



Documento di e-Policy

Liceo Scientifico Statale
“FILIPPO LUSSANA”
via Angelo Maj, 1
24121 - Bergamo (BG) - Lombardia

Data di approvazione: 25/06/2025

Delibera n.176

INDICE GENERALE

Capitolo 1 - Presentazione dell'e-Policy

- 1.1 Scopo dell'e-Policy e aspetti generali
- 1.2 Ruoli e responsabilità nell'implementazione dell'e-Policy
- 1.3 Integrazione dell'e-Policy nei documenti scolastici
- 1.4 Condivisione e comunicazione dell'e-Policy all'intera comunità educante
- 1.5 Monitoraggio dell'e-Policy e suo aggiornamento
- 1.6 I piani d'azione dell'e-Policy

Capitolo 2 - Formazione e curriculum

- 2.1 Curriculum sulle competenze digitali degli studenti
- 2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
- 2.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di internet e delle tecnologie digitali
- 2.4 Il kit didattico
- 2.5 Sensibilizzazione e prevenzione

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

- 3.1 Protezione dei dati personali e GDPR
- 3.2 Accesso a Internet e risorse ICT
- 3.3 Strumenti di comunicazione online PUA della rete
- 3.4 Dispositivi personali

Capitolo 4 - Segnalazione e gestione dei casi

- 4.1 Cosa segnalare
- 4.2 Come segnalare: quali strumenti e a chi
- 4.3 Allegati con Procedure

Cap. 1 - Presentazione dell'e-Policy

1.1 Scopo della e-Policy e aspetti generali

L'e-Policy ha come obiettivo quello di promuovere le competenze digitali per un uso delle tecnologie digitali intelligente, critico e consapevole da parte degli studenti e delle studentesse, guidati dagli adulti coinvolti nel processo didattico-educativo. Non meno importante è sviluppare nei giovani la comprensione delle opportunità e dei rischi di Internet, attraverso iniziative mirate.

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 <https://www.unicef.it/pubblicazioni/i-diritti-dei-minorenni-in-relazione-all-ambiente-digitale>).

L'e-Policy è un documento programmatico, strutturato 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), specificatamente in ambiente scolastico;
4. le misure per la **rilevazione, segnalazione e gestione delle situazioni rischiose**, legate ad un uso non corretto delle tecnologie digitali.

L'Istituto adotta il documento e-Policy come strumento operativo fondamentale per l'intera comunità educante.

L'e-Policy definisce le linee guida per il benessere online e stabilisce regole per l'uso delle Tecnologie dell'Informazione e della Comunicazione (TIC) a scuola. Essa costituisce la base per attività formative ed educative sulle e con le tecnologie digitali, oltre a campagne di sensibilizzazione per un utilizzo responsabile di tali tecnologie.

A questo scopo, l'Istituto adotterà una strategia integrata e globale, attenta alle specifiche esigenze, alle difficoltà e alle domande di aiuto, anche quelle meno esplicite, di ogni studente. Solo un ascolto costante e serio delle richieste degli alunni permetterà di attuare una politica di prevenzione efficace.

Questa politica si basa sull'identificazione e sulla gestione tempestiva di situazioni potenzialmente a rischio, avvalendosi degli strumenti già in dotazione all'Istituto, come il Regolamento per la prevenzione e la lotta al bullismo e al cyberbullismo, consultabile sul sito web della scuola (<https://www.liceolussana.edu.it/wp-content/uploads/2025/03/REGOLAMENTO-BULLISMO.docx.pdf>) e parte integrante del Regolamento d'Istituto.

Inoltre, la presente e-Policy, contiene indicazioni ed eventuali integrazioni ai 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 dotarsi di una regolamentazione condivisa e specifica che tenga in considerazione di eventuali criticità nella e per la didattica.

A tal proposito la scuola ha appena realizzato una propria Politica di Utilizzo Accettabile (PUA) riguardo i dispositivi personali degli studenti utilizzati a scuola da sottoporre alle famiglie per la sottoscrizione.

Tale PUA è allegata al presente documento ed è pubblicata sul sito della scuola.

L'e-Policy di Istituto, ossia il presente documento, è soggetto a revisioni ed aggiornamenti annuali, e sarà sottoposto all'attenzione dei competenti Organi Collegiali.

1.2 Ruoli e responsabilità nell'implementazione dell'e-Policy

Affinché l'e-Policy sia davvero uno strumento operativo efficace per la scuola e per tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, si impegni nell'attuazione e nella promozione di questo progetto. È opportuno che nel documento vengano definiti con chiarezza ruoli, compiti e responsabilità di ciascuna delle figure che operano all'interno dell'Istituto.

1.2.1 - 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 e-Policy;
- promuovere la cultura della sicurezza online – anche attraverso il documento di e-Policy - integrandola e inserendola nelle misure di sicurezza più generali dell'intero Istituto;
- fornire sistemi per un uso sicuro delle TIC, di Internet, dei suoi strumenti e ambienti, garantendo alla popolazione scolastica la sicurezza di navigazione, tramite internet e utilizzando adeguati sistemi informatici e filtri;
- assumere la responsabilità della gestione dei dati e della sicurezza delle informazioni e garantire che l'Istituto segua le pratiche migliori possibili, nella gestione dei dati stessi;
- tutelare la scuola e garantire agli utenti la sicurezza di navigazione, utilizzando adeguati sistemi informatici e servizi di filtri Internet.

Inoltre, il Dirigente Scolastico:

- 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;
- è responsabile della valutazione dei rischi associati all'uso degli strumenti digitali, assicurando l'adozione di misure preventive in linea con la normativa vigente;
- 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.

1.2.2 - 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 e-Policy, dell'attuazione dei piani di azione, con particolare riferimento alla formazione dei docenti. Tali figure sono inoltre responsabili del controllo all'accesso da parte degli studenti delle TIC.

1.2.3 - Il referente per il bullismo e cyberbullismo

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

1.2.4 - 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 dei fenomeni del bullismo e del cyberbullismo, attraverso progetti d'Istituto che

coinvolgano genitori, studenti e tutto il personale; comunica ad alunni, famiglie e a tutto il personale scolastico dell'esistenza del team, a cui fare riferimento per segnalazioni o richieste di informazioni o di aiuto sul fenomeno in oggetto. Nello specifico il Team ha il compito di:

- coadiuvare il Dirigente scolastico, coordinatore del Team, nella definizione degli interventi di prevenzione di bullismo cyberbullismo (per questa funzione partecipano anche il presidente del Consiglio d'Istituto e i Rappresentanti degli studenti);
- intervenire (come gruppo ristretto, composto da Dirigente e referente, o referenti, per il bullismo e il cyberbullismo, psicologo o pedagogo, se presente a scuola) nelle situazioni conclamate di bullismo;
- promuovere l'applicazione della e-Policy e monitorare le segnalazioni.

1.2.5 - I docenti

I docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC (Tecnologie della Comunicazione e dell'Informazione) 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 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 e informazioni personali, ad abbandonare un sito dai contenuti che possono turbare o spaventare, a non incontrare persone conosciute in Rete, senza averne prima parlato con i genitori. Informano in forma critica e consapevole gli alunni sui rischi presenti in Rete, sollecitandone un uso consapevole, in modo che Internet possa rimanere per ragazzi e ragazze una fonte di divertimento e uno strumento di apprendimento.

I docenti osservano con attenzione 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.

1.2.6 - Responsabile della protezione dei dati

Il Responsabile della protezione dei dati (RPD o DPO) conosce l'e-Policy di Istituto, fornisce la propria consulenza in merito agli obblighi derivanti dal GDPR e sorveglia circa l'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.

1.2.7 - 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'e-Policy di Istituto - ed è tenuto alla segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.

1.2.8 - Le studentesse e gli studenti

Le studentesse e gli studenti devono, in relazione al proprio grado di maturità e consapevolezza, utilizzare consapevolmente le tecnologie digitali, in coerenza con quanto richiesto dai docenti. Con il supporto della scuola, gli alunni devono imparare a tutelarsi online, tutelare i propri compagni e rispettarli. Perché questo accada, gli studenti devono partecipare attivamente a progetti e attività sull'uso positivo delle TIC e della Rete; devono farsi promotori di quanto appreso, anche attraverso possibili percorsi di *peer education*. I rappresentanti degli studenti sono informati del documento di e-Policy e invitati a costruire i piani di azione, a partire dal secondo anno di Liceo (della secondaria di II grado).

1.2.9 - 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 in relazione all'uso responsabile degli strumenti personali (smartphone, pc, 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 – ivi incluso il documento di e-Policy; devono

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 i genitori accettino e condividano quanto scritto nell'e-Policy d'Istituto, nel patto di corresponsabilità e nella PUA dei dispositivi personali, in un'ottica di collaborazione reciproca. Si promuove così il coinvolgimento dei rappresentanti di genitori/adulti di riferimento, all'interno del percorso di definizione e implementazione dell'e-Policy.

1.2.10 - Gli enti esterni pubblici e privati e le associazioni

Gli Enti esterni, pubblici e privati, e 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 a valutare la rispondenza delle proposte di attività di sensibilizzazione/formazione coerenti con gli standard qualitativi dell'e-Policy. Dovranno inoltre promuovere comportamenti sicuri, durante le attività che si svolgono con gli/le studenti/esse, e verificare di aver attivato una serie di misure finalizzate a garantire la tutela dei minori, nel caso di insorgenza di problematiche, e ad assicurarne la tempestiva individuazione e segnalazione.

1.3 Integrazione e-Policy nei documenti scolastici

La trasversalità dell'e-Policy 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'e-Policy, 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'e-Policy e alla PUA relativa ai dispositivi personali, 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 consapevole e costruttiva 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 e-Policy.

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, così il patto di corresponsabilità rappresenta l'assunzione di responsabilità da parte di tutti coloro che svolgono un ruolo attivo nella Comunità educante.

Il Regolamento d'Istituto e il Patto di Corresponsabilità Educativa vengono costantemente aggiornati, integrando specifici riferimenti all'e-Policy. Tale adeguamento è realizzato in linea con le Direttive del MIUR e le normative generali vigenti in materia.

1.4 Condivisione e comunicazione dell'e-Policy all'intera comunità educante.

I due aspetti fondamentali che riguardano la condivisione dell'e-Policy di Istituto sono:

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'e-Policy 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. Il documento è pubblicato sul sito della scuola con tutti i relativi allegati (PUA e regolamenti) e sarà inserito nel Patto di corresponsabilità.

2. **Come comunicare e condividere l'e-Policy 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'e-Policy 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'e-Policy è inserita all'interno delle attività didattiche dell'educazione alla cittadinanza, è pubblicata sul sito della scuola ed è inserita nel Patto di corresponsabilità.

1.5 Monitoraggio dell'implementazione della e-Policy e suo aggiornamento

L'e-Policy viene aggiornata con cadenza annuale e/o in occasione di cambiamenti significativi relativi all'uso delle tecnologie digitali all'interno della scuola o all'adozione di nuove disposizioni normative nazionali. Le eventuali modifiche al documento saranno discusse con tutti i membri coinvolti. Il gruppo responsabile del riesame e dell'aggiornamento è composto dal Dirigente Scolastico, dal Team Digitale e dal Referente d'Istituto.

Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia rispetto agli obiettivi specifici che si propone, e potrà essere attuato in una o più delle seguenti modalità:

1. somministrazione annuale di questionari a studenti, docenti e famiglie sull'uso consapevole delle TIC;
2. raccolta dati da segnalazioni online (modulo dedicato sul sito dell'Istituto);
3. analisi delle note disciplinari sul registro elettronico legate all'uso scorretto delle tecnologie;
4. report annuale del Team Digitale e del Referente per il bullismo/cyberbullismo;
5. riunioni periodiche di riesame con i rappresentanti di classe e di Istituto.

1.6 I Piani di Azione dell'e-Policy

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 e-Policy 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:

1. la rilevazione dei bisogni;
2. le iniziative informative e formative;
3. la formazione di docenti, studenti e studentesse, e famiglie;
4. il monitoraggio e la valutazione delle azioni (laddove possibile, anche all'interno del RAV).

I Piani di Azione, che emergono dal presente documento, sono definiti dalla scuola sulla base del proprio contesto territoriale e delle collaborazioni in essere con Istituzioni, associazioni e aziende e saranno rivisti e aggiornati ogni volta che lo si riterrà necessario.

1° anno di attività con l'e-Policy

Nel primo anno di attività gli obiettivi principali sono quelli di Integrare l'e-Policy con i documenti di Istituto, informare al meglio la comunità scolastica ed effettuare una rilevazione dei bisogni.

Nello specifico le azioni previste nel primo anno:

1. integrare l'e-Policy (norme, regolamenti e procedure) nei documenti dell'Istituto quali il Regolamento di Istituto, il PTOF e il Patto di Corresponsabilità;
2. approvare e far sottoscrivere alle famiglie la Politica d'Uso Accettabile (PUA) circa i dispositivi personali della scuola e promuovere le linee guida del MIUR per le politiche attive di BYOD (Bring Your Own Device);
3. rendere maggiormente accessibili regolamenti e modulistica relativi all'e-Policy con una sezione dedicata sul sito del liceo;
4. realizzare un evento di presentazione dell'e-Policy ai docenti dell'Istituto, a studenti/esse e alle famiglie;
5. diffusione dell'e-Policy in occasione degli Open Day e/o in occasione di momenti di apertura della scuola alle famiglie ed a studenti/esse;
6. effettuare una rilevazione del fabbisogno formativo dei docenti sui temi dell'educazione civica digitale;
7. effettuare una rilevazione di interessi, bisogni e comportamenti delle famiglie sull'uso positivo del digitale;
8. effettuare una rilevazione di interessi, bisogni, comportamenti, abitudini di studenti e studentesse sui temi dell'educazione civica digitale;
9. avviare l'introduzione del kit didattico, sviluppato da generazioni connesse, come metodo e risorsa di lavoro in alcune classi che intendono sperimentare;
10. realizzare una versione sintetica dell'e-Policy, che riassume procedure e regolamenti, avvalendosi di un linguaggio accessibile a tutti;
11. realizzare una reportistica delle segnalazioni ricevute e dei relativi esiti previa implementazione di una modulistica online.

2° anno di attività con l'e-Policy

Nel secondo anno di attività gli obiettivi principali sono quelli di realizzare un piano formativo per la comunità scolastica sulla base dei risultati della rilevazione svolta nel corso del primo anno e di diffondere la cultura digitale sicura e la conoscenza delle regole.

Le azioni previste nel secondo anno:

1. formazione rivolta ai docenti, agli studenti ed alle famiglie, sulla base dei risultati della rilevazione svolta nel corso del precedente anno, attraverso il supporto di esperti/associazioni esterne o avvalendosi del percorso disponibile sul sito di Generazioni Connesse;
2. organizzazione di un concorso creativo ("Posta bene!") rivolto a studenti: realizzazione di poster, meme, video o slogan sull'uso consapevole della rete, da diffondere nella scuola;
3. incontri con la Polizia Postale o altre associazioni locali su cyberbullismo, fake news, uso consapevole dei social;
4. progetto "Studenti Digital Mentor": selezione e formazione di un gruppo di studenti tutor che aiutino i compagni più piccoli nell'uso corretto della rete;
5. laboratori pratici di educazione digitale integrati nelle ore di Educazione Civica (es. riconoscere una fake news, costruire una password sicura, conoscere il cyberbullismo);
6. realizzazione di podcast o video a cura degli studenti che trattino le linee di comportamento sicure in situazioni problematiche relative alla rete;
7. progettare e organizzare "la giornata della disconnessione" un momento condiviso tra docenti e studenti in cui per un giorno si rinuncia all'accesso alla rete e si promuovono iniziative di socializzazione.

3° anno di attività con l'e-Policy

Nel terzo anno di attuazione dell'e-Policy d'Istituto, gli obiettivi principali sono il consolidamento, il monitoraggio e il miglioramento delle pratiche già avviate. Si intende rafforzare quanto costruito nei precedenti anni, garantendo la continuità e la coerenza delle azioni intraprese in tema di cittadinanza digitale, sicurezza online e uso consapevole delle tecnologie. Il monitoraggio costante delle attività permetterà di individuare punti di forza e aree critiche, mentre il miglioramento continuo sarà orientato all'aggiornamento delle strategie educative e organizzative, in linea con l'evoluzione del contesto digitale e dei bisogni della comunità scolastica.

Le azioni previste nel terzo anno:

1. aggiornamento dell'e-Policy sulla base dei feedback ricevuti con il coinvolgimento di docenti e studenti;
2. organizzazione di un evento di restituzione del lavoro: giornata aperta alla comunità scolastica con presentazione dei progetti realizzati, premiazioni ed interventi di esperti del settore;
3. costituzione di un "Team Digitale Studenti" permanente per mantenere viva l'attenzione ai temi della cittadinanza digitale anno dopo anno;
4. realizzazione di un sondaggio finale tra studenti, docenti e famiglie per valutare i cambiamenti nel comportamento digitale all'interno della scuola.

Cap 2 - Formazione e curriculum

2.1 Curriculum sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali". Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società". Essa comprende: l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico" ("Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente", C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse ad un uso consapevole e responsabile delle tecnologie digitali.

Ciò avverrà attraverso la progettazione ed **implementazione di un curriculum digitale**.

Il curriculum verticale relativo alle competenze digitali è in corso di definizione puntuale.

In linea generale sarà orientato al raggiungimento dei due obiettivi fondamentali:

1. apprendere l'uso attento e responsabile delle TIC;
2. responsabilizzare gli studenti davanti alla scelta dei comportamenti da assumere durante l'utilizzo delle TIC nei vari contesti d'impiego;

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 all'Istituto non solo agli studenti.

Tale cornice trova poi sviluppo specifico, per gli studenti, nel curriculum di educazione alla Cittadinanza Digitale previsto dalla L. 92/2019 che introduce l'insegnamento trasversale dell'Educazione Civica e che dedica un intero articolo, il 5, alla Cittadinanza Digitale.

Il nostro Liceo, recependo il dettato normativo, elaborerà un curriculum d'Istituto nel quale troverà spazio l'educazione e lo sviluppo delle competenze digitali non solo come conoscenza tecnica degli strumenti ma soprattutto come uso consapevole, critico e responsabile delle tecnologie digitali.

2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

Il piano di formazione dei docenti sull'utilizzo delle TIC nella didattica, già avviato con i fondi del PNRR, prevede una parte dedicata all'alfabetizzazione digitale e una dedicata alla formazione metodologica.

1. **Alfabetizzazione digitale:** attività formative mirate allo sviluppo delle competenze digitali relative alle aree informazione, comunicazione e creazione di contenuti del Digcomp 2.1;
2. **Formazione metodologica:** attività formative e ricerca-azione dei docenti sulle metodologie didattiche innovative mirate al superamento della didattica trasmissiva (v. adesione a Generazioni connesse e la piattaforma eTwinning).

Ai docenti sarà offerta la possibilità di usufruire di attività formative organizzate dalla scuola e tenute da personale interno con adeguate competenze (es. Animatore Digitale e Membri del Team per l'Innovazione), o di partecipare alle proposte formative offerte da altre scuole, anche in rete. È prevista anche la possibilità di autoaggiornamento.

2.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

Saranno previsti inoltre percorsi di formazione e/o autoaggiornamento sulla piattaforma di "Generazioni connesse"; momenti seminariali ed eventi che la scuola organizza anche in accordo con scuole presenti sul territorio e con la collaborazione delle Forze di Polizia.

2.4 Le risorse ed 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 sulle programmazioni scolastiche (etica e digitale, algoritmi...). A tal fine si ritiene utile predisporre 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 grado 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 ed ha lo scopo di inquadrare il corpus di temi e contenuti che sono alla base dello sviluppo di una piena cittadinanza digitale degli e delle studenti, attraverso dei solidi percorsi educativi che intendono guidare l'insegnante nella realizzazione di un vero e proprio laboratorio di educazione civica digitale all'interno della propria classe.

È possibile reperire il materiale <https://www.generazioniconnesse.it/site/it/il-kit-didattico/>

2.5 Sensibilizzazione e prevenzione

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'e-Policy 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. I regolamenti e le attività sviluppate sul tema della prevenzione presenti nell'e-Policy sono parte, costante ma non esclusiva, delle azioni di disseminazione e sensibilizzazione descritte ed attuate dall'Istituto.

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e ad un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura.

L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'e-Policy e dal suo piano di azioni. La scuola, consapevole dell'importanza del coinvolgimento dei genitori nella educazione digitale dei propri figli, sensibilizza le famiglie attraverso la documentazione informativa, i Regolamenti scolastici, il Patto di corresponsabilità, e l' e-Policy al fine di far comprendere i principi che devono regolare l'utilizzo corretto delle TIC.

A tal proposito la scuola si propone di:

1. presentare ai genitori il regolamento dell'e-Policy ed informarli sulla presenza di una sezione dedicata sul sito della scuola;
2. favorire incontri con esperti per potenziare le conoscenze e l'uso dei linguaggi di comunicazione ed il funzionamento del web;
3. promuovere e sviluppare l'utilizzo creativo della rete e delle tecnologie in forma di apprendimento cooperativo, valorizzando le attività di gruppo come occasione di scambio e negoziazione di attitudini, conoscenze e capacità diverse;
4. approfondire le tematiche relative al rapporto adolescenti e nuove tecnologie;
5. far acquisire agli studenti strumenti specifici sulle tematiche critiche come bullismo e cyberbullismo, privacy sul web e sexting e di informarli sulle implicazioni giuridiche e psicologiche.

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») stabilisce che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Le principali normative di riferimento sono il Regolamento Generale sulla Protezione dei Dati

2016/679 noto anche come GDPR, e il Dlgs 196/2003 conosciuto come Codice Privacy.

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

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

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

La nostra scuola:

1. garantisce la tutela in generale della privacy degli studenti ([Regolamento per l'individuazione e il trattamento dei dati sensibili](#));
2. ha sottoscritto un'Informativa per il trattamento dei dati personali effettuati sul sito Web (art. 13 del Reg. UE 2016/679) e ha realizzato il sito (<https://www.liceolussana.edu.it/>), con l'obiettivo di pubblicare dati e documenti relativi alla propria struttura, attività, provvedimenti e servizi nonché di fornire informazioni ai cittadini sulla propria attività (v. le [Note legali relative all'utilizzo del Sito](#));
3. individua e definisce le misure di tutela, le modalità per garantirne nel tempo la continuità e l'adeguatezza e le responsabilità per la gestione dei dati: titolare, responsabile, persone autorizzate al trattamento;
4. ha redatto il [Regolamento per l'adeguamento al GDPR](#) (Reg. UE 2016/679) e per l'impostazione di un Sistema per la Gestione della Sicurezza delle Informazioni; l'[Informativa privacy ex artt. 13 e 14 del Regolamento Europeo 2016/679 \(prove INVALSI\)](#);
5. l'Istituto rispetta la privacy dei propri utenti e si impegna a proteggere i dati personali che gli stessi conferiscono all'istituzione, a trattarli in conformità alla normativa vigente. In caso di raccolta di dati personali, l'istituzione informerà l'utente sulle finalità della raccolta al momento della stessa, ove necessario, richiede il consenso dell'utente. L'Istituto non comunicherà i dati personali dell'utente a terzi senza il consenso dello stesso. Se l'utente decide di fornire alla scuola i propri dati personali, la scuola potrà comunicarli all'interno dell'Istituto o a terzi che prestano servizi alla scuola, solo rispetto a coloro che hanno bisogno di conoscerli in ragione delle proprie mansioni, e, ove necessario, con il permesso dell'utente.

Infine, facendo riferimento a tutto quanto previsto dal Decreto legislativo 30 giugno 2003, n. 196 (c. d. Codice della Privacy), sono individuate le seguenti linee guida di e-safety:

1. i video e le fotografie raccolte dai genitori durante le pubbliche attività scolastiche non violano la privacy. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione. Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime su Internet e sui social network in particolare. In caso di diffusione diventa necessario, di regola, ottenere il consenso informato delle persone presenti nelle fotografie e nei video. Si deve quindi prestare attenzione prima di caricare immagini e video sui social network, oppure di diffonderle attraverso sistemi di messaggistica istantanea. Tale pratica può dar luogo a gravi violazioni del diritto alla riservatezza delle persone riprese, e fare incorrere in sanzioni disciplinari, pecuniarie e in eventuali reati;
2. l'utilizzo di telefoni cellulari, di apparecchi per la registrazione di suoni e immagini, quando autorizzato dai docenti, è consentito, ma esclusivamente per fini personali, e sempre nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte (siano essi studenti o professori) in particolare della loro immagine e dignità;
3. la scuola ha la possibilità di regolare o di inibire l'utilizzo di dispositivi elettronici all'interno delle aule o laboratori. Gli studenti e gli altri membri della comunità scolastica, in ogni caso, non possono diffondere o comunicare sistematicamente i dati di altre persone (ad esempio pubblicandoli su Internet) senza averle prima informate adeguatamente e averne ottenuto l'esplicito consenso. Si veda vademecum Garante della Privacy.

3.2 Accesso a internet e risorse ICT

1. L'accesso a Internet è un diritto fondamentale della persona e una condizione per il suo pieno sviluppo individuale e sociale.
2. Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.
3. Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.
4. L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.
5. Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 entra in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le “misure riguardanti l'accesso a un Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione”.

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente, il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di “fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il “diritto a Internet” diventi una realtà, a partire dalla scuola”.

Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola. Per quanto riguarda l'accesso alla Rete, Il liceo Lussana dispone di una connessione a Internet in fibra ottica a 1Gbps fornita dalla società Intred. Si è provveduto al cablaggio interno di tutti gli spazi della scuola (LAN/W-Lan). Sono state configurate diverse reti WIFI per consentire l'accesso alle diverse tipologie di utenti: wifi-Docenti e wifi-studenti.

L'autorizzazione all'accesso alla rete WIFI dell'Istituto viene concessa a tutto il personale in servizio, agli studenti delle classi digitali e a quelli che ne fanno richiesta per esigenze legate allo svolgimento di particolari attività/progetti. L'accesso viene consentito anche a personale esterno che svolge specifiche attività all'interno dell'Istituto (es. esperti esterni, educatori, ecc.).

L'Istituto è registrato alla piattaforma Microsoft Office 365, a contratto triennale a carico della scuola tramite fondi PNRR: questo consente ai destinatari di utilizzare le funzionalità dell'ambiente online Microsoft 365, per il lavoro collaborativo nelle classi e di scaricare e utilizzare in locale il pacchetto MS Office.

L'Istituto fornisce a studenti e docenti che abbiano un account istituzionale licenze d'uso online o di download del software MATLAB di Mathworks con canone annuo a carico della scuola, dell'antivirus WithSecure e della piattaforma Adobe Creative Cloud.

L'Istituto Lussana dispone di 3 laboratori di informatica, un'aula comunicazione, un'aula di disegno, un laboratorio di lingue e un'aula di robotica. I laboratori mobili sono 6 e sono situati: 2 in aula di robotica, 1 in biblioteca, 1 in aula di disegno e 1 al primo piano e 1 al secondo piano dell'edificio 2 e dispongono di tablet e/o pc. Ogni aula è dotata di monitor interattivo collegato alla Rete.

La scuola fornisce al personale e agli studenti un indirizzo di posta elettronica personale, attivo per il tempo di permanenza nell'Istituto: l'indirizzo si può utilizzare per accedere alle piattaforme e tutte le altre attività ICT della scuola. È prevista la scadenza programmata dell'account entro il primo di ottobre dell'anno scolastico successivo al

diploma per gli studenti e di fine servizio per il personale scolastico (ad esempio per il personale assunto con contratto a tempo determinato).

Sono reperibili sul sito della scuola:

1. Il regolamento generale dei laboratori di informatica
2. Regolamento dei servizi informatici

Si adotta la seguente checklist per la cybersecurity:

1. Aggiornare periodicamente software e Sistema operativo: garantire che il sistema sia aggiornato lo protegge dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo
2. Definire la programmazione di backup periodici: cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi (possibilmente anche una copia offline)
3. Garantire formazione adeguata allo staff, incluso il corpo docenti: la formazione deve riguardare la gestione dei dispositivi, la conoscenza delle regole basilari sulla sicurezza
4. Testare regolarmente le possibili vulnerabilità
5. Predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo: se non è previsto uno standby, il dispositivo resta accessibile nel caso in cui qualcuno dimentichi di spegnerlo, con il rischio potenziale di accesso da parte di persone non autorizzate
6. Programmare l'eliminazione periodica di dati di navigazione, password inutilizzate ad eventuali documenti personali memorizzati
7. Definire una e-Policy delle password: le password devono essere forti: richiedere password complesse con almeno 8 caratteri, con cifre numeriche, maiuscole e minuscole e caratteri speciali
8. Sensibilizzare rispetto al non uso di password facilmente identificabili (nomi dei figli, compleanni, ecc.); Non memorizzare le password nei dispositivi scolastici
9. Non condividere le password con nessuno
10. Minimizzare i privilegi amministrativi: solo poche persone autorizzate dovrebbero avere privilegi amministrativi
11. Studenti e la maggior parte dei docenti possono accedere con account con permessi limitati
12. Sviluppare il regolamento sull'uso delle tecnologie a scuola deve riguardare chiunque abbia accesso alla Rete.

3.3 Strumenti di comunicazione online e politiche d'uso accettabile della rete.

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. Nella Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) vengono definite, dunque, le regole di utilizzo fra tutti gli attori in gioco, nel rispetto dei dati sensibili di ciascuno, in particolar modo degli alunni e delle alunne. L'Istituto ancora non dispone di una PUA delle rete puntuale ma si propone di realizzarla secondo i seguenti obiettivi:

1. **Garantire l'uso sicuro e responsabile della rete:**
Proteggere i membri della comunità scolastica da rischi online, come contenuti inappropriati o cyberbullismo.

2. Promuovere l'uso didattico e formativo:

Favorire l'utilizzo della rete per scopi educativi e di ricerca, incentivando la capacità di apprendere e comunicare.

3. Definire comportamenti accettabili:

Stabilire regole chiare per evitare l'uso improprio della rete, come la navigazione in siti vietati o il download di materiale illegale.

4. Educare al rispetto dei diritti d'autore:

Insegnare a riconoscere e rispettare i diritti d'autore, evitando il plagio o l'uso non autorizzato di contenuti online.

5. Garantire la privacy:

Proteggere i dati personali degli studenti e del personale, rispettando le normative sulla privacy.

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

I principali strumenti e canali di comunicazione adottati in Istituto sono:

1. Registro elettronico:

Le famiglie ricevono le credenziali per l'accesso riservato al registro elettronico Spaggiari, in cui il corpo docente è tenuto a registrare:

- assenze, valutazioni, note e osservazioni;
- risultati scolastici (voti, documenti di valutazione);
- prenotazioni colloqui individuali;
- eventi;
- comunicazione varie..

La pubblicazione delle informazioni attraverso tale strumento assolve l'obbligo di comunicare prontamente ed efficacemente ogni evento riguardante gli alunni.

2. Posta elettronica e indirizzi e-mail

I docenti e il personale amministrativo possono utilizzare i servizi e-mail accedendo alla rete della scuola a fini esclusivamente didattici. Gli stessi dispongono di un account G-Suite Google Education con estensione *@liceolussana.eu*. L'account è strettamente personale, per cui ogni utente dovrà avere cura di disconnettere il proprio accesso al termine del suo utilizzo. Lo spazio del proprio account è destinato alla ricezione di comunicazioni, all'invio di documentazione e alla condivisione di materiali, progetti didattici o progetti con altri docenti. Sono attivi gli account per gli studenti e, a discrezione dei docenti, sono create piattaforme di lavoro condiviso con Google Classroom per attività di e-learning.

Le comunicazioni tra personale scolastico, famiglie e studenti avvengono via mail o registro elettronico.

3. Sito della scuola

Il Dirigente Scolastico e il personale incaricato (in possesso di credenziali) hanno il compito di gestire il sito della scuola e la responsabilità di garantire che i contenuti pubblicati e i servizi siano accurati e appropriati.

3.4 Dispositivi personali

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

nella e per la didattica. I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/le studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

L'uso dei dispositivi personali in classe è normato dai seguenti regolamenti DPR n. 249/1998; DM n 30 del 15/03/2007; [Regolamenti d'Istituto e dal Regolamento di utilizzo dei servizi della G Suite for education, regolamento di Istituto per la prevenzione e il contrasto dei fenomeni di Cyberbullismo](#)

L'Istituto si propone inoltre di introdurre una PUA per i dispositivi personali utilizzati in ambito scolastico che gli studenti devono leggere e sottoscrivere.

Politica d'Uso Accettabile dei dispositivi personali.

Ogni alunno che utilizza un dispositivo mobile di proprietà personale all'interno della scuola deve leggere e firmare per accettazione la PUA :

1. Gli alunni si assumono la responsabilità per l'uso appropriato dei propri dispositivi in ogni momento. La scuola non è responsabile in alcun modo per il dispositivo o per il suo uso. I dispositivi, infatti, devono essere usati a scuola per soli scopi didattici e solo previa autorizzazione esplicita dell'insegnante. Non è consentito usare i dispositivi per scopi diversi da quelli didattici. Audio e video registrati a scuola a fini didattici possono essere pubblicati esclusivamente in canali di comunicazione interni all'I.C., ovvero nel rispetto delle liberatorie privacy firmate dalle famiglie.
2. Gli alunni/genitori/tutori sono responsabili dei propri dispositivi, comprese eventuali rotture, costi di riparazione o sostituzione. La scuola non è in alcun modo responsabile della sicurezza dei dispositivi e di eventuali danni. Gli studenti si impegnano a riportare a casa il dispositivo al termine delle lezioni. Nel caso in cui lo studente lasci a scuola il dispositivo, l'Istituto non sarà ritenuto responsabile per eventuali danneggiamenti o furti.
3. La scuola può ispezionare la memoria del dispositivo dello studente se ritiene che le regole scolastiche non siano state rispettate, questo comprende, ma non è limitato, a registrazioni audio e video, fotografie scattate nelle pertinenze scolastiche e che violano la privacy altrui, o ogni altra questione legata al bullismo o ad atti ritenuti offensivi e lesivi delle persone e delle istituzioni.
4. Non è consentito:
 - usare Internet per scopi diversi da quelli didattici;
 - scaricare musica, video e programmi da internet o qualsiasi file senza il consenso dell'insegnante;
 - giocare sul computer, in rete o diversamente (se non come parte di una lezione, sempre previa autorizzazione dell'insegnante);
 - accedere ai canali social.
5. I dispositivi mobili devono essere caricati prima di essere portati a scuola in modo da essere utilizzabili durante l'orario scolastico. Occorre essere consapevoli che:
 - non sarà possibile ricaricare i dispositivi in aula. A tal scopo si consiglia di dotarsi di caricabatteria portatili (power bank);
 - ogni alunno dovrà contrassegnare il proprio dispositivo con l'indicazione di nome, cognome e classe e il dispositivo dovrà essere protetto da una idonea custodia;
 - la famiglia avrà cura di fare in modo che il proprio figlio sia autonomo nell'accesso e nell'utilizzo del proprio dispositivo.
6. Gli studenti devono rispettare e proteggere la proprietà intellettuale altrui:
 - non è ammessa la copia o il plagio di qualsiasi materiale;
 - non è ammessa la violazione dei copyrights;

- si deve attribuire, citare e richiedere il permesso degli autori o creatori delle informazioni o dei media originali (se richiesto dalla legge);
- la scuola favorisce e incentiva lo sviluppo dell'open source e copyleft.

7. La scuola si riserva il diritto di cambiare il regolamento in linea con la politica generale della scuola pubblica italiana.

Cap 4 - Segnalazione e gestione dei casi

4.1 Cosa Segnalare

Questa sezione dell'e-Policy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse. Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. 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, news inserite nel sito della scuola e comunicazioni fornite durante il collegio docenti.

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

Cyberbullismo: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/le studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione). Si precisa che l'atto di cyberbullismo, nella sua peculiarità, può avvenire una sola volta, ma continuerà a danneggiare a lungo la vittima. Le diffamazioni o le altre vessazioni online, infatti, continuano a colpire, anche se la vittima cambia scuola o si chiude in casa, senza lasciare vie di fuga al soggetto colpito. Il cyberbullismo si configura, pertanto, come un fenomeno a rapida diffusione nei vari contesti di vita, in quanto chiunque può venire in contatto con il materiale diffamatorio. Questo costringe la vittima a restringere sempre di più la sua vita sociale, producendo così sofferenza ed emarginazione.

Può essere utile, valutando accuratamente ciascuna situazione, attivare colloqui individuali con tutti i minori coinvolti, siano essi vittime, testimoni e/o autori.

Il metodo di intervento, previsto dalla scuola, con l'obiettivo di eliminare la minaccia della punizione e stimolare nei responsabili dell'episodio di bullismo/cyberbullismo delle proposte di soluzione al problema, prevede le seguenti strategie comportamentali:

1. il colloquio iniziale con gli aggressori per ricostruire la dinamica dei fatti e responsabilizzare i bulli, circa le gravi conseguenze sulla vittima del loro comportamento violento ed aggressivo
2. il colloquio con la vittima
3. incontri periodici dell'insegnante sia con l'aggressore che con la vittima, per verificare lo svolgimento e l'evoluzione della vicenda

4. la mediazione dei Peer Educators (gli studenti della scuola selezionati per svolgere questo delicato compito, dotati di particolari abilità sociali e comunicative), per aiutare la vittima a raccontare e a condividere la violenza subita.
5. L'incontro finale di gruppo per la reintegrazione della vittima e la presa di coscienza dei fatti avvenuti.

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 minorenni e inoltre è importante non sostituirsi al minorenne, evitando, quindi, di rispondere all'adescatore al suo posto. È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. L'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, deve 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 rimuove i contenuti entro 48 ore.

Si suggeriscono, inoltre, i seguenti servizi:

1. Servizio di Helpline al numero di telefono gratuito 19696;
2. Chat di Telefono Azzurro per supporto ed emergenze;
3. STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

Strumenti di segnalazione

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, che saranno messi a loro disposizione:

1. un indirizzo e-mail cui rivolgersi in caso di bisogno;
2. una scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
3. uno sportello di ascolto con professionisti;
4. un docente referente per le segnalazioni;
5. un protocollo di segnalazione contenente le seguenti voci: tipologia dell'episodio; dinamica e descrizione del fatto; data e luogo dell'episodio; eventuale replica del fenomeno; numero degli studenti attivamente coinvolti; eventuale presenza di testimoni (studenti, insegnanti, personale scolastico, ecc.).

Strategie anti bullismo/cyberbullismo

L'intervento antibullismo si presenta come un approccio multifocale, in grado di agire su tutti i protagonisti.

Per ridurre i fenomeni di bullismo/cyberbullismo, oltre alla modulistica, la scuola mette in atto le seguenti strategie:

1. potenziamento delle vittime predestinate tramite insegnamento di abilità sociali e rafforzamento delle reti di appartenenza;
2. intervento sugli aggressori tramite attività di sensibilizzazione e di controllo;
3. riduzione dei complici tramite attività di responsabilizzazione;
4. riduzione degli spettatori passivi tramite attività che sviluppino empatia per la vittima.

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 e 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 Scolastico,
2. Docente referente,
3. Animatore Digitale (secondo il Piano Nazionale per la Scuola Digitale, 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:

1. Procure Ordinarie: nel caso in cui il minore/i sia la vittima/e e il presunto autore del reato sia maggiorenne;
2. Procura Minorile: in caso il presunto autore del reato sia minorenni.

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

La previsione di possibili incontri di mediazione tra i minori coinvolti va ponderata 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, segnalarli al Dirigente, o al docente coordinatore di classe o referente di Istituto oppure direttamente al team antibullismo attraverso apposita procedura che definisce l'Istituto (e-mail ad hoc, tramite gli uffici e postazioni specifiche, etc...).

Gli insegnanti e i genitori, come gli studenti e le studentesse, si possono rivolgere alla Helpline del progetto Generazioni Connesse, al numero di telefono gratuito 19696, attraverso la chat disponibile sul relativo 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

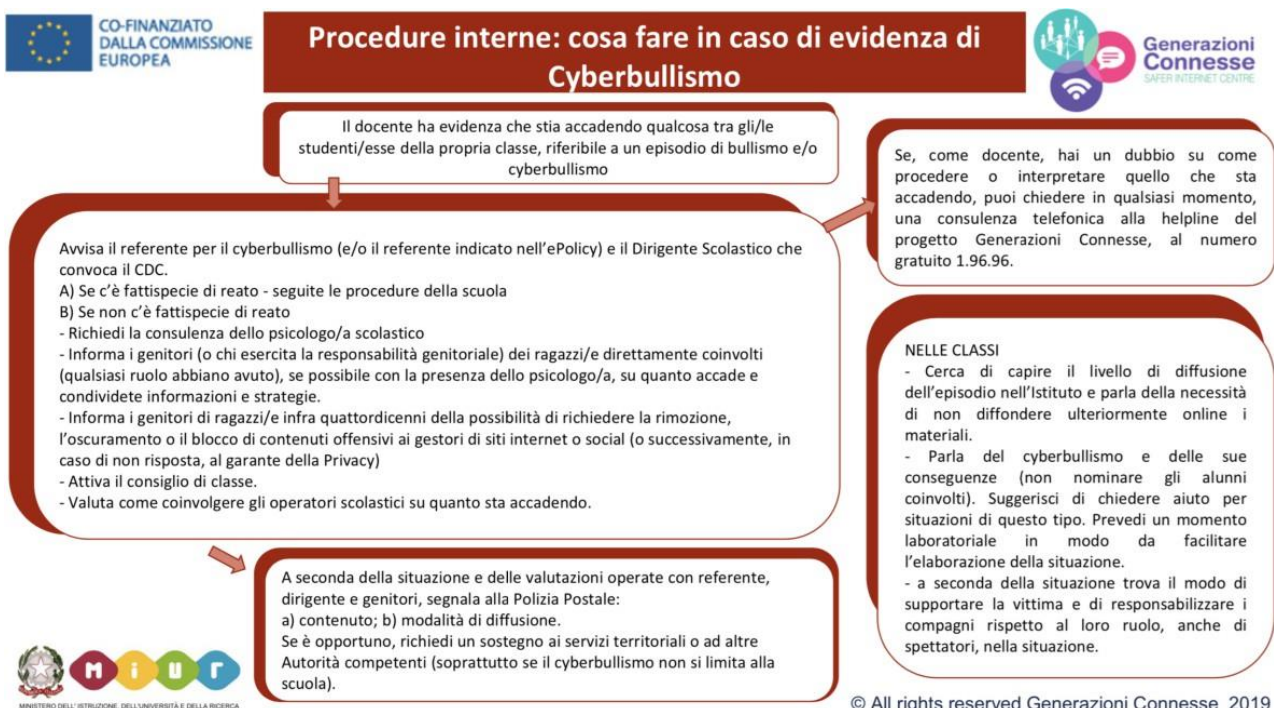
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

4.3 Allegati con procedure

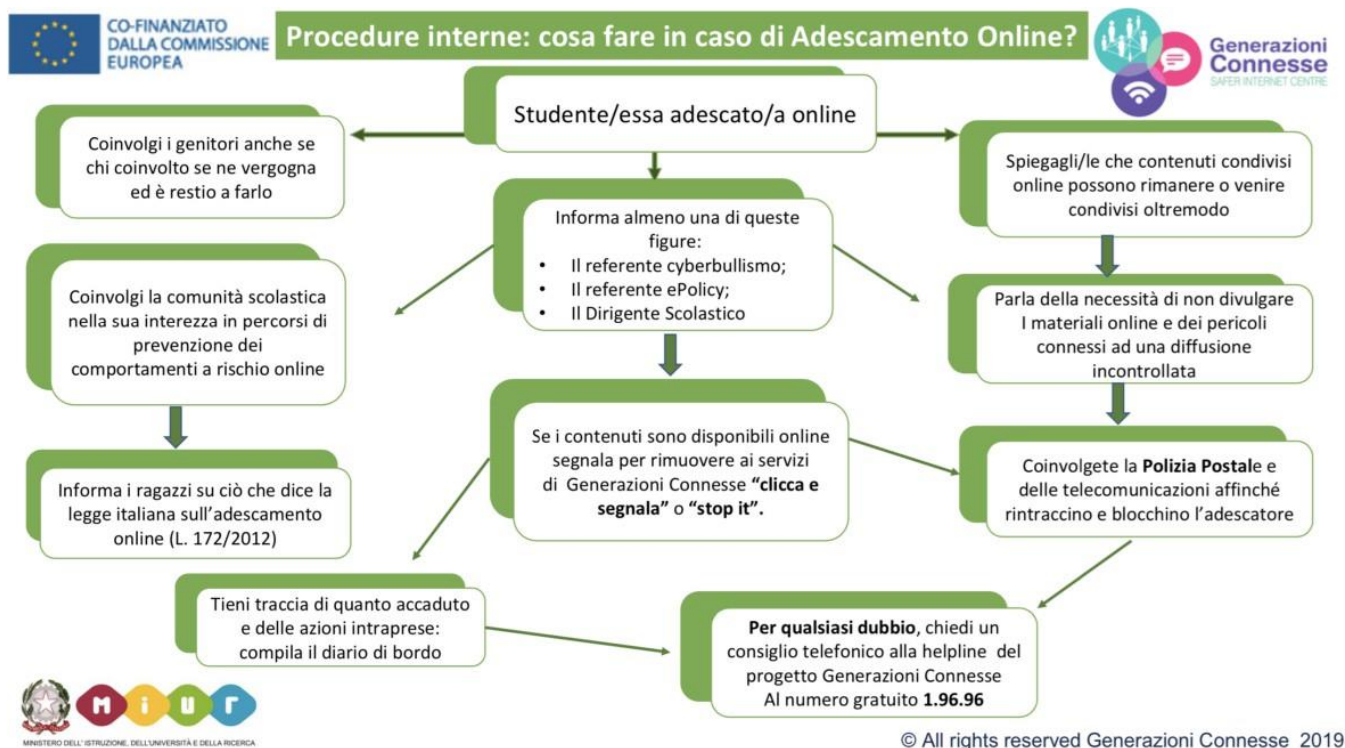
Procedure interne: cosa fare in caso di sospetto Cyberbullismo?



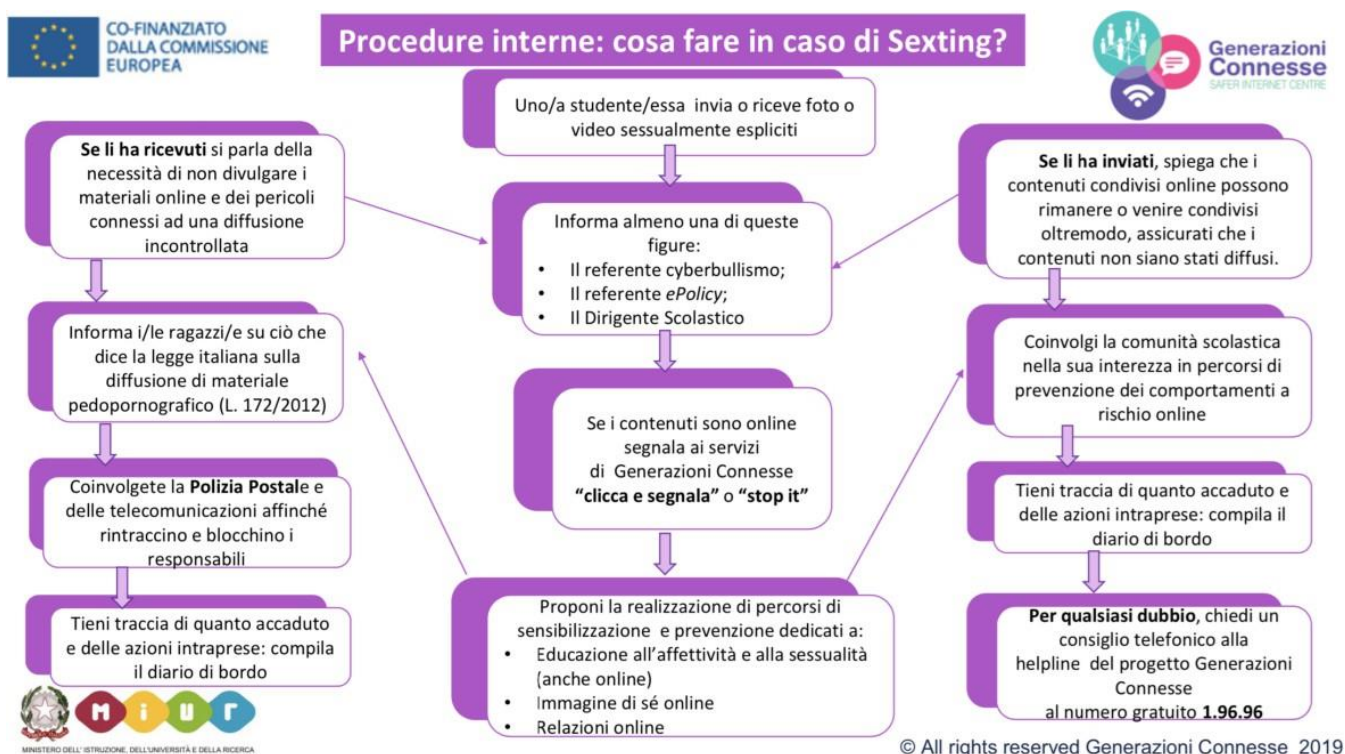
Procedure interne: cosa fare in caso di evidenza di Cyberbullismo?



Procedure interne: cosa fare in caso di adescamento online?



Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di diffusione non consentita di immagini intime?



Procedure di segnalazione per enti, associazioni e professionisti esterni alla scuola.

