



Documento di ePolicy LICEO "BONGHI-ROSMINI"

VIALE FERROVIA 19 - 71036 - LUCERA
Foggia (FG) - Puglia
Data di approvazione: 01/02/2026 - 17:43

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.

Lo scopo principale della ePolicy è di favorire un utilizzo consapevole delle tecnologie digitali all'interno della comunità scolastica in tutte le sue componenti, studenti, docenti, famiglie, fissando linee guida chiare per la sicurezza online, per la prevenzione del cyberbullismo, per la protezione dei dati, per il rispetto delle norme digitali. Ciò contribuirà a realizzare una cittadinanza digitale responsabile e ad affrontare eventuali problematiche online in modo corretto e tempestivo.

Gli obiettivi chiave della ePolicy sono:

- sviluppare competenze digitali negli studenti e nella comunità educativa per un uso efficace e responsabile delle risorse digitali;
- prevenire e gestire il cyberbullismo, fornendo gli strumenti per riconoscere, segnalare, gestire e contrastare eventuali episodi di cyberbullismo;
- garantire la sicurezza online, attraverso il rispetto delle regole fissate per la navigazione in rete, e la tutela della privacy;
- definire linee guida comportamentali, ovvero le regole per l'utilizzo corretto dei vari dispositivi elettronici a scuola e al di fuori di essa;
- creare un approccio educativo condiviso in merito all'uso dei dispositivi digitali, poiché il documento di ePolicy deve essere utilizzato dalla scuola in tutte le sue componenti e dalle famiglie.

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

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

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

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

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

IL DIRIGENTE SCOLASTICO

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

- promuovere la cultura della sicurezza online e garantirla a tutti i membri della comunità scolastica, in linea con il quadro normativo di riferimento, le indicazioni del MIM, delle sue agenzie e attraverso il documento di ePolicy;
- promuovere la cultura della sicurezza online - anche attraverso il documento di ePolicy - integrandola ed inserendola nelle misure di sicurezza più generali dell'intero Istituto;
- ha la responsabilità di fornire sistemi per un uso sicuro delle TIC, internet, i suoi strumenti ed ambienti e deve garantire alla popolazione scolastica la sicurezza di navigazione tramite internet utilizzando adeguati sistemi informatici e filtri;
- ha la responsabilità della gestione dei dati e della sicurezza delle informazioni e garantisce che l'Istituto segue le pratiche migliori possibili nella gestione dei dati stessi;
- deve tutelare la scuola e garantire agli utenti la sicurezza di navigazione utilizzando adeguati sistemi informatici e servizi di filtri Internet;
- ha il compito di garantire a tutto il personale una formazione adeguata sulla sicurezza online per essere tutelato nell'esercizio del proprio ruolo educativo e non;
- deve essere a conoscenza delle procedure da seguire in caso di un grave incidente di sicurezza online;
- deve garantire adeguate valutazioni di rischio nell'usare strumenti e TIC, effettuate in modo che comunque quanto programmato possa soddisfare le istanze educative e didattiche dichiarate nel PTOF di Istituto;
- deve garantire l'esistenza di un sistema che assicuri il monitoraggio e il controllo interno della sicurezza online in collaborazione con le figure di sistema;
- deve essere a conoscenza ed attuare le procedure necessarie in caso di grave incidente di sicurezza online.

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

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

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

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

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

In coerenza con le Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo del Ministero dell'Istruzione (D.M. n. 18 del 13/1/2021, agg. 2021 - nota prot. 482 del 18-02-2021), il Team ha le funzioni di coadiuvare il Dirigente Scolastico, coordinatore del Team nella scuola, nella definizione degli interventi di prevenzione e nella gestione dei

casi di bullismo e cyberbullismo che si possono presentare. Promuove inoltre la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale e comunica ad alunni, famiglie e tutto il personale scolastico dell'esistenza del team, a cui poter fare riferimento per segnalazioni o richieste di informazioni sul tema.

Il Team ha il compito di:

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

I/LE DOCENTI

I/le docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Possono, innanzitutto, integrare la propria disciplina con approfondimenti, promuovendo l'uso delle tecnologie digitali nella didattica. I docenti devono accompagnare e supportare gli/le studenti nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete. Inoltre, educano gli studenti alla prudenza, a non fornire dati ed informazioni personali, ad abbandonare un sito dai contenuti che possono turbare o spaventare e a non incontrare persone conosciute in Rete senza averne prima parlato con i genitori. Informano gli alunni sui rischi presenti in Rete, senza demonizzarla, ma sollecitandone un uso consapevole, in modo che Internet possa rimanere per bambini/e e ragazzi/e una fonte di divertimento e uno strumento di apprendimento.

I/le docenti osservano altresì regolarmente i comportamenti a rischio (sia dei potenziali bulli, sia delle potenziali vittime) e hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che veda coinvolti studenti e studentesse dandone tempestiva comunicazione al Dirigente Scolastico, al Referente per il Cyberbullismo e Bullismo e al Consiglio di Classe per definire strategie di intervento condivise.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Responsabile della protezione dei dati (RPD o DPO) conosce l'ePolicy di Istituto, fornisce la propria consulenza in merito agli obblighi derivanti dal GDPR e sorveglia sull'esatta osservanza della normativa in materia di tutela dei dati personali ed è co-responsabile delle azioni di informazione e formazione nell'Istituto sulla protezione dei dati personali

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

Il personale ATA, all'interno dei singoli regolamenti d'Istituto, è coinvolto nelle pratiche di prevenzione - ivi incluso il processo di definizione e implementazione dell'ePolicy di Istituto - ed è tenuto alla segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.

GLI STUDENTI E LE STUDENTESSE

Gli studenti e le studentesse devono, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti. Con il supporto della scuola dovrebbero imparare a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le. Affinché questo accada devono partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

I rappresentanti degli/delle studenti sono informati del documento di ePolicy e invitati a costruire i piani di azione, a partire dal secondo anno della secondaria di II grado,

I GENITORI/ADULTI DI RIFERIMENTO

I Genitori, in continuità con l'Istituto scolastico, sono attori partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile degli strumenti personali (pc, smartphone, etc). Come parte della comunità educante sono tenuti a relazionarsi in modo costruttivo con i/le docenti sulle linee educative che riguardano le TIC e la Rete e - ivi incluso il documento di ePolicy - comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet.

È estremamente importante che accettino e condividano quanto scritto nell'ePolicy d'Istituto e nel patto di corresponsabilità in un'ottica di collaborazione reciproca. Si promuove il coinvolgimento dei rappresentanti di genitori/adulti di riferimento all'interno del percorso di definizione e implementazione dell'ePolicy.

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

Enti esterni pubblici e privati, il mondo dell'associazionismo dovranno conformarsi alla politica della scuola riguardo all'uso consapevole delle TIC e della rete per la realizzazione di iniziative nelle scuole, finalizzate a promuovere un uso positivo e consapevole delle Tecnologie Digitali da parte dei più giovani, e/o finalizzate a prevenire e contrastare situazioni di rischio online e valutare la rispondenza delle proposte di attività di sensibilizzazione/formazione alle esigenze di qualità contenute nel documento di ePolicy. Dovranno inoltre promuovere comportamenti sicuri durante le attività che si svolgono con gli/le studenti e verificare di aver implementato una serie di misure volte a garantire la tutela dei minori nel caso di insorgenza di problematiche e ad assicurarne la tempestiva individuazione e presa in carico.

Il Dirigente Scolastico del Liceo Bonghi-Rosmini, prof. Matteo Capra, riveste un ruolo centrale nell'attuazione della ePolicy: egli è il garante della sicurezza online e il promotore della formazione per un uso consapevole delle tecnologie digitali.

I suoi compiti principali si articolano nei seguenti punti:

- **Garanzia e tutela:** Protezione della privacy e della sicurezza online per l'intera comunità scolastica.
- **Formazione:** Organizzazione di percorsi formativi sull'uso responsabile delle TIC, in stretta sinergia con i docenti referenti.
- **Gestione e Coordinamento:** Supervisione delle emergenze e coordinamento del Team Bullismo/Cyberbullismo.
- **Regolamentazione:** Supporto nella definizione delle norme per la navigazione sicura

e costante aggiornamento rispetto al quadro normativo vigente.

Le Figure Chiave dell'Istituto

Per rendere operativa questa strategia, il Liceo ha individuato figure e team specializzati:

1. **Animatore Digitale:** Coordina l'innovazione metodologica e tecnologica, promuovendo la cultura digitale e sensibilizzando sui rischi della rete.
2. **Referente d'Istituto per il Bullismo/Cyberbullismo:** Punto di riferimento per docenti e studenti, coordina le azioni di prevenzione e funge da ponte con enti esterni per promuovere il benessere scolastico.
3. **Team Antibullismo e Team per le Emergenze:** Affiancano il DS nella gestione operativa dei casi critici, lavorando sulla creazione di una rete collaborativa interna ed esterna.
4. **Referenti di Classe:** In ogni classe è presente un docente referente per il contrasto al bullismo; per le classi dalla seconda alla quinta, tale ruolo è ricoperto dal **Coordinatore di Classe**.

Nota di Trasparenza: I compiti specifici di ogni componente della comunità scolastica sono dettagliati nelle **Linee di Progetto** consultabili sul sito ufficiale della scuola.

1.3 Integrazione ePolicy nei documenti scolastici

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

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

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

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

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

Così come il PTOF è il risultato di una consapevole concertazione fra le componenti delle istituzioni scolastiche (Dirigente

Scolastico, docenti, alunni, genitori) e fra queste e il territorio, il patto di corresponsabilità rappresenta l'assunzione di responsabilità da parte di tutti coloro che svolgono un ruolo attivo nella Comunità educante.

L'ePolicy è pienamente coerente con i principali documenti della nostra scuola, quali il RAV, il PTOF, il Regolamento d'Istituto (inclusivo del Regolamento per il bullismo e il cyberbullismo), il Regolamento di Disciplina, il Patto di Corresponsabilità Educativa, e il Regolamento sull'uso dei laboratori. Tutti questi documenti riportano specifici riferimenti alla sicurezza sul web, con particolare attenzione alla prevenzione e al contrasto del cyberbullismo.

La scuola si impegna a svolgere un intervento di armonizzazione normativa a breve termine, volto a integrare i principi della sicurezza digitale in tutti i documenti d'istituto (Regolamento di Disciplina, Patto di Corresponsabilità, Regolamento d'Istituto), garantendo così piena coerenza e massima visibilità alle linee guida sulla sicurezza online. L'obiettivo è trasformare l'ePolicy in un documento trasversale che orienti ogni aspetto della vita scolastica digitale, rendendolo un riferimento esplicito e vincolante per l'intera comunità.

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

1. il curriculum sulle competenze digitali per la comunità educante (il DigComp2.2);
2. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative;
3. Come comunicare e condividere l'epolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

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

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

In tal senso, il documento è accompagnato da versioni, allegare 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.

Consapevole che la sicurezza digitale sia una sfida complessa, il nostro Istituto ha scelto di non limitarsi alla redazione di un documento tecnico, ma di trasformare l'ePolicy in uno strumento vivo e accessibile. Data la complessità del tema, la scuola si impegna a "tradurre" norme e linee guida in linguaggi adatti ai diversi interlocutori, attraverso sintesi mirate e percorsi formativi specifici.

Per assicurare la massima diffusione dei contenuti, sono state pianificate le seguenti azioni di coinvolgimento:

- **Accessibilità Digitale:** Una versione sintetizzata e di facile consultazione della ePolicy sarà pubblicata in un'area dedicata del sito web istituzionale.
- **Corpo Docente e Personale ATA:** Il documento e le sue implicazioni operative saranno oggetto di sessioni informative specifiche durante il Collegio Docenti e in incontri dedicati al personale amministrativo e ausiliario.
- **Studenti (Protagonisti della Rete):** La ePolicy verrà presentata durante le **Assemblee di Istituto** e attraverso moduli specifici dedicati alle **classi prime**.
 - Per le classi del **Triennio**, i percorsi formativi (anche in collaborazione con *Generazioni Connesse*) saranno pienamente valorizzati all'interno dei percorsi per le competenze trasversali (**PCTO**) e nelle attività di **Orientamento**.
- **Famiglie:** Per favorire l'alleanza educativa, la scuola organizzerà momenti di incontro o metterà a disposizione dei genitori supporti digitali (slide e vademecum sintetici) facilmente consultabili online.

1.5 - I Piani di Azione dell'ePolicy

I piani di azione rappresentano il **programma triennale** di obiettivi che la scuola intende realizzare per promuovere la conoscenza delle regole e dei protocolli di intervento che sono stati adottati con il documento di ePolicy nella comunità scolastica.

Nei Piani di Azione sono riportati **gli impegni e le responsabilità** che la scuola si assume per promuovere sui temi dell'educazione civica digitale e dell'utilizzo sicuro e consapevole delle tecnologie e della rete:

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

I Piani di Azione si distinguono tra standard, comuni ad ogni scuola che ha adottato l'ePolicy, e autoprodotti ovvero definiti dalla scuola sulla base del proprio contesto territoriale e delle collaborazioni in essere con Istituzioni, associazioni e aziende.

1° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

- Realizzare un evento di presentazione dell'ePolicy ai docenti dell'Istituto;
- Realizzare un evento di diffusione dell'ePolicy in occasione degli Open Day e/o in occasione del SID dell'Istituto dedicato alle famiglie ed a studenti/esse;
- Diffondere l'ePolicy negli ambienti scolastici, a studenti e studentesse, docenti e famiglie attraverso le versioni friendly dell'ePolicy;

MODULO II

- Effettuare una rilevazione del fabbisogno formativo dei docenti sui temi dell'educazione civica digitale;
- Effettuare una rilevazione di interessi, bisogni e comportamenti delle famiglie sull'uso positivo del digitale;
- Avviare l'introduzione del kit didattico come metodo e risorsa di lavoro in alcune classi pilota;

MODULO III

- Integrare l'ePolicy (norme, regolamenti e procedure) nei documenti dell'Istituto;
- Aggiornare la Politica d'Uso Accettabile (PUA) della scuola ed il regolamento BYOD dell'Istituto;

MODULO IV

- Definizione, a partire da quanto definito nell'ePolicy, delle procedure di segnalazione anche con linguaggio child/youth friendly perché possano essere accessibili a studenti e studentesse;
- Realizzare una reportistica delle segnalazioni ricevute e dei relativi esiti.

2° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

- Realizzare una formazione rivolta ai docenti dell'Istituto, sulla base dei risultati della rilevazione svolta nel corso del primo anno, anche attraverso il supporto di esperti/associazioni esterne o avvalendosi del percorso disponibile sul sito di Generazioni Connesse. La formazione deve coprire almeno il 60% del corpo docente.

MODULO II

- L'istituto utilizza il kit didattico come pratica metodologica e risorse a disposizione dei docenti per i percorsi di ECD attraverso la formazione specifica sviluppata per i docenti attraverso il sito di Generazioni Connesse;
- Effettuare una rilevazione di interessi, bisogni, comportamenti, abitudini di studenti e studentesse sui temi dell'educazione civica digitale;
- Realizzare una formazione rivolta agli studenti e alle studentesse attraverso il percorso previsto sulla piattaforma di Generazioni Connesse;
- Realizzare una formazione rivolta alle famiglie attraverso il percorso previsto sulla piattaforma di Generazioni Connesse

Piano Triennale di ePolicy (2025-2028)

Liceo "Bonghi-Rosmini" - Lucera

Il presente Piano definisce la strategia del Liceo Bonghi-Rosmini per la promozione della cittadinanza digitale, la sicurezza in rete e il contrasto al bullismo e cyberbullismo. L'obiettivo è trasformare l'ePolicy in un ecosistema educativo strutturale e condiviso.

ANNUALITÀ I (A.S. 2025/2026): Consolidamento e Lancio

Il primo anno è dedicato all'aggiornamento normativo e alla formazione.

1. Governance e Integrazione Documentale

- **Revisione Normativa:** Aggiornamento del documento di ePolicy e approvazione formale in Collegio Docenti e Consiglio d'Istituto.
- **Armonizzazione:** Integrazione esplicita dell'ePolicy nel **RAV**, nel **PTOF** e nei Regolamenti d'Istituto.
- **Standard Tecnici:** Definizione della **PUA** (Politica d'Uso Accettabile) e del regolamento **BYOD** (*Bring Your Own Device*).

2. Comunicazione e Internazionalizzazione

- **Accessibilità:** Pubblicazione sul sito web delle versioni "dedicated" *family-friendly* dell'ePolicy.
- **Erasmus+:** Integrazione delle pratiche di cittadinanza digitale nei progetti europei già finanziati.

3. Formazione e Rilevazione

- **Analisi dei bisogni:** Rilevazione del fabbisogno formativo e dei comportamenti digitali per docenti, ATA, studenti e famiglie.
- **Corsi:**
 - *Per Studenti:* Eipass
 - *Per Staff:* Adempimenti legali nella scuola digitale ed Educazione Civica Digitale o corsi sull'AI.
- **Incentivi FSL:** Riconoscimento delle ore di formazione sulla piattaforma *Generazioni Connesse* come ore di FLS.

ANNUALITÀ II E III (2026-2028): Strutturalità e Territorio

Il biennio successivo mira a rendere le azioni intraprese una pratica quotidiana e istituzionalizzata.

1. Formazione Permanente e Curricolare

- **Curricolo di Educazione Civica:** L'educazione digitale diventa modulo ineludibile e strutturale del curricolo di Educazione Civica per tutti gli indirizzi.
- **Kit Didattico:** Estensione a tutte le classi del kit di *Generazioni Connesse* come risorsa metodologica ordinaria.
- **Accoglienza:** Presentazione sistematica dell'ePolicy e delle linee guida Privacy ai nuovi docenti, personale ATA e alle classi prime durante l'accoglienza.

2. Gestione Casi e Infrastruttura

- **Reporting:** Perfezionamento della reportistica dei casi di cyberbullismo con procedure di segnalazione semplificate e accessibili agli studenti.
- **Monitoraggio Tecnologico:** Valutazione dell'introduzione di software per il monitoraggio dei device durante le attività didattiche per garantire un ambiente di apprendimento protetto.

3. Apertura al Territorio e Partnership

- **Dialogo Istituzionale:** Comunicazione formale delle scelte di ePolicy all'**USR** e al **Comune**, per creare una rete di protezione territoriale.
- **Eventi per la Comunità:** Organizzazione di iniziative aperte alle famiglie e alla comunità educante del territorio per sensibilizzare sui rischi emergenti e condividere buone pratiche.

Monitoraggio e Valutazione

Il processo è supervisionato dalla **Team per il Contrasto al Bullismo**, che opera attraverso:

1. **Indicatori di Impatto:** Misurazione della crescita delle competenze digitali degli studenti.
2. **Feedback Qualitativo:** Valutazione del grado di soddisfazione e consapevolezza del personale e delle famiglie.
3. **Revisione Ciclica:** Il report finale triennale costituirà la base per il successivo aggiornamento documentale.

Obiettivo Finale: Garantire che il Liceo Bonghi-Rosmini sia un luogo di apprendimento sicuro, dove l'innovazione tecnologica proceda di pari passo con la responsabilità etica e la tutela della persona.

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

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

Per trasformare l'ePolicy da un semplice documento a un progetto di **cittadinanza digitale attiva**, il Liceo Bonghi-Rosmini sfrutterà diverse risorse, differenziandole per canali di comunicazione e attività pratiche.

1. Risorse Istituzionali e Nazionali (I "Fondamentali")

Questi sono i punti di riferimento normativi e contenutistici per docenti e genitori:

- **Piattaforma Generazioni Connesse:** Offre il **Kit Didattico** (con schede pronte all'uso su fake news, privacy e grooming) e corsi di formazione gratuiti per tutta la comunità.
- **Piattaforma ELISA:** Indispensabile per la formazione specifica dei docenti referenti e per il monitoraggio dei fenomeni di bullismo tramite questionari certificati.
- **DigComp 2.2:** Il quadro europeo delle competenze digitali, utile per i docenti per

progettare attività che non siano solo "tecniche" ma legate al pensiero critico e all'etica.

2. Strumenti di Condivisione e Divulgazione

Per rendere l'ePolicy "scansionabile" e memorizzabile:

- **"Infografiche Friendly":** Creare una versione visiva (usando tool come *Canva*) che riassume in 5 punti chiave i diritti e i doveri digitali degli studenti, da affiggere nelle classi e pubblicare su Facebook/Sito Web.
- **Vademecum per Genitori:** Una breve guida digitale che spieghi come la scuola gestisce le emergenze digitali.
- **Canali Social Istituzionali:** Post periodici con "Pillole di ePolicy" (es. "*Lo sapevi che...? Le regole per le foto di gruppo a scuola*").

3. Risorse per la Cittadinanza Attiva (Il "Fare")

Per coinvolgere gli studenti non come spettatori, ma come protagonisti:

- **Peer Education:** Formare un gruppo di studenti "Ambassador della Gentilezza Digitale" che presentino l'ePolicy ai compagni più giovani durante le assemblee.
- **Manifesto della Comunicazione Non Ostile:** Integrare le schede didattiche di *Parole O_Stili* per lavorare sul linguaggio e sull'empatia online.
- **Laboratori di Fact-Checking:** Utilizzare siti come *Sky Academy* o risorse sul debunking per insegnare a distinguere le fake news, parte integrante del percorso FSL.
- **Digital Detox Challenge:** Organizzare una giornata o settimana di sensibilizzazione sull'equilibrio tra vita online e offline (benessere digitale).
- **Ispirazione Progettuale:** Consultazione dei progetti vincitori del contest [The Kids are All Right](#) per ideare nuove attività di sensibilizzazione gestite dagli studenti.
- **Laboratori di Peer-Education:** Gli studenti del triennio utilizzeranno i contenuti della serie YouTube [We are Fearless](#), specificamente rivolta alle scuole superiori, per formare i compagni più giovani.

4. Rilevazione del Fabbisogno Formativo

Al fine di personalizzare la formazione, verranno utilizzati strumenti di autovalutazione standardizzati:

- **Per i Docenti:** Utilizzo di [SELFIE FOR TEACHERS](#), lo strumento della Commissione Europea per riflettere sulle proprie competenze digitali secondo il framework DigCompEdu.
- **Per l'Istituto:** Integrazione con il questionario [SELFIE](#) per analizzare il livello di utilizzo del digitale nell'intera comunità scolastica.
- **Per le Famiglie:** Promozione del test [MYDIGISKILLS](#) (disponibile anche sul sito di

[Repubblica Digitale](#)) per permettere ai genitori di valutare le proprie competenze digitali rispetto al framework DIGCOMP 2.2.

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.

In un'ottica di trasparenza e partecipazione, il Liceo Bonghi Rosmini adotta una strategia integrata di prevenzione basata sulla condivisione della E-policy, del Kit Didattico e di altro materiale. Questi documenti, consultabili sul sito istituzionale, definiscono il framework regolamentare e operativo per l'uso consapevole delle tecnologie, offrendo all'intera comunità scolastica risorse strutturate per promuovere la cittadinanza digitale e la sicurezza in rete.

Le iniziative rivolte agli studenti includono percorsi sull'analisi critica delle fonti, sulla disinformazione, sui rischi emergenti legati alla vita online, sull'uso responsabile dei social network e sulla gestione dell'identità digitale, oltre ad approfondimenti su diritti e doveri in rete e simulazioni finalizzate allo sviluppo dell'autonomia decisionale.

Particolare attenzione è rivolta agli studenti con disabilità, attraverso la predisposizione di attività accessibili, l'utilizzo di tecnologie assistive, la personalizzazione degli interventi formativi e il coordinamento con i docenti di sostegno per garantire una piena partecipazione ai percorsi e un uso sicuro e autonomo degli strumenti digitali.

La collaborazione con le famiglie è promossa mediante la diffusione di informazioni chiare e aggiornate riguardanti l'uso consapevole delle tecnologie, la tutela dei dati personali e le dinamiche relazionali legate al digitale. Saranno possibili momenti di confronto finalizzati a condividere linee educative comuni e a supportare il ruolo genitoriale nella promozione di comportamenti responsabili e rispettosi nell'ambiente online, con particolare attenzione ai bisogni educativi degli studenti più vulnerabili.

Il personale docente e non docente partecipa a percorsi di formazione su competenze digitali avanzate, aspetti normativi e protocolli di gestione delle situazioni critiche, con

aggiornamenti costanti sulle dinamiche digitali giovanili. Il Liceo sostiene inoltre la progettazione interdisciplinare e fornisce strumenti per monitorare i rischi e favorire un clima scolastico positivo anche negli ambienti digitali utilizzati per la didattica.

L'intero impianto educativo si basa su un approccio sistemico di tipo "whole school approach", integrato tra attività curricolari, extracurricolari e progettuali, assicurando inclusività, tutela e partecipazione per tutti gli studenti.

2.2 - Il Curricolo Digitale

Per realizzare questo obiettivo l'istituto utilizza le risorse messe a disposizione a livello nazionale e internazionale.

Il DigComp 2.2, framework europeo sulle competenze digitali, permette di costruire una cornice precisa in cui inquadrare i temi e le corrispondenti competenze da proporre nell'Istituto non solo per gli studenti.

Al suo interno vengono identificati alcuni temi sui quali è costruita una proposta specifica per le famiglie e gli studenti (formazione). Tale cornice trova poi sviluppo specifico, per gli studenti, nel curriculum di educazione alla Cittadinanza Digitale previsto dalla L. 92/2019. Il curriculum prende forma attorno all'ePolicy e le attività didattiche sono legate al documento ed alle scelte dell'Istituto al suo interno.

Nel curriculum va previsto in ogni classe un appuntamento didattico specifico, calibrato sull'età degli alunni, e l'utilizzo dei kit didattici per favorire da parte degli studenti una maggiore conoscenza e consapevolezza delle finalità del presente documento.

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

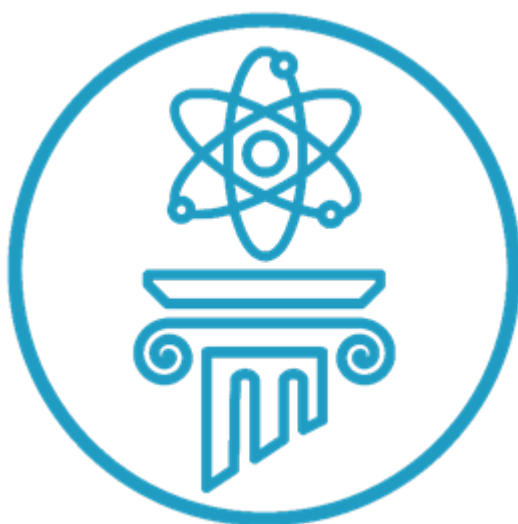
Il curriculum digitale è definito come **un percorso didattico verticale pensato per tutti gli studenti e le studentesse teso a sviluppare, e poi potenziare, le cosiddette "competenze digitali" in ottica trasversale** (su più livelli, anni e gradi di istruzione) **ed interdisciplinare** (per tutte le discipline). Si tratta, quindi, di favorire la capacità dell'uso dei dispositivi digitali non solo da un punto di vista strettamente tecnico ma anche e soprattutto da un punto di vista etico, responsabile e critico (pensiero critico) utile allo sviluppo della **cittadinanza digitale** tramite la progettazione e la sperimentazione di percorsi, attività e laboratori in aule dedicate al digitale tra opportunità, rischi e sfide del prossimo futuro.

Il Curriculum Digitale ha lo scopo di programmare ed implementare percorsi didattici di facile replicabilità, uso e applicazione che siano **"innovativi, strutturati, aperti e in grado di coinvolgere la comunità scolastica allargata"** sul tema del digitale e delle tecnologie digitali. In questo modo, si può rendere quanto più possibile integrato e consapevole l'utilizzo dei dispositivi digitali così come anche esplicitato nel DigComp Edu secondo cui lo sviluppo

delle competenze digitali degli studenti significa **aiutarli “ad utilizzare in modo creativo e responsabile le tecnologie digitali per attività riguardanti l'informazione, la comunicazione, la creazione di contenuti, il benessere personale e la risoluzione dei problemi”**.

Attraverso il curricolo digitale, il nostro Istituto promuove, in ciascun insegnamento, le competenze digitali degli studenti e delle studentesse. Tramite attività, lezioni specifiche, laboratori si vuole **massimizzare il protagonismo di tutta la comunità scolastica** (inclusi i docenti e tutti i professionisti che, nella scuola, svolgono funzioni formative ed educative). Si tratta di percorsi che possono essere svolti sia durante l'orario curricolare che extracurricolare, da singole classi o anche da gruppi di studio/lavoro dell'Istituto su un tema coerente con le tecnologie e lo sviluppo delle competenze digitali.

Inoltre tali percorsi sono inseriti ed incrociati con quelli della legge 20 agosto 2019, n. 92 (**introduzione dell'insegnamento scolastico dell'educazione civica**). All'interno del Curricolo di educazione civica, presente nel nostro Istituto, sono previsti percorsi di cittadinanza digitale, che tengano conto di un approccio metodologico-didattico innovativo, anche attraverso la possibilità di comunicare e condividere quanto creato (tramite la produzione di “artefatti” digitali o comunque di materiale come slide, video, presentazioni, podcast, etc...).



LICEO BONGHI ROSMINI LUCERA

CURRICOLO DIGITALE VERTICALE

CURRICOLO DIGITALE VERTICALE

In coerenza con le più recenti indicazioni europee in materia di educazione digitale e cittadinanza attiva, il **Curricolo Digitale** del Liceo “Bonghi-Rosmini” è stato progettato alla luce del **Quadro di riferimento europeo delle competenze digitali per i cittadini - DigComp 2.2**. Tale quadro rappresenta lo strumento di riferimento per la definizione, lo sviluppo e la valutazione delle competenze digitali, considerate oggi parte integrante delle competenze chiave per l'apprendimento permanente.

Il documento recepisce pienamente gli indirizzi della **Raccomandazione del Consiglio dell'Unione Europea del 22 maggio 2018**, che individua come obiettivo prioritario l'innalzamento e il miglioramento del livello delle competenze digitali in tutte le fasi dell'istruzione e della formazione, per ogni fascia della popolazione. Allo stesso tempo, promuove l'acquisizione delle **competenze chiave di cittadinanza** attraverso molteplici approcci e contesti di apprendimento, valorizzando l'uso consapevole, critico e creativo delle tecnologie digitali nei processi educativi e formativi.

In questa prospettiva, il **Curricolo Digitale Verticale** del Liceo si configura come un percorso strutturato, coerente e trasversale a tutte le discipline, finalizzato allo sviluppo integrato delle competenze digitali e di cittadinanza digitale. Esso promuove la partecipazione attiva, l'inclusione, la sicurezza online, la capacità di ricerca e gestione dell'informazione, la collaborazione e la creazione di contenuti digitali, in linea con le cinque aree di competenza individuate dal **DigComp 2.2**.

Attraverso azioni didattiche mirate e progressivamente articolate nei diversi anni di corso, il curricolo intende fornire agli studenti gli strumenti per diventare **cittadini digitali consapevoli, responsabili e competenti**, capaci di utilizzare le tecnologie non solo come mezzi operativi, ma come risorse culturali e sociali per l'apprendimento, la partecipazione e l'innovazione.

PRIMO BIENNIO

AREA DI COMPETENZA	COMPETENZA	LIVELLO DI PADRONANZA	ABILITÀ	ATTIVITÀ: ESEMPIO D'USO
--------------------	------------	-----------------------	---------	-------------------------

ALFABETIZZAZIONE SU
INFORMAZIONI E DATI

1.1. Navigare, ricercare e filtrare dati, informazioni e contenuti digitali.

Intermedio 3

Da solo e risolvendo problemi diretti, lo studente è in grado di:

- Spiegare i miei fabbisogni informativi.
- Svolgere ricerche ben definite e di routine per individuare dati, informazioni e contenuti negli ambienti digitali.
- Spiegare come accedervi e navigare al loro interno.

Preparare una breve relazione su un argomento specifico.

Nominare all'insegnante siti web, blog e database digitali a cui si accede abitualmente dal PC per consultare la bibliografia per i compiti a casa.

Utilizzare parole chiave ben definite per trovare risorse bibliografiche all'interno di siti web, blog e database digitali e spiegare come accedere ai risultati e navigare al loro interno.

Spiegare ai compagni le parole chiave e le etichette che si utilizzano abitualmente per trovare riferimenti bibliografici negli ambienti digitali (blog, siti web, database) per preparare compiti.

Fornire esempi ai compagni di classe di siti web, blog e database digitali per trovare riferimenti bibliografici sull'argomento di una relazione.

Organizzare la strategia di ricerca per trovare questi siti web, blog e database digitali che contengono riferimenti bibliografici inerenti all'argomento di una relazione.

Descrivere all'insegnante come si accede e si naviga tra i siti web, i blog e i database digitali per trovare i riferimenti bibliografici ottenuti tramite questa ricerca organizzata.

Organizzare con post-it digitali e online sul tablet una lista di parole chiave ed etichette utili per trovare riferimenti bibliografici inerenti all'argomento della relazione. Salvare i contenuti didattici in diversi formati. Realizzare file e cartelle dove raccogliere dati.

Fare il backup dei dati su dispositivi diversi: hard disk, USB e iCloud o Drive. Utilizzare supporti di archiviazione quali chiavette USB, hard disk esterni, CD, DVD.

Utilizzare sistemi di archiviazione quali Google Drive, iCloud, One Drive, Dropbox.

1.3. Gestire dati, informazioni e contenuti digitali.

Intermedio 4

In modo indipendente, secondo i miei fabbisogni e risolvendo problemi ben definiti e non sistematici, lo studente è in grado di:

- Spiegare strategie personali di ricerca ben definite e sistematiche.
- Illustrare fabbisogni informativi.
- Organizzare le ricerche di dati, informazioni e contenuti in ambienti digitali.
- Descrivere come accedere a questi dati, informazioni e contenuti e navigare al loro interno.
- Organizzare strategie di ricerca personali.

- Selezionare dati, informazioni e contenuti allo scopo di organizzarli, archivarli e recuperarli in maniera sistematica all'interno di ambienti digitali.

- Organizzarli in modo sistematico in un ambiente strutturato.

Intermedio 3

Da solo e risolvendo problemi diretti, lo studente è in grado di:

2.1. Interagire con gli altri attraverso le tecnologie digitali.

Intermedio 3

Da solo e risolvendo problemi diretti, lo studente è in grado di:

- Interagire con le tecnologie digitali in modo adeguato e sistematico.
- Scegliere mezzi di comunicazione digitali adeguati e di routine per un determinato contesto.

Creare un account. Utilizzare gli strumenti di condivisione di documento, foglio di calcolo, presentazione, ecc. Utilizzo della classe virtuale. Utilizzo del registro elettronico. Utilizzo della piattaforma di comunicazione a distanza.

Intermedio 4

In modo indipendente, secondo i miei fabbisogni e risolvendo problemi ben definiti e non sistematici, lo studente è in grado di:

- Scegliere molteplici tecnologie digitali semplici per l'interazione.
- Scegliere una varietà di mezzi di comunicazione digitali appropriati per un determinato contesto.
- Utilizzare tecnologie digitali appropriate per condividere dati, informazioni e contenuti digitali.

Utilizzo di sistemi di scrittura collaborativa: scrittura sincrona con note, correzioni, ecc. Aggregatori di contenuti.

Utilizzo di mappe concettuali.

Utilizzo di piattaforme di e-learning o di condivisione cloud in ambito didattico (Google Classroom, WeSchool, Schoolwork, ecc.), anche in modalità flipped con materiali predisposti dai docenti.

2.2. Condividere informazioni attraverso le tecnologie digitali

Intermedio 4

In modo indipendente, secondo i miei fabbisogni e risolvendo problemi ben definiti e non sistematici, lo studente è in grado di:

- Spiegare come agire da intermediari per condividere informazioni e contenuti attraverso le tecnologie digitali.

Utilizzo di una chat di uso comune sullo smartphone (ad es. Messenger o WhatsApp) per parlare con i compagni di classe e organizzare il lavoro di gruppo.

2.5. Netiquette

Base 2

A livello base, in autonomia e con un supporto adeguato, laddove necessario, lo studente è in grado di:

- Spiegare le prassi di riferimento e attribuzione.
- Distinguere le semplici norme comportamentali e il know-how per l'utilizzo delle tecnologie digitali e l'interazione con gli ambienti digitali.
- Scegliere modalità di comunicazione e strategie semplici adatte a un pubblico.
- Distinguere le differenze culturali e generazionali semplici di cui tener conto negli ambienti digitali.

Lavorare in gruppo con i compagni.

Applicare regole di comportamento appropriato, improntate al decoro e al rispetto di sé e degli altri, nell'interazione di ambienti digitali.

Adeguare le strategie di comunicazione al pubblico e al contesto di riferimento.

Saper utilizzare carattere e font adeguati alla comunicazione in rete.

COMUNICAZIONE E
COLLABORAZIONE

CREAZIONE DI CONTENUTI DIGITALI	3.1. Sviluppare contenuti digitali	<p>Intermedio 3 Da solo e risolvendo problemi diretti, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Indicare modalità per creare e modificare contenuti ben definiti e sistematici in formati ben definiti e sistematici. 	<p>Creare prodotti digitali ben definiti: mappe concettuali, timeline, infografiche.</p> <p>Preparare una presentazione digitale animata su un determinato argomento.</p>
		<p>Intermedio 4 In modo indipendente, secondo i miei fabbisogni e risolvendo problemi ben definiti e non sistematici, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Esprimersi attraverso la creazione di strumenti digitali ben definiti e sistematici. - Individuare modalità per creare e modificare i contenuti in diversi formati. 	<p>Utilizzare sistemi di geolocalizzazione (Google Maps, Google Earth).</p> <p>Utilizzare software per la creazione di video, con inserimento di audio dal web, dal vivo, ecc.</p> <p>Creare podcast.</p>
SICUREZZA	4.1. Proteggere i dispositivi	<p>Intermedio 3 Da solo e risolvendo problemi diretti, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Esprimersi attraverso la creazione di strumenti digitali. - Individuare modi ben definiti e sistematici per proteggere i suoi dispositivi, contenuti digitali. 	<p>Creare password forti per l'accesso alle piattaforme digitali della scuola.</p> <p>Effettuare sempre il logout e verificare la disconnessione di un account utente.</p> <p>Risolvere problemi come aggiungere o cancellare membri dal gruppo della chat.</p>
		<p>Intermedio 4 In modo indipendente, secondo i miei fabbisogni e risolvendo problemi ben definiti e non sistematici, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Distinguere rischi e minacce ben definiti e sistematici negli ambienti digitali. - Scegliere misure di sicurezza ben definite e sistematiche. - Distinguere i rischi e le minacce negli ambienti digitali. 	<p>Gestire le impostazioni di privacy nei documenti condivisi.</p> <p>Eseguire il download sicuro dei file.</p>
RISOLVERE PROBLEMI	5.3. Utilizzare in modo creativo le tecnologie digitali	<p>Intermedio 3 Da solo e risolvendo problemi diretti, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Scegliere le misure di sicurezza. - Spiegare modalità per tenere in debita considerazione affidabilità e privacy. - Scegliere strumenti e tecnologie digitali da utilizzare per creare know-how ben definito e processi e prodotti innovativi ben definiti. 	<p>Utilizzare un elenco di risorse didattiche fornite dal docente per rispondere ai bisogni formativi della situazione di apprendimento, conoscenze di base, recupero (anche in apprendimento a distanza).</p> <p>Impostare l'interfaccia in lingua prescelta.</p>
		<p>Intermedio 4 In modo indipendente, secondo i miei fabbisogni e risolvendo problemi ben definiti e non sistematici, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Partecipare individualmente e collettivamente ad alcuni processi cognitivi per comprendere e risolvere problemi concettuali ben definiti e sistematici situazioni problematiche negli ambienti digitali. - Distinguere strumenti e tecnologie digitali per creare know-how e innovare processi e prodotti. - Partecipare individualmente e collettivamente ai processi cognitivi per comprendere e risolvere problemi concettuali e situazioni problematiche negli ambienti digitali. 	<p>Utilizzare risorse di rete per risolvere problemi e difficoltà connesse al proprio apprendimento.</p>

SECONDO BIENNIO

AREA DI COMPETENZA

COMPETENZA

LIVELLO DI PADRONANZA

ABILITÀ

ATTIVITÀ: ESEMPIO D'USO

ALFABETIZZAZIONE SU INFORMAZIONI E DATI	<p>1.2. Valutare dati, informazioni e contenuti digitali</p>	<p>Avanzato 5 Oltre a fornire supporto agli altri, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Svolgere una valutazione della credibilità e dell'affidabilità di fonti diverse dei dati, informazioni e contenuti digitali. - Svolgere una valutazione di dati, informazioni e contenuti digitali diversi. 	<p>Verificare se le fonti citate sono originarie, se ci sono riferimenti a libri e autori autorevoli.</p> <p>Controllare che il server non appartenga ad associazioni prove di affidabilità scientifica.</p>
COMUNICAZIONE E COLLABORAZIONE	<p>2.2. Condividere informazioni attraverso le tecnologie digitali</p>	<p>Avanzato 5 Oltre a fornire supporto agli altri, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Condividere dati, informazioni e contenuti digitali attraverso svariati strumenti digitali. - Mostrare agli altri come agire da intermediari per condividere informazioni e contenuti attraverso le tecnologie digitali. 	<p>Attivare forma di scrittura collaborativa ai fini didattici da condividere con il gruppo classe (Brevi relazioni, sintesi, mappe concettuali e/o mentali, presentazioni, ecc.).</p>
CREAZIONE DI CONTENUTI DIGITALI	<p>2.3. Esercitare la cittadinanza attraverso le tecnologie digitali</p>	<p>Intermedio 3 Da solo e risolvendo problemi diretti, lo studente è in grado di:</p> <p>Intermedio 4 In modo indipendente, secondo i suoi fabbisogni e risolvendo problemi ben definiti e non sistematici, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Scegliere semplici servizi digitali ben definiti e sistematici per partecipare alla vita sociale. - Scegliere semplici servizi digitali per partecipare alla vita sociale. - Discutere su tecnologie digitali appropriate per potenziare le sue capacità personali e professionali e partecipare come cittadino alla vita sociale. - Applicare modi per creare e modificare contenuti digitali in diversi formati. 	<p>Organizzare, insieme ai compagni, un evento in occasioni di giornate a tema o in occasioni rilevanti per la comunità scolastica.</p> <p>Utilizzare la piattaforma di apprendimento digitale della scuola per condividere informazioni a livello del gruppo classe.</p> <p>Utilizzare l'account della piattaforma Gsuite della scuola per comunicazioni di Istituto (Cartella Drive con aggiornamenti da parte dei rappresentanti d'Istituto, rappresentanti della Consulta, materiali in vista delle elezioni degli OO.CC., ecc.).</p>
	<p>3.1. Sviluppare contenuti digitali</p>	<p>Avanzato 5 Oltre a fornire supporto agli altri, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Mostrare modalità per esprimersi attraverso la creazione di materiali digitali. - Spiegare modi per modificare, affinare, migliorare e integrare voci ben definite di nuovi contenuti e informazioni per crearne di nuovi e originali. 	<p>Utilizzare un software di infografica.</p> <p>Utilizzare un software pre creare una mappa mentale e/o una mappa concettuale.</p> <p>Preparare un presentazione/video.</p>
	<p>3.2. Integrare e rielaborare contenuti digitali</p>	<p>Intermedio 3 Da solo e risolvendo problemi diretti, lo studente è in grado di:</p> <p>Intermedio 4 In modo indipendente, secondo i suoi fabbisogni e risolvendo problemi ben definiti e non sistematici, lo studente è in grado di:</p> <p>Base 2 A livello base, in autonomia e con un supporto adeguato, laddove necessario, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Discutere modi per modificare, affinare, migliorare e integrare nuovi contenuti e informazioni per crearne di nuovi e originali. - Individuare semplici regole di copyright e licenze da applicare a dati, informazioni e contenuti digitali. 	<p>Aggiornare una presentazione digitale animata, aggiungendo testo, immagini ed effetti visivi.</p> <p>Preparare un breve tutorial. Elaborare prodotti multimediali originali, anche partendo da modelli predeterminati.</p> <p>Creare storie di digital storytelling.</p> <p>Creare libri digitali. Trovare per i contenuti digitali e le informazioni acquisite dalla Rete le licenze di utilizzo secondo le regole del copyright.</p>
	<p>3.3. Copyright e licenze</p>	<p>Intermedio 3 Da solo e risolvendo problemi diretti, lo studente è in grado di:</p> <p>Base 2 A livello base, in autonomia e con un supporto adeguato, laddove necessario, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Individuare regole di copyright e licenze ben definite e sistematiche da applicare a dati, informazioni digitali e contenuti. - Elencare semplici istruzioni per un sistema informatico per risolvere un semplice problema o svolgere un compito semplice. - Elencare istruzioni ben definite e sistematiche per un sistema informatico per risolvere problemi sistematici o svolgere compiti sistematici. 	<p>Individuare il simbolo che indica un'immagine protetta da copyright. Preparare una presentazione/video su un determinato argomento.</p> <p>Saper applicare licenze Creative Commons su contenuti digitali di propria creazione.</p> <p>Utilizzare banche dati per trovare immagini scaricabili gratuitamente. Utilizzare un'interfaccia di programmazione semplice.</p>
	<p>3.4. Programmazione</p>	<p>Intermedio 3 Da solo e risolvendo problemi diretti, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Elencare istruzioni ben definite e sistematiche per un sistema informatico per risolvere problemi sistematici o svolgere compiti sistematici. 	<p>Fornire semplici istruzioni per sviluppare un gioco educativo.</p> <p>Risolvere il debug del programma e risolvere semplici problemi nel proprio codice.</p>

SICUREZZA	4.1. Proteggere i dispositivi	<p>Avanzato 5 Oltre a fornire supporto agli altri, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Applicare differenti modalità per proteggere i dispositivi e i contenuti digitali. - Distinguere una varietà di rischi e minacce negli ambienti digitali. - Applicare misure di sicurezza. - Individuare varie modalità per tenere in debita considerazione l'affidabilità e la privacy. - Discutere modalità per proteggere i suoi dati personali e la privacy negli ambienti digitali. 	<p>Individuare rischi come la ricezione di tweet e messaggi da follower con profili falsi o tentativi di phishing. Applicare misure per evitarli (ad es. controllo delle impostazioni della privacy).</p> <p>Proteggere informazioni, dati e contenuti sulla piattaforma di apprendimenti digitale della scuola (ad es. una password forte, controllo dei login recenti).</p> <p>Utilizzare account Gmail, Facebook, Instagram e Twitter.</p>
	4.2. Proteggere i dati personali e la privacy	<p>Intermedio 4 In modo indipendente, secondo i suoi fabbisogni e risolvendo problemi ben definiti e non sistematici, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Discutere modalità per utilizzare e condividere informazioni personali proteggendo sé stesso e gli altri da danni. - Indicare clausole della politica sulla privacy su come vengono utilizzati i dati personali nei servizi digitali. - Applicare modalità diverse per proteggere i suoi dati personali e la privacy negli ambienti digitali. 	<p>Proteggere i dati personali mentre condivido contenuti digitali.</p> <p>Utilizzare la piattaforma di apprendimento digitale della scuola per condividere informazioni.</p> <p>Distinguere tra contenuti appropriati e inappropriati.</p>
	4.3. Proteggere la salute e il benessere	<p>Avanzato 5 Oltre a fornire supporto agli altri, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Applicare modalità specifiche diverse per condividere i suoi dati proteggendo sé stesso e gli altri da pericoli. - Spiegare le clausole della politica sulla privacy inerenti alle modalità di utilizzo dei dati personali nei servizi digitali. - Mostrare diverse modalità per evitare rischi per la salute e minacce al benessere psicofisico quando si utilizzano le tecnologie digitali. 	<p>Valutare se i dati personali vengono utilizzati in modo appropriato.</p> <p>Percepire quali sono i confini della libertà in rete e i rischi.</p> <p>Percepire i concetti di "legale" e "illegale".</p> <p>Navigare in sicurezza.</p>
RISOLVERE PROBLEMI	5.3. Utilizzare in modo creativo le tecnologie digitali	<p>Avanzato 5 Oltre a fornire supporto agli altri, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Applicare diverse modalità per proteggere sé stesso e gli altri da pericoli negli ambienti digitali. - Mostrare diverse tecnologie digitali per il benessere sociale e l'inclusione sociale. - Applicare diversi strumenti e tecnologie digitali per creare know-how e processi e prodotti innovativi. 	<p>Creare una campagna digitale sui possibili rischi per la salute.</p> <p>Guidare ed elaborare applicativi originali con un linguaggio semplice.</p>

QUINTO ANNO

AREA DI COMPETENZA	COMPETENZA	LIVELLO DI PADRONANZA	ABILITÀ	ATTIVITÀ: ESEMPIO D'USO
COMUNICAZIONE E COLLABORAZIONE	2.2. Condividere informazioni attraverso le tecnologie digitali	Avanzato 6 A un livello avanzato, secondo i suoi fabbisogni e quelli degli altri, all'interno di contesti complessi, lo studente è in grado di:	<ul style="list-style-type: none"> - Valutare le tecnologie digitali più appropriate per condividere informazioni e contenuti. - Adeguare il suo ruolo intermediario. - Variare l'utilizzo delle prassi di riferimento e di attribuzione più appropriate. - Proporre servizi per partecipare alla vita sociale. 	<p>Utilizzare la piattaforma di apprendimento digitale della scuola per condividere informazioni a livello del gruppo classe.</p> <p>Attivare forma di scrittura collaborativa ai fini didattici da condividere con il gruppo classe (brevi relazioni, sintesi, mappe concettuali e/o mappe mentali, presentazioni sui nodi concettuali, ecc.).</p> <p>Elaborare eBook. Informare i compagni di classe e mostrare come utilizzare piattaforme digitali (blog, wiki) per potenziare le capacità personali e professionali di partecipazione alla vita sociale.</p>
	2.3. Esercitare la cittadinanza attraverso le tecnologie digitali	Avanzato 5 Oltre a fornire supporto agli altri, lo studente è in grado di:	<ul style="list-style-type: none"> - Utilizzare tecnologie digitali appropriate per potenziare le sue capacità personali e professionali e partecipare come cittadino alla vita sociale. - Individuare un'identità digitale. 	<p>Elaborare un Wiki journal e promuovere il giornalismo partecipativo dal basso anche per promuovere iniziative culturali e sociali.</p>
	2.6. Gestire l'identità digitale	Base 2 A livello base, in autonomia e con un supporto adeguato, laddove necessario, lo studente è in grado di:	<ul style="list-style-type: none"> - Descrivere modi semplici di proteggere la sua reputazione online. - Riconoscere dati semplici che produce attraverso strumenti, ambienti o servizi digitali. - Distinguere tra una serie di identità digitali ben definite e sistematiche. 	<p>Utilizzare l'account della piattaforma Gsuite della scuola per comunicazioni con i compagni di Istituto con consapevolezza e responsabilità sulla gestione dell'identità digitale.</p> <p>Riconoscere azioni che potrebbero danneggiare la reputazione degli studenti e della scuola.</p>
			Intermedio 3 Da solo e risolvendo problemi diretti, lo studente è in grado di:	<ul style="list-style-type: none"> - Spiegare modalità ben definite e sistematiche per tutelare la sua reputazione online. - Descrivere dati ben definiti che produce in modo sistematico attraverso strumenti, ambienti o servizi digitali. - Modificare contenuti digitali utilizzando i formati più appropriati.
CREAZIONE DI CONTENUTI DIGITALI	3.1. Sviluppare contenuti digitali	Avanzato 6 A un livello avanzato, secondo i suoi fabbisogni e quelli degli altri, all'interno di contesti complessi, lo studente è in grado di:	<ul style="list-style-type: none"> - Adattare i suoi atti espressivi attraverso la creazione di materiali digitali più opportuni. - Lavorare con contenuti e informazioni nuovi e diversi, modificandoli, affinandoli, migliorandoli e integrandoli per crearne di nuovi e originali. 	<p>Preparare una presentazione o un video su un determinato argomento.</p> <p>Preparare un prodotto digitale per la fruizione collettiva e pubblicarlo in contesti protetti.</p>
	3.2. Integrare e rielaborare contenuti digitali	Avanzato 5 Oltre a fornire supporto agli altri, lo studente è in grado di:	<ul style="list-style-type: none"> - Discutere regole di copyright e licenze da applicare a informazioni e contenuti digitali. 	<p>Creare brevi tutorial.</p>
	3.3. Copyright e licenze	Intermedio 4 In modo indipendente, secondo i suoi fabbisogni e risolvendo problemi ben definiti e non sistematici, lo studente è in grado di:	<ul style="list-style-type: none"> - Adottare diverse regole di copyright e licenze da applicare a dati, informazioni e contenuti digitali. 	
	3.4. Programmazione	Intermedio 4 In modo indipendente, secondo i suoi fabbisogni e risolvendo problemi ben definiti e non sistematici, lo studente è in grado di:	<ul style="list-style-type: none"> - Elencare le istruzioni per un sistema informatico per risolvere un problema diverso e svolgere compiti diversi. 	
		Avanzato 5 Oltre a fornire supporto agli altri, lo studente è in grado di:	<ul style="list-style-type: none"> - Operare con istruzioni per un sistema informatico per risolvere un problema diverso o svolgere compiti diversi. 	

SICUREZZA	4.2. Proteggere i dati personali e la privacy	<p>Avanzato 6 A un livello avanzato, secondo i suoi fabbisogni e quelli degli altri, all'interno di contesti complessi, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Scegliere le modalità più appropriate per proteggere i suoi dati personali e la privacy negli ambienti digitali. - Valutare le modalità più appropriate per utilizzare e condividere informazioni personali proteggendo sé stesso e gli altri da danni. - Valutare l'adeguatezza delle clausole della politica sulla privacy inerenti le modalità di utilizzo dei dati personali. - Creare soluzioni a problemi complessi con definizione limitata, inerenti la protezione dei dati personali e della privacy negli ambienti digitali, l'utilizzo e la condivisione di informazioni personali tutelando sé stessi e gli altri da pericoli e le politiche sulla privacy per l'utilizzo dei suoi dati personali. 	<p>Scegliere le modalità più appropriate per proteggere i suoi dati personali prima di condividerli.</p> <p>Valutare se le modalità con cui vengono utilizzati i suoi dati personali sono appropriate e accettabili per tutelare i suoi diritti e la sua privacy.</p>
	4.3. Proteggere la salute e il benessere	<p>Altamente specializzato 7 A un livello altamente specializzato, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Integrare le sue conoscenze per fornire un contributo alle pratiche e alle conoscenze professionali e fornire supporto ad altri nella protezione dei dati personali e della privacy. - Distinguere le modalità più appropriate per evitare rischi per la salute e minacce al benessere psico-fisico quando si utilizzando le tecnologie digitali. 	<p>Utilizzo di account e di piattaforme di apprendimento digitali con la consapevolezza di ogni azione in merito alla protezione dei dati personali e della privacy.</p> <p>Saper superare situazioni complesse che possono verificarsi con i propri dati personali e quelli dei propri compagni fornendo supporto ad altri nella protezione dei dati personali e della privacy.</p>
RISOLVERE PROBLEMI	5.1. Risolvere problemi tecnici	<p>Avanzato 6 A un livello avanzato, secondo i suoi fabbisogni e quelli degli altri, all'interno di contesti complessi</p>	<ul style="list-style-type: none"> - Adattare le modalità più appropriate per proteggere sé stesso e gli altri da pericoli negli ambienti digitali. - Variare l'utilizzo delle tecnologie digitali per il benessere sociale e l'inclusione sociale. - Creare soluzioni a problemi complessi con definizione limitata finalizzate a eliminare anomalie tecniche che si verificano quando si utilizzano i dispositivi e gli ambienti digitali. 	<p>Controllare la divulgazione di dati sensibili durante le attività didattiche.</p> <p>Indicare i comportamenti a rischio eventualmente adottati dai compagni di classe durante le attività didattiche.</p> <p>Trovare soluzioni per sé stessi e per gli altri per evitare rischi per la salute e minacce al benessere psico-fisico durante le attività didattiche.</p>
	5.2. Utilizzare in modo creativo le tecnologie digitali	<p>Altamente specializzato 7 A un livello altamente specializzato, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Integrare le sue conoscenze per fornire un contributo alla prassi e alle conoscenze professionali e fornire supporto ad altri nella risoluzione dei problemi tecnici. - Adattare gli strumenti e le tecnologie digitali più appropriati per creare know-how e innovare processi e prodotti. 	<p>Individuare un semplice problema tecnico da un elenco di problemi che possono verificare quando si utilizza una piattaforma di apprendimento digitale, e individuare il tipo di supporto IT capace di risolverlo.</p> <p>Utilizzare le esperienze pregresse per risolvere i problemi che si incontrano nell'uso delle tecnologie digitali.</p> <p>Compiere dei procedimenti di analisi delle criticità e padroneggiare le possibili soluzioni.</p>
	5.3. Utilizzare in modo creativo le tecnologie digitali	<p>Avanzato 6 A un livello avanzato, secondo i suoi fabbisogni e quelli degli altri, all'interno di contesti complessi, lo studente è in grado di:</p>	<ul style="list-style-type: none"> - Risolvere individualmente e collettivamente problemi concettuali e situazioni problematiche negli ambienti digitali. 	<p>Utilizzare piattaforme di e-learning o di condivisione cloud in ambito didattico (Gsuite e Classroom) anche in modalità flipped con materiali predisposti dai docenti.</p> <p>Allegare materiale didattico o un compito in ambiente cloud.</p> <p>Creare libri digitali attraverso software open source e tool vari.</p>

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.

L'Istituto mette a disposizione, nell'apposita sezione del proprio sito web, il nuovo KIT DIDATTICO fornito da Generazioni Connesse (Safer Internet Centre - MIM). Per assicurarne un utilizzo efficace e consapevole, la scuola si impegna a promuovere percorsi formativi e/o webinar specifici, garantendo ai docenti un accesso flessibile, immediato e mirato alle risorse disponibili. Il KIT DIDATTICO, integrato dalle "pillole scientifiche", si configura come uno strumento fondamentale per l'attività in aula, supportando l'attuazione del Curriculum digitale d'istituto. L'adozione di queste risorse mira a consolidare un approccio didattico innovativo, capace di rendere l'apprendimento più dinamico, inclusivo e coinvolgente.

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

3.1 - Protezione dei dati personali e GDPR

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

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

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

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

"Il sistema educativo di istruzione e formazione, dalla scuola dell'infanzia all'università, rappresenta una risorsa preziosa per il nostro Paese, che ha il fine di assicurare l'effettività del fondamentale diritto all'istruzione, offrendo ai giovani le competenze e le conoscenze necessarie all'inserimento nella vita economica e sociale, ma anche accompagnando la loro crescita e la loro maturazione. In un contesto in cui l'innovazione tecnologica rivoluziona i processi formativi - dall'uso del web ai tablet su cui consultare i libri, dai sistemi di messaggistica e i social media al registro elettronico - resta centrale la necessità di riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà e rispetto, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino di oggi e di domani." (Documento di indirizzo "La scuola a prova di privacy", che attualizza e amplia i contenuti già presenti nel vademecum diffuso nel 2023)

La protezione dei dati personali è un vero e proprio diritto fondamentale. La Carta dei Diritti Fondamentali dell'Unione, quanto il Trattato sul funzionamento dell'Unione Europea sanciscono che ogni individuo ha diritto alla protezione dei dati personali che lo riguardano.

Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi alle attuali norme di riferimento in materia privacy, al Regolamento Europeo 2016/679 meglio conosciuto come "GDPR" e il Decreto Legislativo n.101 del 2018.

Pertanto il nostro Istituto individua delle Linee Guida che disciplinano il trattamento dei dati personali gestiti:

Predisposizione e condivisione con l'intera comunità scolastica di un'informativa che illustri il ruolo del DPO, la tipologia di dati raccolti, il loro utilizzo e il fine per cui vengono utilizzati.

Predisposizione di apposito regolamento che disciplina l'uso di immagini e video. All'atto dell'iscrizione è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video. I nomi completi di alunne e alunni saranno evitati sul sito web come pure nei blog, forum e wiki, in particolare se in associazione con le loro fotografie.

Predisposizione di una liberatoria specifica per la condivisione di immagini e video durante eventi a carattere pubblico particolarmente rilevanti.

Predisposizione di una liberatoria specifica per la condivisione di elaborati ai fini della partecipazione a concorsi e a eventi pubblici.

Predisposizione di liberatorie specifiche, contenenti le modalità di trattamento, la conservazione dei dati raccolti e le misure di sicurezza adottate per la somministrazione di questionari di ricerca e per la partecipazione ad attività che coinvolgono personale esterno alla scuola.

Messa a disposizione dei genitori sul sito istituzionale del modello di reclamo al Garante per la protezione dei dati personali in caso di violazioni in materia di cyberbullismo.

Regolamentazione sull'uso di dispositivi in grado di registrare gli strumenti compensativi previsti nei PDP/PEI.

Inoltre:

- 1) Creazione sul sito di due "Aree riservate", una per i Docenti e una per il Consiglio di Istituto.
- 2) Definizione, sul sito istituzionale della scuola, di una specifica sezione dedicata Documento di ePolicy.
- 3) Pubblicazione, nella sezione Privacy, delle informative: agli studenti e alle loro famiglie al personale ai fornitori specifica per l'uso di G Suite (o altra piattaforma simile) per la attività didattiche a distanza e documentali.
- 4) Pubblicazione, nella sezione Privacy, dei dati del DPO (nominativo, PEO, PEC, riferimento telefonico)

A differenza di quanto si potrebbe credere la normativa privacy non tende a limitare la circolazione delle informazioni anzi, l'esatto opposto. Questa normativa si pone come obiettivo fondamentale quello di favorire la circolazione delle informazioni all'interno dell'Unione Europea, ponendo tutta una serie di parametri e tutele a protezione degli individui.

L'obbligo dell'informativa è sancito dall'art. 13 del GDPR. Mediante questo documento, la scuola fornisce all'interessato, vale a dire persona fisica cui si riferiscono i dati personali oggetto di trattamento, tutta una serie di informazioni.

Premesso che la scuola non è tenuta a richiedere il consenso laddove il trattamento dei dati personali viene effettuato per perseguire delle finalità di natura istituzionale, in quanto ciò è previsto dalla legge. Il consenso privacy diventa necessario laddove la scuola intenda effettuare un trattamento di dati personali finalizzato ad attività che non rientrano tra quelle istituzionali o didattiche, come ad esempio l'organizzazione di corsi di musica, di corsi teatrali o comunque attività che non rientrano in quello che è il curriculum scolastico.

Pertanto in adempimento a quanto previsto dal GDPR abbiamo introdotto nella nostra scuola un responsabile esterno della protezione dei dati personali (DPO). Questo soggetto, dotato di particolari competenze rispetto alla protezione dei dati personali, è dotato di autonomia rispetto al Titolare del trattamento. Nell'ambito del suo mandato il DPO informa e fornisce consulenza all'istituto scolastico e ai suoi dipendenti, in merito alla normativa in materia di protezione dei dati personali. Inoltre sorveglia che all'interno dell'istituto scolastico tale normativa sia rispettata, forma il personale scolastico, ha la possibilità di rilasciare pareri e comunque funge da punto di contatto tra Autorità Garante per la Protezione dei Dati Personali e la scuola.

Inoltre la nostra scuola adempie alla normativa prevista tenendo un registro dei trattamenti, vale a dire un documento di sintesi, in cui sono riportate tutte le informazioni sui trattamenti effettuati e sulle categorie di dati trattati e ha predisposto una procedura per la gestione delle violazioni dei dati personali. Questa procedura consente alla scuola di reagire prontamente in caso di violazione dei dati

personali.

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.

Regolamento P.U.A. (Politica d'Uso Accettabile della Rete)

Il presente documento sulla Politica d'Uso Accettabile per la rete, che fa parte delle strategie delle TIC (Tecnologie dell'Informazione e della Comunicazione) è stato concepito nell'osservanza degli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni (D. Lgs. 33/2013).

Il documento è parte integrante del Regolamento di Istituto e sarà portato a conoscenza dei genitori, degli allievi e di tutto il personale della scuola e da loro sottoscritto; con questo atto si intende attivare e mantenere una "Politica di uso accettabile" (PUA) in materia di "Tecnologie dell'Informazione e della Comunicazione" (TIC) da tutti condivisa, con l'obiettivo di definire all'interno dell'istituzione scolastica delle regole chiare, funzionali ed che incoraggino un uso consapevole e critico delle tecnologie informatiche.

Il presente documento è stilato sulla base delle direttive ben precise del ministero dell'Istruzione e si poggia sulla normativa vigente.

Contenuti

1. **I vantaggi di Internet a scuola**
2. **Accertamento dei rischi e valutazione dei contenuti di Internet**
3. **Le strategie della scuola per garantire la sicurezza delle TIC**
4. **Norme e linee guida**
5. **La gestione del sito dell'Istituto**
6. **Servizi on line alle Famiglie / Utenti esterni**
7. **Altre tecnologie di comunicazione**

8. **Informazioni per gli Studenti sulla PUA dell'Istituto**
9. **Informazioni per il Personale scolastico sulla PUA dell'Istituto**
10. **Informazioni per i Genitori/Tutori sulla PUA dell'Istituto**

Art.1- I vantaggi di Internet a scuola

Considerazioni generali

L'uso di Internet e delle tecnologie informatiche nella didattica e nell'organizzazione generale della scuola è prassi consolidata da anni: a scuola ci si connette alla rete sia per svolgere significative esperienze formative, sia per condurre in modo più efficiente le funzioni amministrative.

Il curriculum scolastico prevede che gli studenti imparino a trovare materiale, recuperare documenti e scambiare informazioni utilizzando le TIC. Internet offre sia agli studenti che agli insegnanti una vasta scelta di risorse, condivisione dei materiali, strumenti di comunicazione e opportunità di scambi culturali con realtà di altri paesi.

Inoltre, su Internet si possono recuperare risorse per il tempo libero, le attività scolastiche e sociali. Analogamente la Pubblica Amministrazione interconnette i suoi Uffici centrali e periferici attraverso la rete.

Non si può d'altro canto ignorare che Internet è anche una potenziale fonte di rischi, soprattutto se gli utenti non posseggono adeguata consapevolezza delle funzioni, delle norme e dei pericoli connessi alla Rete.

La scuola inoltre è dotata di un complesso sistema di computer in rete, a cui afferiscono aule, laboratori, uffici amministrativi; pertanto, si devono considerare non solo i pericoli presenti in Internet, ma anche quelli relativi alla rete interna dell'Istituto, il cui uso improprio può generare problemi nella didattica e/o nei servizi, con conseguenti danni funzionali ed economici.

Art. 2 -Accertamento dei rischi e valutazione dei contenuti di Internet

Pur nella consapevolezza che l'Istituto non può farsi carico della responsabilità dell'uso improprio della rete, esso mette in atto tutte le precauzioni necessarie per garantire agli studenti l'accesso al materiale appropriato e per limitare:

- rischi relativi all'utilizzo della rete da parte di personale non autorizzato ad accedere ai dati;
- rischi relativi all'accesso ai dati da parte di persone estranee all'amministrazione attraverso gli eventuali punti di ingresso/uscita verso Internet;
- rischi dovuti ad intrusioni nel sistema da parte di *hacker/racket*;
- rischi dovuti a intrusioni da parte di studenti;
- rischi di scaricamento virus e/o *trojan* per mezzo di posta elettronica e/o operazioni di *download*.

Art. 3 - Strategie della scuola per garantire la sicurezza delle TIC

Al fine di garantire una gestione il più possibile corretta delle TIC, la scuola attua le seguenti strategie.

La rete didattica è separata dalla rete amministrativa.

L'Istituto dispone di un "dominio" informatico; tutti i computer che dispongono di una scheda di rete fissa vi si devono collegare.

Il collegamento di computer portatili o palmari personali alla rete di Istituto deve essere autorizzato dal Dirigente Scolastico; l'amministratore della rete assegnerà un indirizzo IP univoco (previa comunicazione del *MAC address*) in modo da non ostacolare altri utenti della rete.

Viene limitato l'accesso e l'uso della rete interna ed esterna (Internet) secondo i normali canali di protezione presenti nei sistemi operativi e utilizzando *software* aggiuntivi come *Firewall*; in particolare il sistema tende a:

- § impedire l'accesso a siti non appropriati;
- § monitorare e tracciare i collegamenti di ogni dispositivo;
- § bloccare e/o consentire l'accesso a risorse in rete attraverso l'uso di parole chiave appropriate;
- § bloccare e/o consentire l'utilizzo di risorse *online* quali *chat*, *mail* e *forum*.

Il sistema informatico delle TIC dell'Istituto viene regolarmente controllato per prevenire ed eventualmente rimediare a possibili disfunzioni dell'*hardware* e/o del *software*, dagli amministratori della rete, con periodicità mensile.

L'utilizzo dei laboratori di informatica e multimediale è regolamentato da un apposito orario settimanale e comunque gli alunni possono accedere solo se accompagnati da docenti o in presenza del docente o dell'assistente tecnico responsabile del laboratorio.

L'insegnante di classe è responsabile di quanto avviene nelle proprie ore di laboratorio
La scuola controlla (per tramite dei docenti e degli assistenti tecnici autorizzati) regolarmente i file utilizzati, i file temporanei e i siti visitati.

Ogni utente si dota di una password personale di connessione che non deve essere divulgata.

Al termine di ogni collegamento la connessione deve essere chiusa; l'utilizzo di CD, chiavi USB e *floppy* personali deve essere autorizzato dal docente e solo dopo controllo antivirus.

In generale, il *software* utilizzabile è solamente quello autorizzato dall'Istituto, regolarmente licenziato e/o *open source*.

Il materiale didattico dei docenti può essere messo in rete, anche su siti personali collegati all'Istituto.

È vietato

- § agli allievi usare i computer in rete senza l'ausilio e il coordinamento del docente

- § scaricare file video-musicali protetti da *copyright*;
- § scaricare da Internet *software* non autorizzati
- § visitare siti non necessari ad una normale attività didattica;
- § alterare i parametri di protezione dei computer in uso;
- § utilizzare la rete per interessi privati e personali che esulano dalla didattica;
- § non rispettare le leggi sui diritti d'autore;
- § navigare su siti non accettati dalla protezione interna alla scuola.

Nonostante tali mezzi di prevenzione, non si può escludere che lo studente, durante la navigazione sui computer dell'Istituto, si imbatta in materiale non appropriato e/o indesiderato.

La scuola non può farsi carico *in toto* delle responsabilità per il materiale non idoneo trovato o per eventuali conseguenze causate dall'accesso al Web.

Gli utilizzatori devono quindi essere pienamente coscienti degli eventuali rischi cui si espongono collegandosi alla rete, riconoscendo ed evitando gli aspetti negativi, quali la pornografia, la violenza, il razzismo e lo sfruttamento dei minori.

Art. 4 - Norme e linee guida

Tutti gli utenti connessi ad Internet devono rispettare:

- la legislazione vigente applicata anche alla comunicazione su Internet;
- la *netiquette* (etica e norme di buon uso dei servizi di rete).

L'Amministratore di rete dell'Istituto controlla l'efficacia del sistema di filtraggio. L'Istituto riferisce alle autorità competenti se è stato trovato materiale illegale.

Di seguito le linee guida inserite nella PUA della scuola. Alcuni di questi consigli riguardano l'uso sicuro di Internet anche a casa.

Alunni

- § non utilizzare giochi né in locale, né in rete;
- § salvare sempre i documenti in cartelle personali e/o di classe e non sul *desktop* o nella cartella del programma in uso. Sarà cura di chi mantiene il corretto funzionamento delle macchine cancellare file di lavoro sparsi al di fuori delle cartelle personali;
- § non rivelare *online* il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della scuola;
- § non rivelare dettagli o informazioni personali propri o di altre persone, come indirizzi, numeri di telefono;
- § chiedere sempre ad un insegnante o ad un adulto il permesso di scaricare documenti da Internet;

- § chiedete sempre il permesso prima di iscriversi a qualche concorso o prima di riferire l'indirizzo della vostra scuola;
- § riferire agli insegnanti il reperimento o la ricezione di immagini offensive ed evitare di rispondere;
- § non rispondere a richieste di incontri di persona giunte via internet e riferire ad un insegnante, comunque ad un adulto: le persone incontrate in Rete sono degli estranei e non sempre sono quello che dicono di essere;
- § l'invio e la ricezione di allegati sono soggetti al permesso dell'insegnante;
- § non caricare o copiare materiale da Internet senza il permesso di un insegnante o del responsabile di laboratorio.

Insegnanti

- § evitare di lasciare le *e-mail* o file personali sui computer o sul server della scuola: lo spazio è limitato;
- § salvare sempre i lavori in cartelle personali e/o di classe e non sul desktop o nella cartella del programma in uso. Sarà cura di chi mantiene il corretto funzionamento dei dispositivi cancellare *file* al di fuori delle cartelle personali;
- § discutere con gli alunni della PUA della scuola e degli eventuali problemi che possono verificarsi nella mancata applicazione delle regole relative all'uso di Internet;
- § dare chiare indicazioni sui vari utilizzi della rete e informare gli studenti che le navigazioni saranno monitorate;
- § ricordare di chiudere la connessione di tutti i computer del laboratorio alla fine della sessione di lavoro su Internet;
- § non lasciare a lungo sul server o sul computer in uso file di grosse dimensioni e/o non più utilizzati per molto tempo onde evitare di occupare spazio eccessivo;
- § evitare di collegarsi a siti piuttosto "pesanti" dal punto di vista dell'occupazione della banda di trasmissione.

Sanzioni

La violazione delle regole stabilite dalla politica scolastica, la scuola, su valutazione del responsabile dei laboratori di informatica, del responsabile della rete informatica e del Dirigente Scolastico, comporta la temporanea sospensione dell'accesso ad Internet dell'utente per un periodo commisurato alla gravità del fatto.

La violazione o il dolo accertati, oltre all'intervento disciplinare del consiglio di classe, daranno luogo alla richiesta di risarcimento delle ore perse per ripristinare il sistema e renderlo nuovamente operante ed affidabile.

Rimangono comunque applicabili ulteriori sanzioni disciplinari, azioni civili per danni, nonché l'eventuale denuncia del reato all'autorità giudiziaria.

Nel caso di infrazione consapevole da parte dei docenti o del personale non docente sarà compito del Dirigente Scolastico intervenire per via amministrativa secondo le norme vigenti.

Art. 5 - Gestione del sito web della scuola

Il *webmaster* e i collaboratori interni gestiscono il sito e la pagina Facebook dell'Istituto ed è loro responsabilità garantire

che i contenuti pubblicati siano accurati e appropriati.

Il sito assolverà alle linee guida sulle pubblicazioni dell'Istituto.

L'Istituto detiene i diritti d'autore dei documenti pubblicati, oppure è legittimato ad utilizzarli avendo chiesto ed ottenuto il permesso all'autore proprietario.

Le informazioni pubblicate sul sito e sulla pagina *social* dell'Istituto relative alle persone devono includere solo l'indirizzo di posta elettronica e il telefono dell'Istituto, ma non informazioni relative agli indirizzi del personale della scuola o altre informazioni del genere.

L'Istituto non pubblicherà materiale prodotto dagli studenti o le loro fotografie senza il permesso dei loro genitori o tutori. Le fotografie degli studenti selezionate attentamente facendo attenzione al rispetto della *privacy* e dei dati sensibili.

Art. 6 - Servizi on line alle Famiglie / Utenti esterni

La scuola offre (all'interno del proprio sito web) tutta una serie di servizi alle famiglie ed agli utenti esterni:

- orari delle classi, dei docenti, delle strutture;
- informazioni sulle iniziative e sui progetti;
- comunicazioni alle famiglie;
- reperimento modulistica;
- registro elettronico

Si precisa che tutti i servizi offerti non trattano dati sensibili, ovvero dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Art. 7 - Altre tecnologie di comunicazione

Agli studenti non è permesso utilizzare i telefoni cellulari a scuola.

Art. 8 - Informazioni per gli Studenti sulla PUA dell'Istituto

Le regole di base relative all'accesso ad Internet verranno espone vicino al laboratorio di informatica. Gli studenti saranno informati che l'utilizzo di Internet è monitorato e verranno date loro delle istruzioni per un uso responsabile e sicuro. Gli studenti e i loro genitori/tutori devono firmare il documento.

Art. 9 - Informazioni per il Personale scolastico sulla PUA dell'Istituto

Al personale scolastico sarà data copia della Politica d'Uso Accettabile dell'Istituto e sarà informato che l'uso di Internet verrà monitorato e segnalato. Tutto il personale scolastico sarà coinvolto nello sviluppo delle linee guida della Politica

d'Uso Accettabile dell'Istituto e nell'applicazione delle istruzioni sull'uso sicuro e responsabile di Internet. In caso di dubbi legati alla legittimità di una certa istanza utilizzata in Internet, l'insegnante dovrà contattare il dirigente scolastico o il coordinatore responsabile delle TIC per evitare malintesi. Gli insegnanti saranno provvisti di informazioni concernenti le problematiche sui diritti d'autore.

Art. 10 - Informazioni per i Genitori / Tutori sulla PUA dell'Istituto

I genitori vengono informati della PUA dell'Istituto attraverso il sito web del Liceo Bonghi - Rosmini, dove è pubblicato il documento che regola l'uso accettabile e responsabile di Internet.

L'Istituto richiede ai genitori degli studenti minori di 18 anni di età il consenso all'uso di internet e alla pubblicazione dei lavori e delle fotografie del/la proprio/a figlio/a.

Gli studenti maggiorenni non hanno bisogno del consenso scritto dei genitori.

3.3 - BYOD

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

I. Regole di Utilizzo dei Dispositivi Digitali del Liceo Bonghi-Rosmini

Art. 1 - Divieto Generale di Utilizzo dei Dispositivi Elettronici Personali (Circ. MIM n. 3392 del 16 giugno 2025)

1. In stretta ottemperanza alla Circolare MIM n. 3392 del 16 giugno 2025, è severamente e tassativamente vietato l'utilizzo degli *smartphone* e di altri dispositivi elettronici personali assimilabili, durante il tempo scuola. Il divieto si applica a tutti i momenti della vita scolastica.
2. Per tutta la durata dell'orario scolastico, i dispositivi personali devono essere mantenuti completamente spenti e riposti all'interno del proprio zaino, borsa o altro contenitore personale, e non devono essere in alcun modo visibili o accessibili.
3. La mera esposizione del dispositivo sul banco, la sua tenuta in mano o la sua consultazione, costituisce un'infrazione

disciplinare e sarà sanzionata secondo quanto previsto dall'Art. 15 del presente Regolamento.

4. L'Istituto non fornisce alcun servizio di custodia per i dispositivi personali e, pertanto, non si assume alcuna responsabilità in caso di furto, smarrimento o danneggiamento dei dispositivi introdotti a scuola dagli studenti e dalle studentesse. La responsabilità della custodia è e rimane esclusivamente a carico dello/a studente/essa e della sua famiglia.

Art. 2 - Autorizzazione all'Uso degli Strumenti Digitali Personali per uso didattico

In deroga al divieto generale, l'utilizzo degli strumenti digitali personali è consentito nelle seguenti condizioni:

1. Finalità esclusivamente didattica: l'uso è permesso solo per lo svolgimento di attività di apprendimento, ricerca, produzione di elaborati, consultazione di testi digitali o altre attività strettamente connesse alla programmazione didattica della disciplina.
2. È vietato agli studenti usare dispositivi di registrazione audio, videocamere o fotocamere (o dispositivi che li prevedano) per registrare media o fare foto in classe senza il permesso dell'insegnante. Agli studenti non è permesso usare i dispositivi per giochi durante le ore scolastiche né utilizzare il cellulare per chiamate, sms, o messaggistica in genere. Scaricare musica, video e programmi da internet o qualsiasi file senza il consenso dell'insegnante. Audio e video registrati a scuola a fini didattici possono essere pubblicati esclusivamente in canali di comunicazione dell'Istituto
3. Autorizzazione esplicita del docente: l'utilizzo deve avvenire su esplicita e puntuale richiesta del docente presente in aula, che ne autorizza l'accensione e l'impiego per un tempo definito e per compiti specifici.
4. Supervisione costante: l'attività deve svolgersi sotto la costante vigilanza del docente, che ha il compito di assicurare che l'uso del dispositivo rimanga circoscritto alle finalità autorizzate. Al termine dell'attività didattica per cui è stato autorizzato, o su semplice richiesta del docente, il dispositivo deve essere immediatamente riposto. Qualsiasi utilizzo dei dispositivi per scopi personali durante le ore di lezione costituisce una grave infrazione disciplinare.

Art. 3 - Aree e Momenti di Applicazione

Il presente Regolamento si applica in modo vincolante in tutti gli spazi dell'Istituto. Le norme restano valide durante l'intero arco temporale in cui gli studenti e le studentesse sono affidati alla responsabilità della scuola, comprendendo quindi non solo l'orario delle lezioni, ma anche tutte le attività didattiche ed educative organizzate dall'Istituto, quali uscite didattiche, visite guidate, viaggi d'istruzione, attività sportive e progetti pomeridiani. Durante tali attività, l'uso dei dispositivi personali rimane vietato, salvo diverse e specifiche indicazioni fornite dai docenti accompagnatori per motivate esigenze organizzative o di sicurezza.

II. Ruoli, Responsabilità e Sicurezza

Art. 4 - Responsabilità della Scuola

L'Istituzione Scolastica si impegna a:

1. Fornire e mantenere un'infrastruttura di Rete Scolastica Wi-Fi sicura, stabile e dotata di adeguati sistemi di filtraggio dei contenuti, per i dispositivi gestiti dalla scuola.
2. Organizzare e promuovere attività di formazione continua per il personale docente, finalizzate allo sviluppo di competenze metodologico-didattiche per l'integrazione efficace e innovativa delle tecnologie nell'insegnamento.
3. Assicurare la periodica revisione del presente Regolamento e del Patto Educativo di Corresponsabilità, al fine di mantenerli aggiornati rispetto all'evoluzione normativa e tecnologica.
4. Nominare un Responsabile della Protezione dei Dati e definire chiaramente ruoli e procedure per la gestione della *privacy*, come previsto dalla normativa vigente.

Art. 5 - Responsabilità dei Docenti e delle Docenti

Il personale docente svolge un ruolo centrale nell'attuazione del presente Regolamento. A ciascun docente è richiesto di:

1. Autorizzare, guidare e supervisionare attivamente l'uso dei dispositivi durante le lezioni, stabilendo con chiarezza gli obiettivi, i tempi e le modalità di lavoro, e indicando esplicitamente quando i dispositivi devono essere utilizzati e quando riposti.
2. Esercitare il dovere di vigilanza, assicurando che gli studenti e le studentesse utilizzino i dispositivi in modo corretto e conforme alle regole, e intervenendo tempestivamente in caso di abusi.
3. Segnalare al Dirigente Scolastico, tramite annotazione sul registro elettronico, ogni infrazione al presente Regolamento, al fine di avviare il procedimento disciplinare previsto.
4. Svolgere un'azione educativa costante, promuovendo tra gli studenti e le studentesse la conoscenza e il rispetto dei principi di cittadinanza digitale, quali la *netiquette*, la tutela della *privacy* propria e altrui, il rispetto del diritto d'autore e la prevenzione dei rischi *online*.

Art. 6 - Responsabilità degli Studenti e delle Studentesse

Ogni studente e studentessa è tenuto/a a:

1. Rispettare scrupolosamente e in ogni sua parte il divieto di utilizzo dei dispositivi digitali per uso personale.
2. Utilizzare gli strumenti digitali esclusivamente per le finalità didattiche, nei tempi e secondo le modalità indicate dal docente.
3. Adottare un comportamento responsabile e rispettoso *online*, astenendosi da qualsiasi azione che possa ledere la dignità, l'immagine o la *privacy* di altri studenti o studentesse, docenti e personale scolastico.

Art. 7 - Corresponsabilità delle Famiglie

L'efficacia del Regolamento si basa sulla stretta collaborazione tra scuola e famiglie, che devono partecipare attivamente e condividere le responsabilità, impegnandosi a:

1. Prendere attenta visione del presente Regolamento e sottoscriverlo, unitamente al Patto Educativo di Corresponsabilità, di cui esso è parte integrante. La sottoscrizione implica l'accettazione di tutte le norme in esso contenute e l'impegno a collaborare per la loro applicazione.
2. Sostenere l'azione educativa della scuola, evitando di contattare i propri figli sui loro dispositivi personali durante l'orario scolastico. Per ogni comunicazione necessaria, i canali ufficiali sono quelli della segreteria della scuola.

III. Norme Tecniche e di Comportamento

Art. 8 - Accesso alla Rete Scolastica Wi-Fi

L'accesso alla Rete Scolastica Wi-Fi è consentito esclusivamente al personale amministrativo e al personale docente.

Art. 9 - Comunicazioni e Condivisione dei Materiali

Il Sito Web di Istituto, il registro elettronico AXIOS e Google Classroom sono le piattaforme definite per la comunicazione ufficiale scuola-studente e per la condivisione di materiali didattici, compiti e avvisi. L'utilizzo di altre piattaforme per comunicazioni didattiche non è autorizzato né riconosciuto dalla scuola.

Art. 10 - Tutela della *privacy* e del Diritto d'Autore

In applicazione della normativa nazionale sulla *privacy*, si stabilisce quanto segue:

1. Divieto di registrazioni e riprese: È assolutamente vietato effettuare registrazioni audio, scattare fotografie o realizzare riprese video che coinvolgano docenti, personale ATA o compagni di classe e in generale studenti e studentesse, senza aver ottenuto il preventivo, esplicito e informato consenso di tutte le persone coinvolte e la specifica autorizzazione del docente per finalità didattiche chiaramente documentate.
2. Divieto di diffusione: La pubblicazione o la condivisione di immagini, video o audio registrati all'interno dell'ambiente scolastico su qualsiasi piattaforma esterna costituisce una gravissima violazione della *privacy* e del presente Regolamento. Tali comportamenti saranno perseguiti con sanzioni disciplinari, fatta salva la segnalazione alle autorità competenti per le eventuali responsabilità civili e penali.
3. Diritto d'Autore: È fatto obbligo a tutti gli utenti di rispettare la normativa sul diritto d'autore. È vietato copiare,

scaricare, distribuire o utilizzare illegalmente *software*, testi, immagini, musica, video o qualsiasi altro materiale protetto da *copyright*. Il plagio, totale o parziale, di elaborati digitali è una grave infrazione accademica e disciplinare.

Art. 11 - Prevenzione e Contrasto del Cyberbullismo

L'Istituto adotta una politica di tolleranza zero nei confronti di ogni forma di bullismo e cyberbullismo.

1. Definizione. Qualsiasi utilizzo di un dispositivo digitale e della rete per compiere atti intenzionali e ripetuti di molestia, denigrazione, diffamazione, esclusione sociale, minaccia o prevaricazione nei confronti di altri membri della comunità scolastica è classificato come cyberbullismo e costituisce un'infrazione disciplinare di massima gravità.
2. Procedure di segnalazione. In conformità con le Leggi n. 71/2017 e 70/2024, l'Istituto ha nominato un docente referente per il contrasto al bullismo e al cyberbullismo e ha definito procedure chiare per la segnalazione e la gestione dei casi. Ogni studente e ogni studentessa che si senta vittima o sia testimone di tali atti ha il dovere di segnalarli immediatamente.
3. Azioni educative. L'Istituto si impegna a promuovere, nell'ambito dell'insegnamento dell'Educazione Civica e attraverso iniziative dedicate, percorsi formativi volti a sensibilizzare gli studenti e le studentesse sui rischi del cyberbullismo e a promuovere una cultura dell'empatia e del rispetto reciproco *online*, anche in collaborazione con enti esterni qualificati come la Polizia Postale.

IV. Infrazioni e Disposizioni Finali

Art. 12 - Sanzioni Disciplinari

Le violazioni al presente Regolamento costituiscono infrazioni disciplinari e saranno sanzionate in base alla loro gravità e all'eventuale recidiva, secondo un principio di proporzionalità e finalità educativa. Le sanzioni sono stabilite dal Dirigente Scolastico o dal Consiglio di Classe, nel rispetto delle procedure previste dallo Statuto delle Studentesse e degli Studenti. Si stabilisce la seguente progressione sanzionatoria:

1. Infrazioni lievi (es. prima violazione del divieto di uso degli *smartphone*, uso non autorizzato dei dispositivi digitali per scopi personali): - Richiamo verbale da parte del docente. - Annotazione dell'infrazione sul registro elettronico.
2. Infrazioni di media gravità (es. violazioni ripetute, rifiuto di riporre il dispositivo su richiesta del docente): - Convocazione della famiglia per un colloquio con il Coordinatore di Classe e/o il Dirigente Scolastico. - Ammonizione scritta da parte del Dirigente Scolastico.
3. Infrazioni gravi (es. realizzazione di foto/video non autorizzati, atti di cyberbullismo, accesso a siti illegali, violazione reiterata delle norme): - Sospensione dalle attività didattiche da uno a quindici giorni, deliberata dal Consiglio di Classe. Come previsto dalle recenti normative, la sospensione sarà convertita in attività formative e di "cittadinanza solidale". Tali infrazioni incideranno in modo significativo e negativo sulla valutazione del comportamento, con possibili conseguenze sulla media finale e sull'ammissione all'anno successivo o all'Esame di Maturità.

Si precisa che il personale docente e ATA non è autorizzato a sequestrare o ritirare forzatamente i dispositivi degli studenti e delle studentesse. Il personale è tenuto a segnalare l'infrazione e ad avviare l'iter disciplinare.

Art. 13 - Deroghe e Casi Particolari

In conformità con la normativa vigente e con il principio di inclusione, sono previste deroghe al presente regolamento per studenti e studentesse con bisogni educativi speciali. L'utilizzo di dispositivi specifici, inclusi gli *smartphone* qualora siano configurati come ausili medico-sanitari o come strumenti compensativi indispensabili, è consentito agli studenti e alle studentesse con disabilità certificata ai sensi della Legge 104/92 o con Disturbi Specifici dell'Apprendimento (DSA) diagnosticati ai sensi della Legge 170/2010. Tale utilizzo deve essere esplicitamente previsto, descritto e regolamentato all'interno del Piano Educativo Individualizzato (PEI) o del Piano Didattico Personalizzato (PDP) dello/a studente/essa.

Art. 14 - Integrazione del Patto Educativo di Corresponsabilità

Il presente Regolamento costituisce un allegato e parte integrante e sostanziale del Patto Educativo di Corresponsabilità dell'Istituto. All'atto dell'iscrizione, o all'inizio di ogni anno scolastico, gli studenti e le studentesse e le loro famiglie sono tenuti a prenderne visione e a sottoscrivere il Patto per accettazione. La sottoscrizione attesta la conoscenza e l'impegno al rispetto di tutte le norme qui contenute, rafforzando l'alleanza educativa indispensabile per il successo formativo degli studenti e delle studentesse. Un estratto contenente i principali doveri di studenti e studentesse e famiglie sarà allegato al modulo di sottoscrizione del Patto.

Art. 15 - Entrata in Vigore e Diffusione

Il presente Regolamento entra in vigore il giorno successivo alla sua approvazione da parte del Consiglio di Istituto. Per garantirne la massima conoscenza e diffusione, l'Istituto provvederà a

1. Pubblicarlo in modo permanente sul sito web istituzionale, nella sezione dedicata ai regolamenti.
2. Inviarlo tramite circolare a tutto il personale scolastico, a tutti gli studenti e studentesse e a tutte le famiglie attraverso il registro elettronico.
3. Organizzare, all'inizio di ogni anno scolastico, momenti informativi dedicati.

Cap 4 - Segnalazione e gestione dei casi

4.1 - Cosa Segnalare

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

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

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

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

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

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

Adescamento online: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minore 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.

Sono da considerare degni di segnalazione:

- contenuti afferenti alla violazione della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);
- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

4.2 - Quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale (ex [art. 357 c.p.](#)) in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Il Codice Penale Italiano, all'[art. 357](#), definisce il pubblico ufficiale come colui che esercita una "pubblica funzione legislativa, giudiziaria o amministrativa". Questa definizione si estende ai docenti nel momento in cui sono impegnati nell'esercizio delle loro funzioni all'interno degli istituti scolastici.

La Corte di Cassazione, con la sentenza [n. 15367/2014](#), ha ribadito la qualifica di pubblico ufficiale per l'insegnante, estendendo tale riconoscimento non solo alla tenuta delle lezioni, ma anche a tutte le attività connesse. Questo include, ad esempio, gli incontri con i genitori degli allievi.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite da un team di docenti composto da:

1. Dirigente
2. Docente referente,
3. L'animatore digitale (secondo il Piano Nazionale per la Scuola Digitale, abbreviato in PNSD, introdotto dalla Legge 107/2015)
4. Referente bullismo (ex. Legge Italiana Contro il Cyberbullismo, l. 71/2017)
5. Altri docenti già impegnati nelle attività di promozione dell'educazione civica.

Le situazioni di pregiudizio presunto o reale possono richiedere il supporto e l'intervento di esperti esterni alla scuola.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due macro - casi:

CASO A (SOSPETTO) - Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente. La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, il Dirigente e i docenti coinvolti procedono alla valutazione del caso (valutare l'invio o meno della relazione agli organi giudiziari preposti) e agiscono tramite percorsi di sensibilizzazione.

CASO B (EVIDENZA) - Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente. La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, si procede alla valutazione approfondita e alla verifica di quanto segnalato, avviando (se appurato la rilevanza penale) la procedura giudiziaria con denuncia all'autorità giudiziaria per attivare un procedimento penale.

Qualora si rilevasse un fatto riconducibile alla fattispecie di reato, l'insegnante - nel ruolo di pubblico ufficiale - non deve procedere con indagini di accertamento ma ha sempre l'obbligo di segnalare l'evento all'autorità giudiziaria. (ex. l. 71/2017). Con autorità competente si intendono:

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

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

La segnalazione come da procedura interna è il primo passo per aiutare un minore che vive una situazione di rischio o di grave difficoltà e va intesa come un momento di condivisione e solidarietà nei confronti del minore. La mancata segnalazione costituisce, infatti, omissione di atti d'ufficio (art.328 C.P.).

Può essere utile, valutando accuratamente ciascuna situazione, attivare colloqui individuali con tutti i minori coinvolti, siano essi vittime, testimoni e/o autori. È importante considerare il possibile coinvolgimento dei genitori e di coloro incaricati della tutela dei minori coinvolti. L'intervento va indirizzato valutando l'eventuale impatto educativo e/o il contesto emotivo senza discriminare tra vittime, testimoni e/o autori.

Prevedere possibili incontri di mediazione tra i minori coinvolti vanno ponderati con la consapevolezza del loro stato emotivo, anche e in base agli elementi raccolti in merito del fatto/episodio avvenuto (elementi che si dovrebbero valutare di caso in caso). Importante è prevedere il coinvolgimento dei genitori sia della vittima che del bullo (ove possibile).

Anche i genitori devono e possono segnalare casi di sospetto o evidenza dei fenomeni, segnalarlo al Dirigente, o al docente coordinatore di classe o referente di istituto oppure direttamente al team antibullismo attraverso apposita procedura che definisce l'istituto (mail ad hoc, tramite gli uffici e postazioni specifiche, etc...).

Gli insegnanti e i genitori, come studenti e studentesse, si possono rivolgere alla Helpline del progetto Generazioni Connesse, al numero gratuito 19696, attraverso la chat disponibile sul [sito](#) o tramite chat WhatsApp per ricevere supporto e consulenza. Per tutti i dettagli, il riferimento è agli allegati con le procedure.

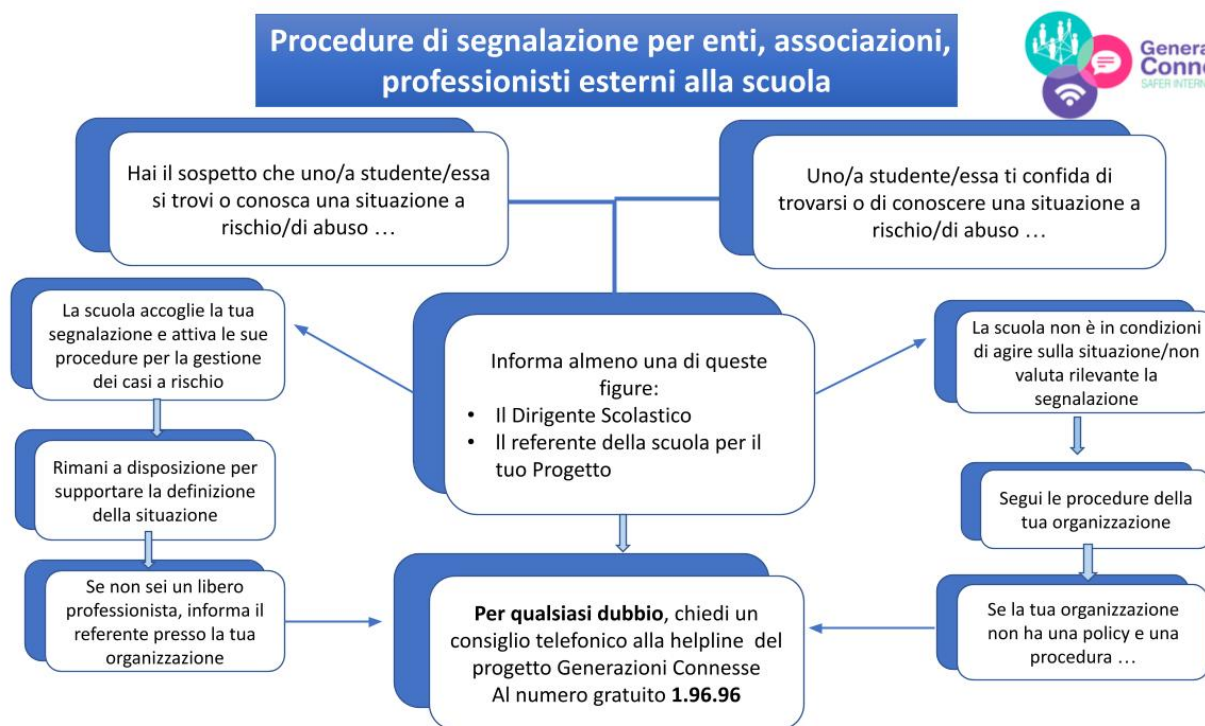
Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola; sportello di ascolto con professionisti; docente referente per le segnalazioni.

In particolare, sarebbe utile che la scuola attivi un sistema di segnalazione utile anche al monitoraggio dei fenomeni dal quale partire per integrare azioni didattiche preventive e giornate di sensibilizzazione, insieme agli Enti/Servizi presenti sul territorio di riferimento. Importante, altresì, immaginare e programmare percorsi di peer education per la prevenzione e il contrasto degli agiti.

Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle [Linee di Orientamento per la prevenzione e il contrasto dei fenomeni di Bullismo e Cyberbullismo del MI \(Ministero dell'Istruzione\)](#) aggiornate al 2021, al Patto educativo di corresponsabilità e annessa appendice relativa agli impegni che le parti in causa dovranno assumere per l'espletamento efficace della DID e, in ultimo, al Piano scolastico per la Didattica Digitale Integrata, allegato al PTOF.

Procedure



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo



Il docente ha evidenza che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Se non è già stato fatto, avvisa il referente per il cyberbullismo (e/o il team antibullismo) che attiva le procedure ("Corso 4" della piattaforma ELISA) e il Dirigente Scolastico.

Ricordare sempre che in base alla legge 71-2017:

A) Se c'è fattispecie di reato va fatta la segnalazione alle forze dell'ordine

B) Se non c'è fattispecie di reato.

Il DS (e/o il team antibullismo):

- informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto) su quanto accade e 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.

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 valutata se

- affrontare direttamente l'accaduto o
- sensibilizzare la classe (vedi Corso 4 Piattaforma Elisa)
- trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.

A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla Polizia Postale:

a) contenuto; b) modalità di diffusione.

Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



Il docente riceve una segnalazione (da un genitore, un altro studente ...) o sospetta che stia accadendo qualcosa a uno/a studente/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

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

Condividi con il referente o al team antibullismo: si attiva il processo di attenzione e valutazione a cura del referente.

- Insieme si valuta se è il caso
- di avvisare il consiglio di classe;
 - di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.

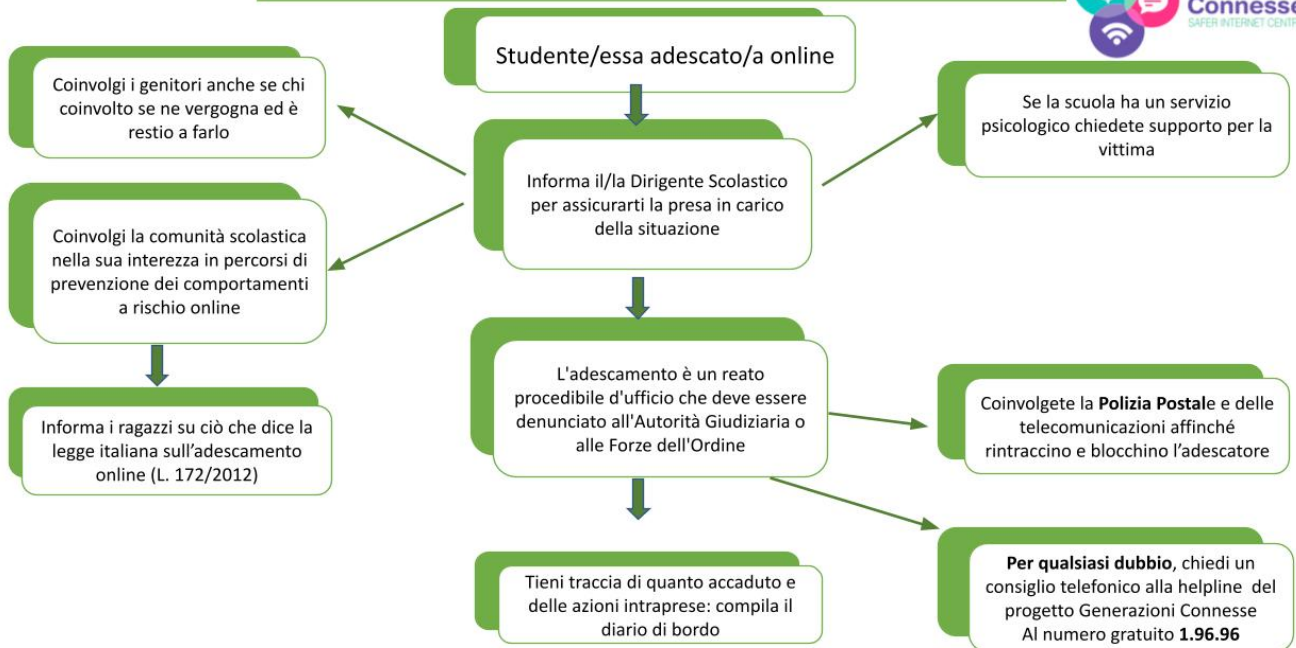
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

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

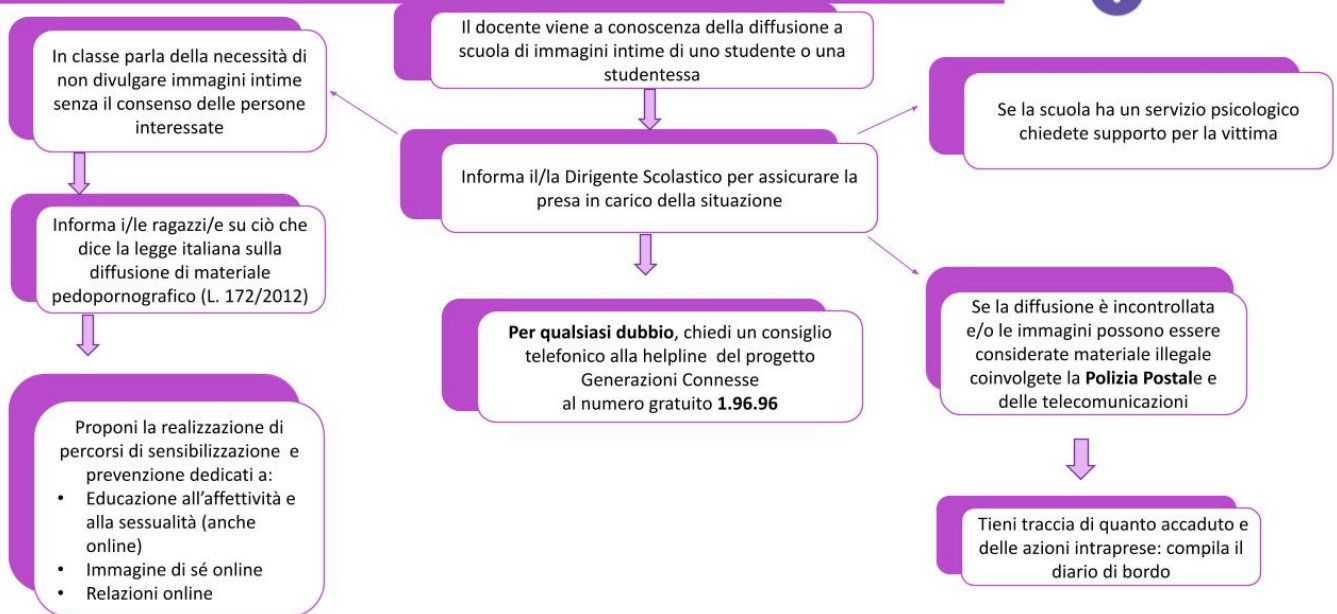
Se emergono evidenze passa allo schema successivo

Ricorda a studenti/esse che possono chiedere in qualsiasi momento una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 o via chat

Procedure interne: cosa fare in caso di Adescamento Online?



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



Il Liceo Bonghi-Rosmini ha individuato i docenti del Team Anti Bullismo e Cyberbullismo che faranno da supporto agli altri docenti nella formazione e il monitoraggio degli eventuali casi e i docenti del Team per l'Emergenza che valuteranno in maniera approfondita le segnalazioni e sceglieranno la strategia di intervento più opportuna.

Ritenendo fondamentale coinvolgere tutti gli studenti e le studentesse nel contrasto ai fenomeni di bullismo e cyberbullismo, il Liceo Bonghi Rosmini fa partecipare tutte le classi prime in un progetto di sensibilizzazione e formazione per il contrasto al bullismo e al cyberbullismo. Inoltre il Liceo Bonghi Rosmini riconosce come credito formativo l'attestato di formazione rilasciato dalla piattaforma Generazioni connesse agli studenti che hanno completato il percorso formativo online sul tema del contrasto al bullismo e cyberbullismo.

Il sito della scuola include una sezione dedicata alla prevenzione e al contrasto del bullismo e del cyberbullismo, intitolata "Stop Bullying". All'interno di quest'area vengono presentate le attività realizzate, le iniziative formative e i progetti di sensibilizzazione promossi dall'istituto sul tema.

La sezione raccoglie inoltre tutta la documentazione utile per l'attuazione del protocollo scolastico, tra cui:

- a) la modulistica per la prima segnalazione, la valutazione approfondita e il monitoraggio;
- b) il documento di e-policy dell'Istituto;
- c) il protocollo di intervento in situazioni di bullismo e cyberbullismo.

La prima segnalazione può essere effettuata da qualsiasi docente, dai genitori/tutori e, nella secondaria, dagli stessi studenti e ha lo scopo tenere una traccia della presa in carico della situazione e delle prime informazioni sull'accaduto. Il **MODULO DI PRIMA SEGNALAZIONE**, reperibile nella sezione Stop bullying del sito della scuola deve essere compilato e consegnato all'indirizzo mail **fgpc1500c@istruzione.it** all'attenzione del referente d'istituto per il bullismo.

In ottemperanza a quanto stabilito dall'articolo 4 della Legge n. 70/2024, il Liceo Bonghi Rosmini ha formalmente istituito il **Tavolo Permanente di Monitoraggio** (come previsto dal comma 2-bis), organo composto dai rappresentanti di studenti, docenti, famiglie ed esperti.

Inoltre, l'Istituto celebra annualmente il **20 gennaio** la "**Giornata del Rispetto**", istituita con la medesima Legge 17 maggio 2024, n. 70, in memoria di Willy Monteiro Duarte. L'iniziativa è volta a promuovere attivamente la lotta al bullismo, al cyberbullismo e a ogni forma di discriminazione.