogiochi e social.	

	AREA DI COMPETENZA 5: RISOLVERE PROBLEMI	
DESCRITTORE DELLA COMPETENZA	OBIETTIVI	ATTIVITA' PROPOSTE E RISORSE SUGGERITE
5 .1 Risolvere problemi tecnici 5.2 Identificare i bisogni e le soluzioni Tecnologiche 5.3 Utilizzare in modo creativo le tecnologie digitali 5.4 Identificare i divari di competenze	• Individuare e risolvere i più comuni problemi tecnici nell'utilizzodei dispositivi. • Effettuare semplici controlli del sistema in uso. • Riconoscere fra le applicazioni quelle più adeguate alle esigenze di lavoro • Individuare le proprie esigenze e selezionare gli strumenti digitali adeguati.	• Animate • Creare Gif

2.3 - Il Kit Didattico

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

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

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

3.1 - Protezione dei dati personali e GDPR

La protezione dei dati personali delle persone fisiche costituisce un diritto fondamentale. L'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea e l'art. 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Le principali normative di riferimento sono il Regolamento Generale sulla Protezione dei Dati 2016/679 noto anche come GDPR, e il Dlgs 196/2003 conosciuto come Codice Privacy.

Il settore dell’istruzione è particolarmente impattato dalla tematica privacy in considerazione del fatto che gli Istituti Scolastici sono chiamati, necessariamente, a trattare un’enorme mole di dati personali.

Con l’entrata in vigore del GDPR è stato introdotto l’obbligo per ciascun Istituto scolastico di provvedere alla designazione di un Responsabile della protezione dei dati personali (RPD o DPO).

I principali obblighi in materia di protezione dei dati personali consistono nella definizione di un “organigramma privacy”, nel rilascio dell’informativa al momento della raccolta dei dati e nella tenuta di un registro dei trattamenti.

3.2 - Strumenti di comunicazione online (PUA)

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

3.3 - BYOD

La presente ePolicy conterrà indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l’uso

dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device"). Risulta infatti fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

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.

4.2 - 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

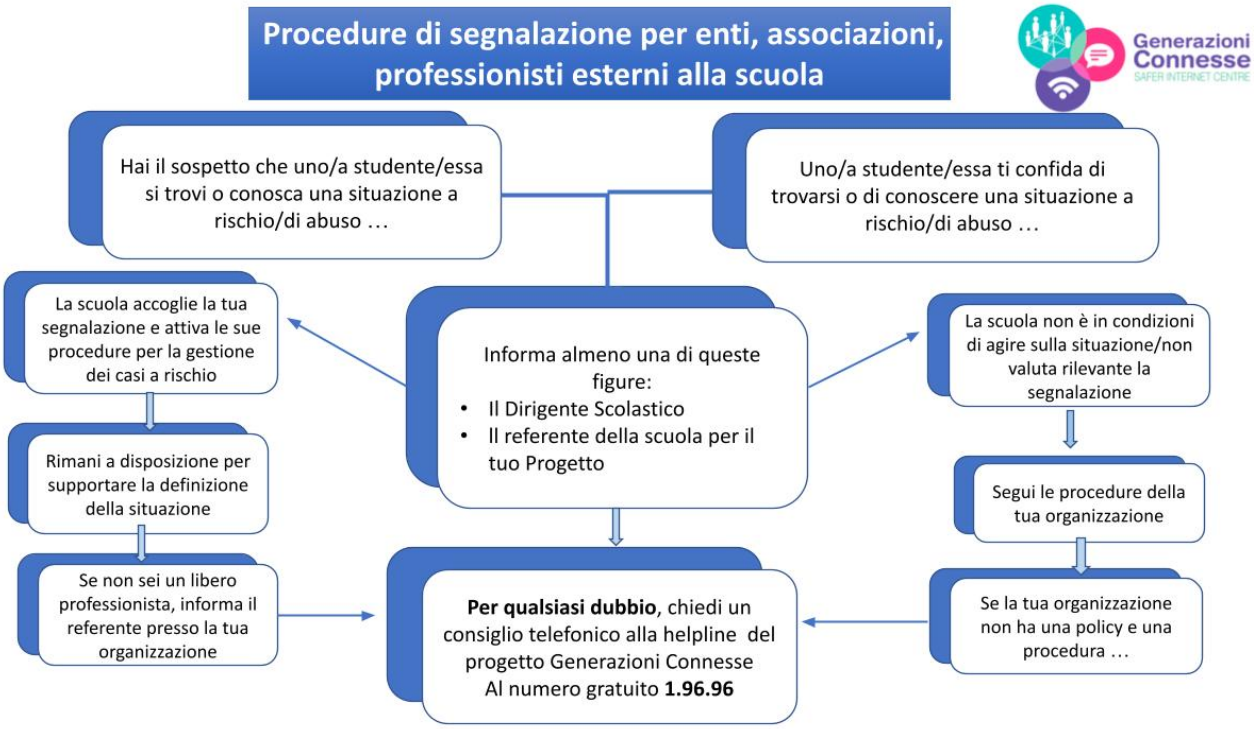
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

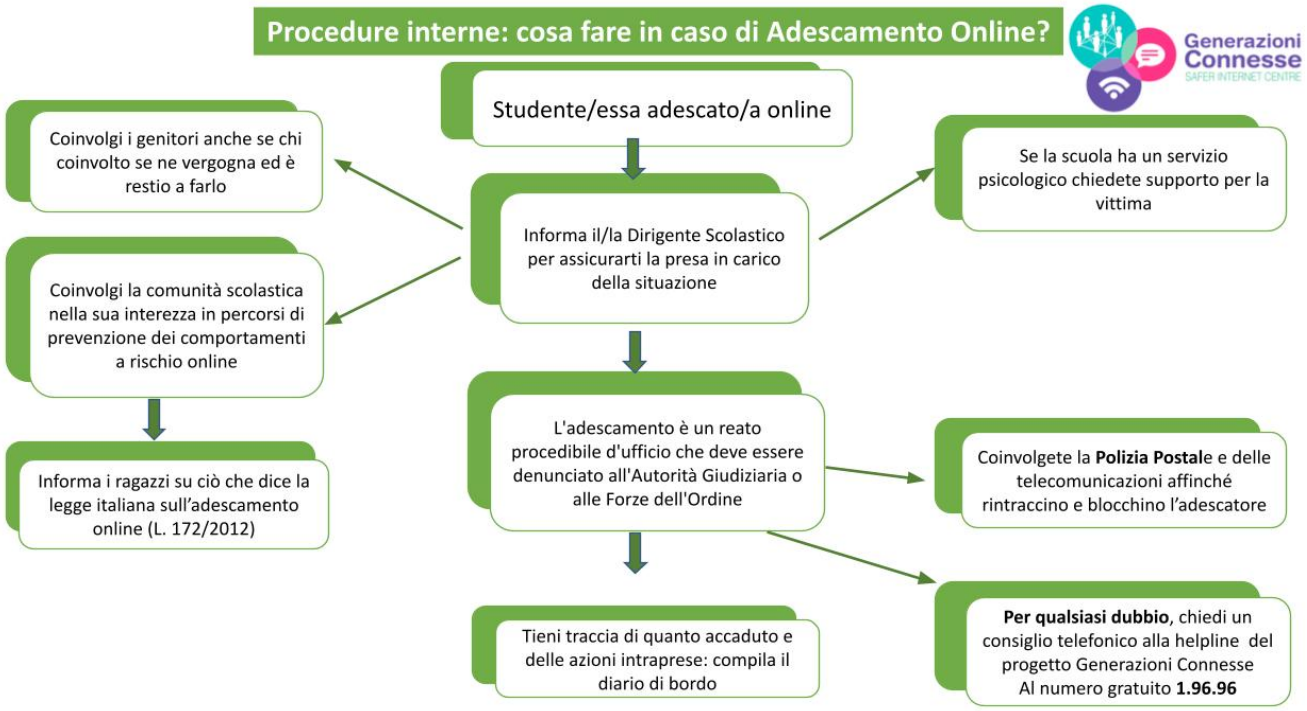
Se emergono evidenze passa allo schema successivo

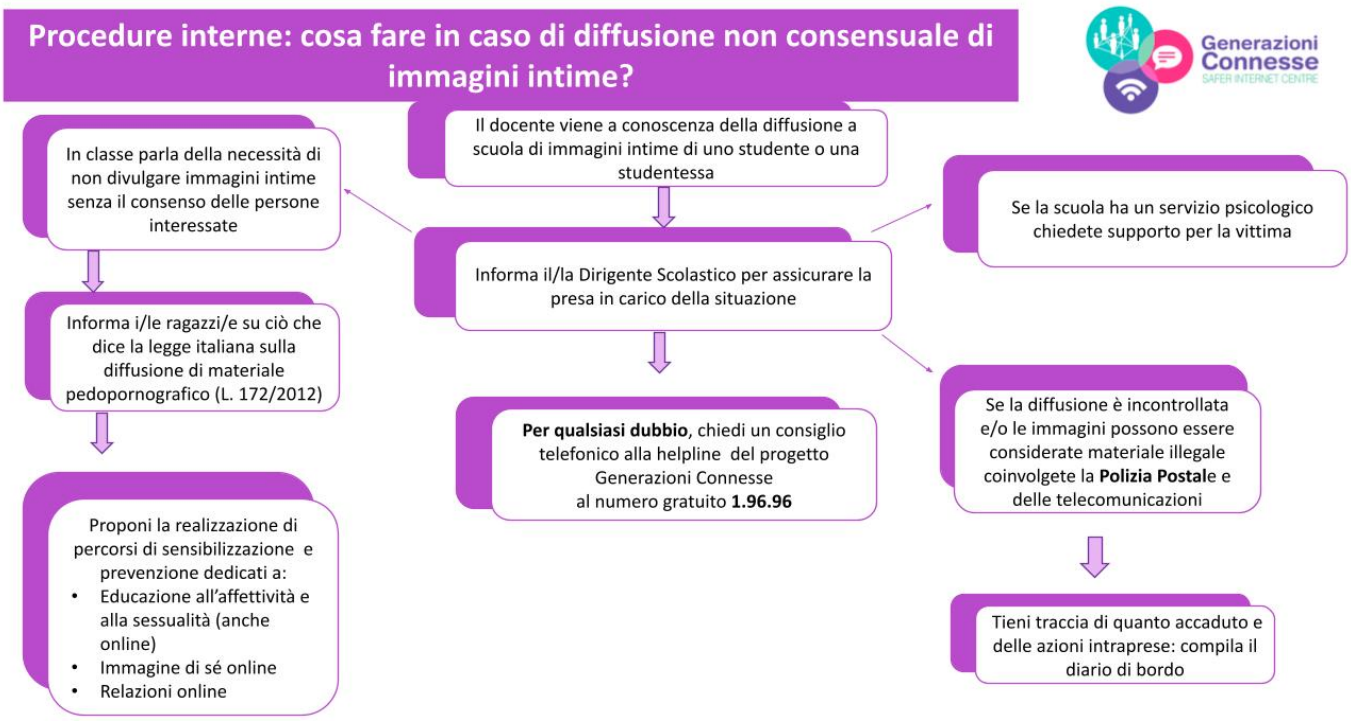
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

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


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


Procedure interne: cosa fare in caso di diffusione non consensuale di immagini intime?
In classe parla della necessità di non divulgare immagini intime senza il consenso delle persone interessate
Il docente viene a conoscenza della diffusione a scuola di immagini intime di uno studente o una studentessa
Se la scuola ha un servizio psicologico chiedete supporto per la vittima
Informa il/la Dirigente Scolastico per assicurare la presa in carico della situazione
Informa i/le ragazzi/e su ciò che dice la legge italiana sulla diffusione di materiale pedopornografico (L. 172/2012)
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse al numero gratuito 1.96.96
Se la diffusione è incontrollata e/o le immagini possono essere considerate materiale illegale coinvolgete la Polizia Postale e delle telecomunicazioni
Proponi la realizzazione di percorsi di sensibilizzazione e prevenzione dedicati a:
• Educazione all'affettività e alla sessualità (anche online)
• Immagine di sé online
• Relazioni online
Tieni traccia di quanto accaduto e delle azioni intraprese: compila il diario di bordo