Documento di ePolicy

INDICE

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
5. I piani di Azione dell'ePolicy

Capitolo 2 - Sensibilizzazione e prevenzione

1. Sensibilizzazione e prevenzione
2. Il Curricolo Digitale

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. Uso responsabile e sicuro della rete Internet e delle risorse digitali d'Istituto
4. Strumentazione personale (BYOD)

Capitolo 4 - Segnalazione e gestione dei casi

1. Cosa segnalare
2. Come segnalare: quali strumenti e a chi

Cap 1 – Presentazione dell'ePolicy

1.1 Scopo dell'ePolicy

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

La competenza digitale è una competenza chiave del cittadino europeo come indicato dal Consiglio Europeo (Raccomandazione del 2018) che permette ad ogni cittadino di esercitare i propri diritti all'interno degli ambienti digitali (ONU - Commento Generale 25: I diritti dei minori negli ambienti digitali).

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

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

Il documento di ePolicy del nostro Istituto è lo strumento operativo di riferimento per tutta la comunità scolastica, finalizzato a promuovere un utilizzo delle tecnologie digitali che sia consapevole, critico e responsabile. Esso intende guidare studenti, docenti e famiglie verso una maggiore comprensione delle opportunità offerte dal digitale, ma anche dei rischi connessi all'uso di Internet e dei dispositivi connessi.

Attraverso linee guida chiare e condivise, la ePolicy definisce le modalità corrette di utilizzo delle tecnologie dell'informazione e della comunicazione (TIC) nell'ambiente scolastico, promuovendo il benessere digitale e un clima di convivenza rispettosa anche online.

Il nostro Istituto si impegna ad adottare una strategia educativa attenta ai bisogni, alle difficoltà e alle eventuali richieste di supporto da parte degli studenti, ponendo al centro una politica di prevenzione quanto più efficace. Sono promosse attività formative, percorsi di sensibilizzazione e interventi mirati per accompagnare gli alunni in un uso critico e sicuro delle tecnologie, sia in ambito scolastico che nella vita quotidiana.

1.2 - Ruoli e responsabilità nell'implementazione dell'ePolicy

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, si impegni nell'attuazione e promozione di essa.

Il documento definisce con chiarezza ruoli, compiti e responsabilità di ciascuna delle figure all'interno dell'Istituto.

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, 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 segua 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 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 alle Tic da parte degli studenti.

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

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

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

In coerenza con le Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo del Ministero dell'Istruzione (D.M. n. 18 del 13/1/2021, agg. 2021 – nota prot. 482 del 18-02-2021), il Team ha le funzioni di coadiuvare il Dirigente Scolastico, coordinatore del Team nella scuola, nella definizione degli interventi di prevenzione e nella gestione dei casi di bullismo e cyberbullismo che si possono presentare. Promuove inoltre la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale e comunica ad alunni, famiglie e tutto il personale scolastico dell'esistenza del team, a cui poter fare riferimento per segnalazioni o richieste di informazioni sul tema.

Il Team ha il compito di:

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

I DOCENTI

I 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 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, informano gli studenti sui rischi della rete, ma sollecitandone un uso consapevole.

I 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 tempestivamente al Dirigente Scolastico e al Referente per il bullismo/cyberbullismo qualunque problematica, violazione o abuso, anche online, che veda coinvolti studenti e studentesse, al fine di 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 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 propri compagni e rispettarli. 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 GENITORI/GLI 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.

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 degli studenti, 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 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.

Un ruolo cruciale ha la Polizia Postale, con la quale l'Istituto Superiore G. Terragni collabora da anni per sensibilizzare la comunità scolastica a un utilizzo critico, responsabile e sicuro delle tecnologie digitali e della rete. Questa collaborazione ha dato origine a iniziative formative e percorsi di prevenzione che rafforzano la consapevolezza dei rischi online e promuovono comportamenti corretti e rispettosi nell'ambiente digitale.

1.3 Integrazione dell'ePolicy con regolamenti e normativa generale esistenti

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, è 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 è 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'Istituto G. Terragni ha quindi sviluppato un documento di E-Policy per il triennio 2025-2028 che, a partire dalla sua approvazione, è stato debitamente integrato nel Piano Triennale dell'Offerta Formativa (PTOF), nei Regolamenti interni dell'Istituto e nel Patto di Corresponsabilità educativa.

L'integrazione del documento nel PTOF indica che la tecnologia e l'innovazione digitale sono centrali nell'approccio educativo dell'Istituto per il periodo indicato, e che verranno stabiliti protocolli chiari riguardo alla gestione dei dispositivi, la sicurezza dei dati e l'educazione digitale.

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

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

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.

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 sulle 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.

Il documento di ePolicy dell'IIS G. Terragni, redatto dal Team Antibullismo e per l'Emergenza, approvato dal Collegio Docenti e dal Consiglio d'Istituto, è stato pubblicato sul sito istituzionale nella sezione *"Le Carte della Scuola"*, al seguente link: https://liceoterragni.edu.it/scuola/le-carte-della-scuola/.
Il documento viene condiviso annualmente con studenti e famiglie, a garanzia della trasparenza e della partecipazione consapevole alla vita scolastica.

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).

L'Istituto Giuseppe Terragni si impegnerà, nel corso del triennio 2025-2028, a realizzare attività di rilevazione dei bisogni, monitoraggio, valutazione in itinere e finale delle iniziative attuate. Questo processo avrà anche l'obiettivo di progettare con maggiore consapevolezza ed efficacia le azioni da intraprendere nel triennio successivo.

L'Istituto G. Terragni di Olgiate Comasco (CO) ha istituito un team dedicato alla valutazione degli strumenti digitali da adottare. Nel corso del triennio, verrà implementata una sezione del sito istituzionale con lo scopo di fornire a studenti, insegnanti e famiglie materiali utili per garantire un uso consapevole e sicuro delle tecnologie digitali, in linea con gli obiettivi dell'ePolicy.

Cap 2 - Sensibilizzazione e prevenzione

2.1 Sensibilizzazione e prevenzione

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

In questa direzione l'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.

Il nostro istituto si impegna attivamente nella promozione di percorsi educativi finalizzati allo sviluppo delle competenze digitali, con l'obiettivo di guidare gli studenti e le studentesse verso un uso consapevole, critico e responsabile delle tecnologie. Tale impegno mira a preparare i giovani a navigare con sicurezza e consapevolezza nel vasto mondo digitale, affrontando le sfide quotidiane con un approccio etico e orientato alla tutela della propria privacy e sicurezza online.

Oltre a formare gli studenti, il nostro istituto dedica una particolare attenzione alla crescita professionale dei docenti, offrendo corsi di aggiornamento e formazione continua. Questi corsi sono progettati per fornire ai docenti le competenze necessarie per creare e gestire ambienti di apprendimento digitali innovativi, inclusivi e sicuri, in grado di stimolare una partecipazione attiva e motivata degli studenti al processo educativo. L'obiettivo è garantire che ogni studente abbia accesso a opportunità educative moderne e di qualità, utilizzando le tecnologie in modo efficace per favorire il loro successo scolastico e la loro crescita personale.

I corsi di aggiornamento e i percorsi formativi saranno organizzati e proposti attraverso piattaforme digitali riconosciute come FUTURA, ELISA e GENERAZIONI CONNESSE, che offrono una vasta gamma di risorse e strumenti per il miglioramento delle competenze digitali sia degli studenti che dei docenti. Queste piattaforme permettono di accedere a materiali formativi, seminari online, laboratori e attività pratiche, supportando un apprendimento continuo e personalizzato che risponde alle esigenze di un contesto educativo in costante evoluzione.

2.2 Il Curricolo Digitale

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

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

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

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

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

L'Istituto G. Terragni si riserva di valutare, nel corso degli anni futuri, le azioni più adeguate da intraprendere in relazione

all'evoluzione delle tecnologie e delle necessità educative. A partire da questo triennio, l'Istituto inizierà gradualmente a farsi carico di queste tematiche, con l'obiettivo di adottare approcci sempre più mirati e coerenti con le esigenze della comunità scolastica.

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.

L'Istituto, in linea con la normativa vigente, si impegna a garantire la protezione dei dati personali di tutti gli studenti, docenti e membri della comunità scolastica, riconoscendo il diritto fondamentale alla privacy sancito dalla Carta dei diritti fondamentali dell'Unione europea e dal GDPR.

A tal fine, l'Istituto ha provveduto alla nomina di un Responsabile della Protezione dei Dati (RPD/DPO) nella persona di Luca Corbellini (c/o Studio AG.I.COM. S.r.l. - Via XXV Aprile, 12 – 20070 SAN ZENONE AL LAMBRO), che si occupa di supervisionare e garantire il corretto trattamento dei dati personali.

Inoltre, vengono forniti adeguati avvisi informativi al momento della raccolta dei dati e viene mantenuto un registro dei trattamenti, come previsto dalla normativa. L'Istituto assicura che ogni trattamento di dati personali avvenga nel pieno rispetto della legge, con la massima trasparenza e tutela della privacy di ciascun individuo coinvolto.

3.2 Accesso ad internet

L'accesso alla rete Internet dell'Istituto avviene esclusivamente mediante credenziali personali e riservate (username e password) assegnate a ciascun utente. È severamente vietato cedere, condividere o utilizzare le credenziali di accesso altrui.

Ogni utente è direttamente responsabile di tutte le attività effettuate in rete tramite il proprio account.

3.3 Uso responsabile e sicuro della rete Internet e delle risorse digitali d'Istituto

Il nostro Istituto riconosce le potenzialità educative di Internet, ma anche i rischi connessi al suo utilizzo. Per questo, ha adottato misure di sicurezza per garantire un uso sicuro, consapevole e regolamentato delle risorse digitali e della rete interna. L'accesso a Internet è consentito solo per finalità didattiche; sono vietati l'utilizzo per scopi personali, il download non autorizzato di contenuti e l'accesso a siti non approvati. È inoltre proibita qualsiasi modifica ai parametri di sicurezza dei dispositivi scolastici.

Vengono promosse attività di sensibilizzazione sui rischi online (privacy, copyright, contenuti inappropriati), e adottate misure per la tutela dei dati personali e della sicurezza informatica. Tali regole mirano a prevenire virus, intrusioni nella rete, malfunzionamenti e a garantire un ambiente digitale sicuro e funzionale per l'apprendimento.

3.4 Strumentazione personale (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.
In conformità con le nuove linee guida emanate dal Ministero dell'Istruzione e del Merito (MIM) relative all'uso dei dispositivi digitali nelle scuole secondarie di secondo grado, e in particolare con quanto previsto dalla normativa vigente per l'anno 2025 (Disposizione Ministeriale Prot. n. 3392 del 16 giugno 2025), il nostro Istituto ha aggiornato la propria regolamentazione interna sull'impiego dei dispositivi personali durante l'orario scolastico.

A partire dall'entrata in vigore del nuovo regolamento, è stabilito che tutti gli studenti dovranno depositare i propri telefoni cellulari in apposite cassette di sicurezza, chiuse a chiave, per tutta la durata delle attività didattiche. Tale misura è volta a promuovere un ambiente di apprendimento più efficace, riducendo le distrazioni e favorendo una maggiore concentrazione durante le lezioni.

Deroghe all'obbligo di deposito potranno essere concesse agli studenti in possesso di un Piano Didattico Personalizzato (PDP) o di un Piano Educativo Individualizzato (PEI), qualora l'uso del dispositivo mobile risulti funzionale alle specifiche esigenze didattiche o inclusive previste nel piano stesso. In tali casi, l'utilizzo sarà disciplinato in maniera individualizzata, con il coinvolgimento dei docenti e dei referenti per l'inclusione, garantendo una supervisione adeguata.

Il corpo docente confida nella collaborazione di studenti e famiglie per l'attuazione responsabile di questa disposizione, a beneficio dell'intera comunità scolastica.

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. 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 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, 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 avviene attraverso circolari, informative sul sito dell'istituto, assemblee che coinvolgono i genitori, gli studenti e il personale della scuola, durante i collegi docenti e attraverso tutti i canali maggiormente utili a un'efficace comunicazione.

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

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 studenti coinvolti.

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 allo studente, 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.

Il personale della scuola, in caso di sospetto o certezza che uno studente sia coinvolto in episodi di cyberbullismo, sexting o adescamento online, può seguire procedure standardizzate previste dall'Istituto-reperibili nel Protocollo di Intervento per l'Esame e la Gestione dei Casi redatto dal Team Antibullismo-che:

- guidano l'identificazione e la gestione dei casi;
- definiscono le figure preposte alla presa in carico (es. referente bullismo/cyberbullismo, Dirigente Scolastico, team dedicato);
- prevedono la collaborazione con enti e servizi esterni, se necessario.

Le procedure sono condivise con l'intera comunità scolastica per favorire l'emersione dei casi e garantire un ambiente sicuro.

4.2 Come segnalare: 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.

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.

Protocollo di intervento

Se il personale scolastico ha il sospetto che stia avvenendo qualcosa nella comunità discente riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online, comunica l'informazione al Referente e/o al Dirigente, oralmente o tramite la mail **sosbullismo@istitutoterragni.it**. Da qui, il Dirigente e i docenti coinvolti procedono alla valutazione del caso e agiscono con adeguati interventi.

Se il personale scolastico ha evidenza certa che stia accadendo qualcosa nella comunità discente, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online, comunica l'informazione al Referente e/o al Dirigente, oralmente o tramite la mail **sosbullismo@istitutoterragni.it**. 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.

Anche gli studenti e i genitori devono e possono segnalare casi di sospetto o evidenza dei fenomeni, segnalarlo al Referente, al Dirigente o al docente coordinatore di classe, oralmente, tramite la mail **sosbullismo@istitutoterragni.it** o tramite segnalazione anonima tramite un modulo google reperibile al seguente link:
https://docs.google.com/forms/d/e/1FAIpQLSctHdPT1eAzze7fDQtotJONOpsJg2qFX9IyVCyoTL7pAGDCeA/viewform

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. 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.

Qualora si rilevasse un fatto riconducibile alla fattispecie di reato, l'insegnante ha sempre l'obbligo di segnalare tempestivamente l'evento all'autorità giudiziaria. (ex. l. 71/2017). 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.

Segnalazione di Bullismo e Cyberbullismo

Il personale scolastico è tenuto a segnalare tempestivamente eventuali episodi, anche presunti, di bullismo o cyberbullismo,

utilizzando il modulo disponibile sul sito della scuola e inviandolo all'indirizzo **sosbullismo@istitutoterragni.it**.
La gestione dei casi prevede il coinvolgimento del Dirigente Scolastico, del Team Antibullismo e, se necessario, di enti esterni.

Le **procedure complete** sono consultabili nel **Protocollo di gestione delle segnalazioni** al seguente link:
https://liceoterragni.edu.it/servizi/bullismo-e-cyberbullismo/

L'Istituto segnala, 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.