



Documento di ePolicy IC BORGONOVO VAL TIDONE

VIA SARMATO N. 1 - 29011 - BORGONOVO VAL TIDONE
Piacenza (PC) - Emilia-Romagna
Data di approvazione: 14/01/2026 - 15:27

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.

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.

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.

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, allegate e sintetiche, all'interno delle quali sono individuati gli elementi principali del documento; una versione è diretta agli studenti ed una è diretta alle famiglie con un linguaggio e una presentazione dei contenuti adeguata, flessibile e chiara. La versione sintetica rivolta agli studenti è inserita all'interno delle attività didattiche dell'educazione alla cittadinanza mentre la versione per le famiglie è consegnata nel corso dei colloqui scuola-famiglia.

Il documento è altresì pubblicato sul sito della scuola ed inserito nel Patto di corresponsabilità.

2. Come comunicare e condividere l'ePolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

La presenza dell'ePolicy nell'Istituto scolastico è garanzia, per il territorio, della presenza di un presidio informato, sensibile e attento sulla rete e le tecnologie in relazione con i più giovani.

In questo senso l'Istituto può rappresentare per le Istituzioni del territorio, le aziende, e le realtà del Terzo Settore un luogo di confronto privilegiato e di sperimentazione per tutti coloro che intendono costruire progetti di cittadinanza digitale rivolte ai più giovani.

A tal fine l'adozione dell'ePolicy è comunicata all'USR di riferimento e al Municipio (servizi istruzione e servizi sociali) attraverso gli allegati sintetici progettati che indicano gli elementi del documento e le prospettive per la comunità.

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

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

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

Cap 2 - Sensibilizzazione e prevenzione

2.1 - Sensibilizzazione e prevenzione

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

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

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

2.2 - Il Curricolo Digitale

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

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

Al suo interno vengono identificati alcuni temi sui quali è costruita una proposta specifica per le famiglie e gli studenti (formazione). Tale cornice trova poi sviluppo specifico, per gli studenti, nel 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.

1. Finalità del curriculum digitale d'istituto

Il curriculum digitale dell'Istituto nasce per:

- garantire pari opportunità di accesso alle competenze digitali, in particolare per studenti provenienti da contesti fragili;
- promuovere l'inclusione linguistica e culturale attraverso strumenti digitali accessibili;
- sviluppare competenze di cittadinanza digitale in linea con la L. 92/2019;
- favorire un uso sicuro, responsabile e critico delle tecnologie;
- sostenere famiglie e studenti con percorsi formativi dedicati, in coerenza con l'ePolicy;
- utilizzare le risorse nazionali e internazionali disponibili (PNSD, piattaforme ministeriali, repository europei, programmi Erasmus+, DigCompEdu, DigComp 2.2).

2. Cornice normativa di riferimento

Il curriculum si articola sulle 5 aree del [DigComp 2.2](#):

1. Alfabetizzazione su informazioni e dati
2. Comunicazione e collaborazione
3. Creazione di contenuti digitali
4. Sicurezza
5. Problem solving

Ogni area è declinata in obiettivi di competenza per i tre ordini di scuola.

2.1 Quadro normativo di riferimento (italiano ed europeo)

- Raccomandazioni UE sulle competenze chiave per l'apprendimento permanente
- DigComp 2.2
- L. 92/2019 - Educazione Civica
- DM 183/2024 - Nuove linee guida per l'educazione Civica
- Linee guida PNSD L. 107/2015

- Indicazioni Nazionali 2012 e successivi aggiornamenti (ultimo aggiornamento: 2025)

2.2 Regolamento d'istituto

Fa fede il Regolamento d'istituto per la regolamentazione dell'utilizzo delle tecnologie digitali, con le relative sanzioni disciplinari applicabili.

3. Principi pedagogici in base al contesto culturale

L'istituto Comprensivo di Borgonovo si caratterizza per il suo contesto socioculturale.

L'inclusione scolastica si realizza attraverso diverse strategie integrate. Un primo ambito riguarda l'**accessibilità linguistica**, che si promuove mediante l'uso di immagini, video, mappe concettuali e strumenti di traduzione, insieme alla semplificazione linguistica pensata per studenti di lingua seconda (L2) e per i neoarrivati in Italia (NAI).

Un secondo pilastro è la **didattica laboratoriale e cooperativa**, che favorisce l'apprendimento attivo, il peer tutoring e la collaborazione tra gruppi eterogenei, valorizzando le competenze di ciascuno.

Fondamentale è anche la **riduzione del divario digitale**, perseguita attraverso l'uso di device condivisi, attività offline o low-tech quando necessario e la valorizzazione delle risorse gratuite disponibili.

L'**inclusione culturale** si concretizza nella valorizzazione delle lingue madri e nella proposta di attività digitali che stimolano la narrazione e rafforzano l'identità degli studenti.

Infine, il **coinvolgimento delle famiglie** rappresenta un elemento chiave: incontri formativi multilingue, tutorial semplici e supporto pratico all'uso delle piattaforme scolastiche contribuiscono a rendere la comunità educativa più coesa e partecipativa.

4. Curricolo digitale per ordini di scuola

4.1 Scuola dell'Infanzia

Obiettivi

- Familiarizzare con strumenti digitali semplici.
- Riconoscere simboli e icone.
- Comprendere le prime regole di sicurezza.

Attività

- Uso di tablet con app educative intuitive.
- Coding unplugged (percorsi, sequenze, logica).
- Visione guidata di contenuti multimediali.

- Mini-laboratori con kit ePolicy.

Competenze DigComp 2.2

- Navigazione elementare.
- Comunicazione mediata dall'adulto.
- Prime regole di sicurezza.

4.2 Scuola Primaria

Obiettivi

- Ricerare informazioni semplici.
- Comunicare in modo rispettoso.
- Creare contenuti digitali di base.
- Comprendere i rischi online.

Attività

- Un appuntamento annuale per classe dedicato alla cittadinanza digitale.
- Uso di strumenti gratuiti (suite educative, app di disegno).
- Introduzione al coding (Scratch, attività unplugged).
- Percorsi di educazione ai media.
- Kit ePolicy: sicurezza, privacy, cyberbullismo.

Competenze DigComp 2.2

- Ricerca e valutazione di informazioni semplici.
- Collaborazione online protetta.
- Produzione di contenuti multimediali.

- Riconoscimento dei rischi digitali.

4.3 Scuola Secondaria di Primo Grado

1. Ricerca critica delle informazioni

Gli studenti imparano a:

- distinguere fonti attendibili da contenuti manipolati o falsi;
- riconoscere fake news, clickbait, manipolazioni visive e deepfake;
- comprendere l'importanza della verifica incrociata delle informazioni.

2. Uso consapevole e responsabile dei social media

L'obiettivo è sviluppare:

- consapevolezza delle dinamiche dei social (algoritmi, bolle informative, reputazione digitale);
- capacità di comunicare in modo rispettoso e conforme alla netiquette;
- conoscenza dei limiti di età, delle condizioni d'uso e dei rischi connessi.

3. Produzione di contenuti digitali complessi

Gli studenti imparano a:

- progettare e realizzare video, podcast, presentazioni multimediali;
- utilizzare strumenti digitali gratuiti e accessibili;
- rispettare copyright, licenze e citazioni.

4. Conoscenza dei diritti digitali

Gli alunni acquisiscono consapevolezza di:

- privacy e protezione dei dati personali;

- diritto all'immagine;
- responsabilità penale e civile online;
- norme su sexting, adescamento, diffusione illecita di immagini.

5. Prevenzione dei rischi online

Il curriculum affronta:

- cyberbullismo e bullismo online;
- grooming, sexting, sextortion;
- dipendenze digitali e benessere online;
- gestione dei conflitti digitali.

6. Inclusione linguistica tramite strumenti digitali

Gli studenti L2 e NAI vengono supportati con:

- strumenti di traduzione e sintesi vocale;
- dizionari digitali multilingue;
- attività multimodali (video, immagini, mappe concettuali).

7. Attività Didattiche

1. Modulo annuale di cittadinanza digitale

Ogni classe affronta un percorso strutturato che comprende:

- diritti e doveri online,
- sicurezza digitale,
- prevenzione del cyberbullismo,
- uso consapevole dei social,

- gestione dell'identità digitale.

2. Laboratori di fact-checking

Attività pratiche su:

- analisi di articoli, video e post social;
- riconoscimento di manipolazioni digitali;
- uso di strumenti di verifica (reverse image search, controlli sulle fonti).

3. Storytelling digitale (video, podcast, blog)

Gli studenti realizzano contenuti su temi come:

- sicurezza online,
- identità digitale,
- inclusione e intercultura,
- prevenzione del cyberbullismo.

4. Peer education

Studenti formati diventano "ambasciatori digitali" e:

- supportano i compagni nell'uso sicuro del digitale,
- collaborano nella prevenzione del cyberbullismo,
- partecipano a campagne interne di sensibilizzazione.

5. Percorsi per studenti NAI

Attività specifiche:

- uso di app di traduzione e dizionari digitali,
- supporto visivo e multimediale,
- creazione di glossari digitali bilingue,

- tutoraggio tra pari.

6. Incontri formativi per famiglie

Incontri multilingue su:

- uso sicuro dei social,
- rischi online,
- gestione dei dispositivi a casa,
- supporto alla comunicazione scuola-famiglia

Integrazione con il Protocollo Cyberbullismo e l'ePolicy

Questa sezione è fondamentale per rendere il curriculum coerente con le politiche interne dell'istituto. In particolare si riferisce alle norme contenute nel Regolamento d'Istituto e al Protocollo per contrastare Bullismo e Cyberbullismo dell'IC Borgonovo.

1. Prevenzione del cyberbullismo

Il curriculum integra:

- definizione e riconoscimento del cyberbullismo;
- differenza tra conflitto e comportamento aggressivo;
- responsabilità penali e civili;
- procedure interne dell'istituto in caso di segnalazione;
- ruolo del referente cyberbullismo.

2. Uso corretto dei social e delle piattaforme digitali

Gli studenti imparano a:

- rispettare la netiquette;
- evitare comportamenti rischiosi (provocazioni, flame, hate speech);
- riconoscere e segnalare contenuti inappropriati;

- gestire la propria reputazione digitale.

3. Diffusione illecita di immagini e tutela dell'identità

Il curriculum affronta in modo esplicito:

- divieto di condividere immagini di compagni senza consenso;
- rischi legati a screenshot, chat di gruppo, challenge;
- conseguenze legali della diffusione di immagini intime (anche tra minori);
- diritto all'oblio e rimozione dei contenuti.

4. Ricerche consapevoli e navigazione sicura

Gli studenti imparano a:

- evitare siti non sicuri o illegali;
- riconoscere truffe, phishing, malware;
- impostare filtri e controlli di sicurezza;
- comprendere il funzionamento dei motori di ricerca e dei suggerimenti automatici.

Riferimenti alle competenze DigComp 2.2

1. Valutazione critica delle fonti (Area 1)

- analisi dell'attendibilità delle informazioni,
- riconoscimento di manipolazioni digitali,
- uso di strategie di verifica.

2. Comunicazione responsabile (Area 2)

- rispetto della netiquette,
- gestione dei conflitti online,

- uso corretto dei social e delle piattaforme scolastiche.

3. Creazione di contenuti complessi (Area 3)

- produzione di video, podcast, presentazioni,
- rispetto del copyright,
- uso di licenze aperte.

4. Gestione della sicurezza online (Area 4)

- protezione dei dati personali,
- prevenzione dei rischi (cyberbullismo, sexting, phishing),
- consapevolezza dei diritti digitali.

5. Problem solving digitale (Area 5)

- risoluzione di problemi tecnici,
- uso strategico degli strumenti digitali,
- pensiero computazionale.

2.3 - Il Kit Didattico

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

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

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

3.1 - Protezione dei dati personali e GDPR

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

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

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

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

Si fa riferimento al documento [INSERIRE ESTREMI DEL REGOLAMENTO PRIVACY FORNITO DAL DPO]

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.

Ambito di applicazione

Il presente regolamento si applica a:

- Studenti e studentesse di ogni ordine e grado dell'Istituto Comprensivo
- Docenti e personale ATA
- Dirigente scolastico
- Educatori, esperti esterni e collaboratori che operano in contesto scolastico
- Famiglie, per quanto riguarda l'uso della rete e dei dispositivi in ambito domestico connesso alle attività scolastiche

2. Principi generali

L'uso della rete e delle tecnologie digitali deve essere:

- Responsabile, evitando comportamenti che possano arrecare danno a sé o agli altri
- Consapevole, con attenzione ai rischi online e alla qualità delle informazioni
- Etico, nel rispetto dei diritti d'autore, della privacy e della dignità delle persone
- Sicuro, seguendo le indicazioni fornite dalla scuola per la protezione dei dati e dei dispositivi
- Coerente con la mission educativa dell'Istituto, promuovendo un clima positivo e inclusivo

3. Comportamenti consentiti

Gli utenti sono autorizzati a:

- Utilizzare la rete scolastica per attività didattiche, ricerche, progetti e comunicazioni istituzionali
- Accedere a piattaforme digitali e ambienti di apprendimento indicati dalla scuola
- Utilizzare dispositivi personali (BYOD) solo se previsto dal regolamento interno e sotto supervisione
- Segnalare tempestivamente al personale scolastico eventuali contenuti inappropriati o situazioni di rischio

1.

4. Comportamenti vietati e soggetti a sanzione

Fermo restando che l'utilizzo della rete è regolamentato dal Regolamento di Istituto e dalle regole dell'aula informatica, per ciascun utente è severamente vietato:

- Accedere, ricercare o diffondere contenuti non conformi allo stile educativo della scuola (violenti, discriminatori, pornografici, illegali)
- Utilizzare la rete scolastica per attività di gioco online o per scopi non didattici
- Commettere o tentare azioni illecite (hacking, furto di dati, accesso non autorizzato a sistemi o account)
- Violare la privacy di altri utenti (fotografare, registrare, diffondere dati personali senza consenso)
- Scaricare o condividere materiale protetto da copyright senza autorizzazione
- Utilizzare piattaforme di streaming illegali, che violino le norme vigenti in materia di copyright e diritto d'autore
- Utilizzare linguaggi offensivi, minacciosi o discriminatori nelle comunicazioni digitali
- Installare software non autorizzati sui dispositivi scolastici, anche su quei dispositivi che vengono utilizzati in classe nell'ambito del BYOD

5. Tutela dei dati personali

L'Istituto si impegna a:

- Proteggere i dati sensibili di studenti e del personale
- Utilizzare piattaforme conformi alle normative sulla privacy e alle linee guida ministeriali
- Informare famiglie e utenti sulle modalità di trattamento dei dati, in linea con le direttive del DPO (nel caso dell'Istituto Comprensivo di Borgonovo, il DPO facente capo è Vargiu Scuola)
- Garantire che ogni attività digitale avvenga nel rispetto del GDPR e delle linee guida ministeriali

Gli utenti (alunni, docenti e ATA) devono:

- Custodire con cura le proprie credenziali, evitandone la diffusione
- Non condividere password o dati personali con terzi

- Segnalare eventuali violazioni o sospetti di violazione
- Disconnettersi sempre dagli account personali in caso di postazioni condivise, su LIM, monitor touch e altri dispositivi in condivisione

6. Responsabilità

Gli studenti hanno l'obbligo di:

- Usare la rete in modo corretto e rispettoso, restando all'interno dei termini imposti dalla normativa vigente e dal Regolamento di Istituto
- Seguire le indicazioni dei docenti
- Rispettare i compagni e il personale anche negli ambienti digitali

Il personale docente ha l'obbligo di:

- Vigilare sull'uso corretto delle tecnologie
- Promuovere comportamenti digitali sicuri e consapevoli
- Segnalare eventuali violazioni

Le famiglie devono:

- Collaborare con la scuola nel monitoraggio dell'uso domestico dei dispositivi
- Favorire un clima di responsabilità digitale
- Conservare le credenziali dei propri figli (i genitori/tutori sono responsabili delle credenziali dei figli e delle azioni illecite con esse compiute)
- Comunicare con la scuola attraverso i canali istituzionali (mail istituzionale dal dominio @icborgonovo.edu.it oppure mail indicata nella delega fornita a inizio anno; registro elettronico; udienze settimanali o generali).

I professionisti esterni devono:

- Attenersi alle norme del presente regolamento
- Utilizzare la rete scolastica esclusivamente per attività autorizzate

9. Sanzioni

La violazione del presente regolamento comporta l'applicazione di misure disciplinari proporzionate alla gravità dell'infrazione, nel pieno rispetto del Regolamento di Istituto e delle sanzioni in esso previste. Le misure sono finalizzate non solo alla correzione del comportamento scorretto, ma anche alla promozione di un uso consapevole e responsabile delle tecnologie digitali.

9.1 Richiamo verbale o scritto

In caso di comportamenti non conformi alle norme della P.U.A., il docente o il personale responsabile può procedere con un richiamo verbale. Tale richiamo viene registrato per iscritto sul registro elettronico Nuvola, come previsto dalle procedure interne dell'Istituto. Il richiamo costituisce un primo livello di intervento educativo e ha lo scopo di rendere lo studente consapevole della violazione commessa.

9.2 Limitazione temporanea dell'accesso alla rete o ai dispositivi

Qualora il comportamento scorretto riguardi l'uso improprio della rete o dei dispositivi digitali, può essere applicata una limitazione temporanea dell'accesso. La durata e le modalità della limitazione vengono deliberate:

Qualora il comportamento scorretto riguardi l'uso improprio della rete o dei dispositivi digitali, può essere applicata una limitazione temporanea dell'accesso. La durata e le modalità della limitazione vengono deliberate:

- dal Consiglio di Classe per la scuola secondaria di I grado
- dal team docenti/interclasse per la scuola primaria

La misura è registrata negli atti interni e comunicata alla famiglia tramite canali istituzionali.

8.3 Comunicazione alla famiglia

Per garantire trasparenza e collaborazione educativa, la famiglia viene informata delle violazioni e delle sanzioni applicate esclusivamente attraverso canali istituzionali (registro elettronico, email istituzionale, convocazioni ufficiali). La comunicazione ha valore informativo e preventivo, favorendo un intervento congiunto scuola-famiglia.

8.4 Attivazione del protocollo disciplinare d'Istituto

In caso di infrazioni più gravi o reiterate, si procede con l'attivazione del Protocollo disciplinare dell'Istituto, che può prevedere:

- annotazioni formali
- attività riparative o educative
- colloqui con il referente digitale, il docente coordinatore o il Dirigente Scolastico
- convocazione della famiglia per un confronto strutturato

Il comportamento reiterato o particolarmente dannoso può comportare anche la sospensione dell'alunno dalle attività in aula informatica o da specifici progetti digitali, per un periodo stabilito dagli organi collegiali competenti.

8.5 Segnalazione alle autorità competenti

Nei casi più gravi, quali:

- violazioni della privacy
- accessi non autorizzati a sistemi informatici
- diffusione di contenuti illeciti

- atti configurabili come reati informatici

L'Istituto si riserva di procedere alla segnalazione alle autorità competenti, nel rispetto delle normative vigenti e del Regolamento di Istituto.

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.

L'Istituto Comprensivo di Borgonovo promuove un uso consapevole e responsabile delle tecnologie digitali, nel rispetto del Regolamento d'Istituto e delle norme vigenti. L'accesso al BYOD è una possibilità educativa, non un diritto, e può essere sospeso in caso di uso scorretto.

1. Finalità BYOD

- Favorire attività didattiche innovative.
- Sviluppare competenze digitali e cittadinanza responsabile.
- Utilizzare strumenti personali come supporto all'apprendimento, sotto la supervisione dei docenti.

2. Autorizzazione

- L'uso dei dispositivi personali è consentito solo previa autorizzazione scritta delle famiglie.
- Ogni utilizzo deve essere richiesto e approvato dal docente durante l'attività didattica.

3. Tipologia di dispositivi ammessi

- Tablet (connesso alla rete della scuola e all'account istituzionale dell'alunno).
- Notebook (connesso alla rete della scuola e all'account istituzionale dell'alunno).

4. Modalità d'uso

- I dispositivi possono essere accesi solo quando il docente lo indica.
- È vietato registrare audio, video o scattare foto senza autorizzazione esplicita dell'insegnante e delle persone coinvolte.
- È vietato l'uso per scopi personali (messaggistica, social network, giochi, telefonate).
- Il dispositivo deve altresì essere disconnesso da qualsiasi collegamento esterno allo smartphone personale.
- L'accesso a Internet avviene esclusivamente tramite la rete scolastica, quando disponibile.

5. Sicurezza e tutela della privacy

- È vietato condividere contenuti che riguardino compagni, docenti o ambienti scolastici.
- È vietato installare o utilizzare applicazioni non autorizzate durante le attività.
- Gli studenti devono rispettare le norme sul diritto d'autore e sull'uso corretto delle fonti.

6. Responsabilità

- Ogni studente è responsabile del proprio dispositivo. La scuola non risponde di furti, smarrimenti o danni.
- L'uso improprio comporta richiami, sospensione dal BYOD e ulteriori provvedimenti disciplinari secondo il Regolamento d'Istituto.

7. Custodia dei dispositivi

- I dispositivi devono rimanere spenti e riposti nell'armadietto al di fuori delle attività autorizzate. Possono essere prelevati soltanto al termine delle lezioni.
- Non è consentito l'uso negli spazi comuni (corridoi, bagni, intervallo).
- A fine giornata, i dispositivi personali devono essere riportati a casa dagli studenti. Non è consentito lasciare negli armadietti i dispositivi elettronici.

8. Alunni con BES, DSA o con disabilità certificata

- Gli alunni con DSA, BES o disabilità possono utilizzare dispositivi personali come strumenti compensativi, secondo quanto previsto dal PDP o dal PEI, e in accordo con la famiglia.
- L'uso dei dispositivi ha finalità esclusivamente didattiche e deve essere coerente con le misure indicate nei documenti ufficiali sottoscritti bilateralmente con le famiglie.
- I docenti garantiscono che l'utilizzo degli strumenti digitali sia integrato nelle attività di classe in modo inclusivo e non discriminante.
- Gli studenti possono utilizzare software specifici (lettori vocali, sintesi vocale, mappe concettuali, dizionari digitali, applicazioni per l'organizzazione del lavoro) quando previsto dal percorso personalizzato.
- Non si possono utilizzare i dispositivi personali per giocare con applicazioni oppure online, salvo giochi a scopo didattico (es. Genially, Kahoot, Wordwall, ecc...)
- In caso di verifiche, l'uso degli strumenti compensativi digitali è consentito solo se indicato nel PDP/PEI e autorizzato dal docente della disciplina; in qualsiasi modo il dispositivo deve essere disconnesso dalla rete durante lo svolgimento di qualsiasi test scritto, salvo in caso di verifiche che richiedono l'accesso a Google Moduli o all'account istituzionale.
- I dispositivi devono essere configurati in modo da non consentire distrazioni o accessi non pertinenti all'attività didattica.
- Le stesse regole di sicurezza, privacy e responsabilità previste per tutti gli studenti si applicano anche ai dispositivi utilizzati come strumenti compensativi.

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 minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

Sexting: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere, per quanto possibile, la rimozione del materiale on-line e il blocco della sua diffusione per mezzo dei dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete.

Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;
- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

4.2 - Quali strumenti e a chi

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

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

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

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

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

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

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

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

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

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

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

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

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

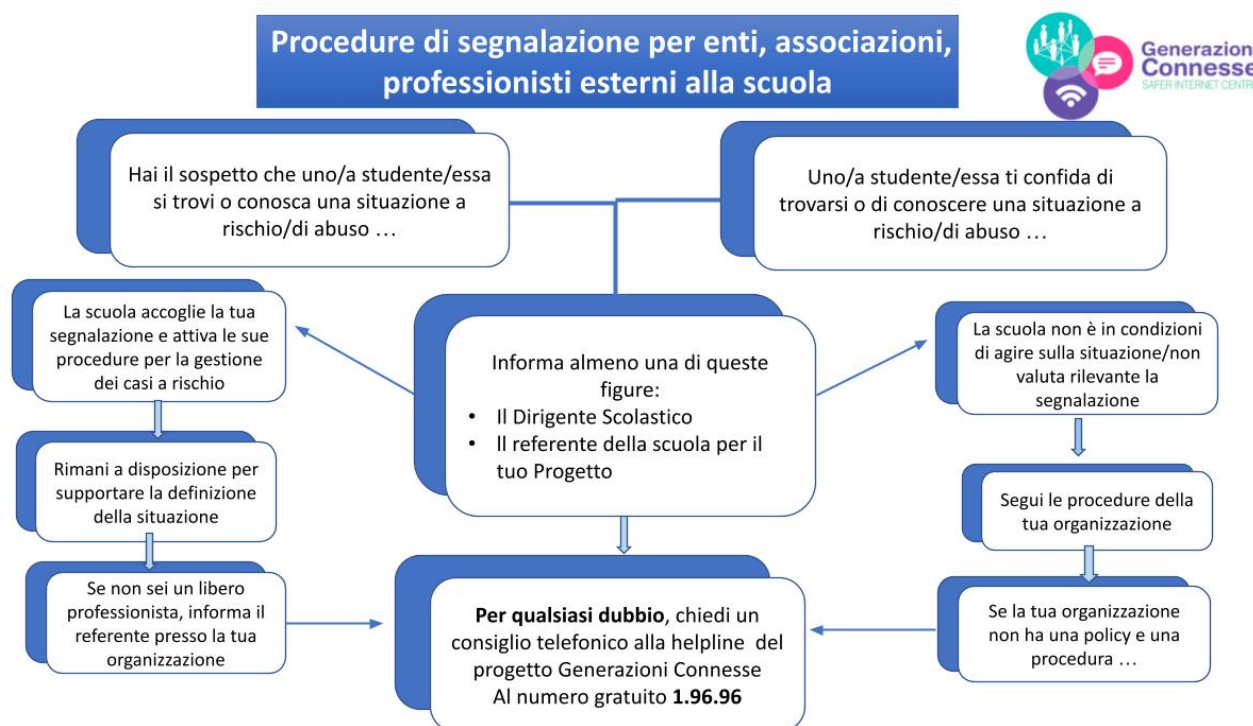
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

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

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.

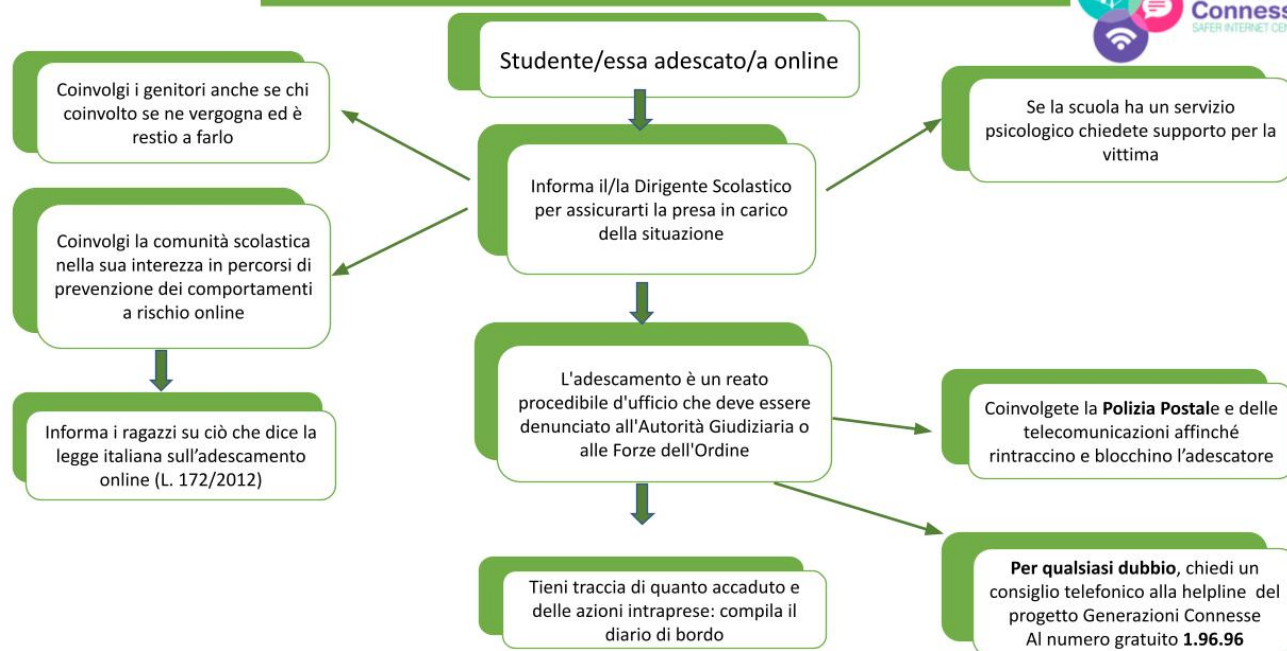
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

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?

