

# ePolicy d'Istituto

## INDICE

### 1. PRESENTAZIONE DELL' ePOLICY

- 1.1. Scopo dell'ePolicy
- 1.2. Ruoli e responsabilità
- 1.3. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
- 1.4. Gestione delle infrazioni alla ePolicy
- 1.5. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
- 1.6. Integrazione dell'ePolicy con regolamenti esistenti

### 2. FORMAZIONE E CURRICOLO

- 2.1. Curricolo sulle competenze digitali per gli studenti
- 2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica
- 2.3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
- 2.4. Sensibilizzazione delle famiglie e Patto di corresponsabilità

### 3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE TIC DELLA E NELLA SCUOLA

- 3.1. Protezione dei dati personali
- 3.2. Accesso ad Internet
- 3.3. Strumenti di comunicazione online
- 3.4. Strumentazione personale

### 4. RISCHI ON LINE: CONOSCERE, PREVENIRE E RILEVARE

- 4.1. Sensibilizzazione e prevenzione
- 4.2. Cyberbullismo: che cos'è e come prevenirlo
- 4.3. Hate speech: che cos'è e come prevenirlo
- 4.4. Dipendenza da Internet e gioco online
- 4.5. Sexting
- 4.6. Adescamento online
- 4.7. Pedopornografia

## 5. SEGNALAZIONE E GESTIONE DEI CASI

- 5.1. Cosa segnalare
- 5.2. Come segnalare: quali strumenti e a chi
- 5.3. Gli attori sul territorio per intervenire

### ALLEGATI:

6. Piano di azioni
7. Regolamento d'Istituto
8. Regolamento di Disciplina
9. Disposizioni utilizzo internet

# 1. PRESENTAZIONE DELL'ePOLICY

## 1.1. Scopo dell'ePolicy

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.

Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una ePolicy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'ePolicy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

L'ePolicy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Attraverso l'ePolicy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

L'ePolicy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

## 1.2. Ruoli e responsabilità

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.

### **Il Dirigente scolastico**

Il Dirigente scolastico si impegna a garantire la sicurezza, anche online, di tutti i membri della comunità scolastica. Si impegna a formarsi adeguatamente sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIUR; promuove la cultura della sicurezza online e, ove possibile, dà il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC. Il Dirigente scolastico ha la responsabilità di gestire ed intervenire nei casi di episodi di cyberbullismo ed uso improprio delle tecnologie digitali.

### **L'Animatore digitale**

L'Animatore digitale supporta il personale scolastico in riferimento ai rischi online, alla protezione e gestione dei dati personali, ed è uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con



riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica); raccoglie le segnalazioni relative a eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e sollecita gli utenti autorizzati ad accedere alla Rete della scuola con apposita password, esclusivamente per scopi istituzionali e consentiti (istruzione e formazione).

## **Il Referente bullismo e cyberbullismo**

“Ogni Istituto scolastico, nell'ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo” (Art. 4 Legge n.71/2017, “Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo”). Tale figura ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Ha un ruolo non solo in ambito scolastico ma anche (ove possibile) in quello extrascolastico, in quanto potrebbe coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

## **I Docenti**

I Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Hanno il dovere morale e professionale di segnalare al Dirigente scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse, e riferiscono all'Animatore digitale segnalazioni relative a eventuali episodi o problematiche connesse all'uso delle TIC a scuola.

I docenti accompagnano e supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete.

Possono, innanzitutto, integrare parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica.

## **Il personale Amministrativo, Tecnico e Ausiliario (ATA)**

Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il Dirigente scolastico e con il personale docente tutto. Diverse figure che, in sinergia, si occupano ciascuno per la propria funzione, del funzionamento dell'Istituto scolastico che passa anche attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola. Il personale ATA è coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

## **Gli Studenti e le Studentesse**

Gli Studenti e le Studentesse, in relazione al proprio grado di maturità e consapevolezza raggiunta, devono 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; partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e si fanno promotori di quanto appreso anche attraverso possibili percorsi di peer education.

## **I Genitori**

I Genitori, in continuità con l'Istituto scolastico, dovrebbero essere partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali; dovrebbero relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet. Accettano e condividono quanto scritto nell'ePolicy dell'Istituto.

## **Gli Enti educativi esterni e le associazioni**

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola si conformano alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC; promuovono comportamenti sicuri, la sicurezza online e assicurano la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme. Nel contratto si inserisce una specifica indicazione al rispetto delle linee guida dell'Istituto e si sottolinea che tutti coloro che entrano in relazione con la scuola hanno il dovere morale e professionale di segnalare ai docenti qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse, e riferiscono al docente referente segnalazioni relative a eventuali episodi o problematiche connesse all'uso delle TIC a scuola.

## **1.3. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica**

Il documento di ePolicy viene condiviso con tutta la comunità educante: esso comporta compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/le studenti/esse) si faccia a sua volta promotore del documento. L'ePolicy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;

- ai docenti con comunicazione annuale durante un collegio docenti (indicativamente il secondo dell'anno scolastico) qualora non fosse necessario apportare modifiche al testo;
- alle famiglie attraverso la firma del Patto di Corresponsabilità.

Il documento è condiviso nel Collegio dei Docenti e approvato dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete e accessibili agli studenti.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

## 1.4. Gestione delle infrazioni alla ePolicy

La scuola gestisce le infrazioni all'ePolicy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni. Queste azioni vengono normate nel Regolamento di disciplina.

Le possibili condotte sanzionabili, in relazione all'uso improprio delle TIC e della Rete a scuola da parte degli studenti e delle studentesse, sono ad esempio:

- l'invio di testi, immagini o video volti all'esclusione di compagni/e
- la condivisione online di immagini o video di compagni/e senza il loro consenso o che li ritraggono in pose offensive e denigratorie; la condivisione di dati personali;
- la condivisione di scatti intimi e di materiale a sfondo sessuale.

A seconda dell'età dello studente o della studentessa, si pongono in essere interventi su tutto il contesto classe con attività specifiche educative e di sensibilizzazione, allo scopo di promuovere una maggior consapevolezza circa l'utilizzo delle TIC e di Internet.

A seconda della natura e della gravità di quanto accaduto, non si esclude la possibilità di denunciare l'episodio (con il coinvolgimento ad es. della Polizia Postale) o di garantire immediato supporto psicologico allo/la studente/ssa attraverso i servizi predisposti, qualora ciò fosse necessario.

## 1.5. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

L'ePolicy viene riesaminata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento vengono condivise con il Collegio Docenti e approvate anche dal Consiglio d'Istituto. Con la revisione periodica è prevista anche una valutazione della sua efficacia a partire dagli obiettivi specifici che lo stesso si pone (promozione delle competenze digitali e dell'uso delle TIC nei percorsi educativi e didattici, prevenzione e gestioni dei rischi online etc...).

Referente per la revisione e/o l'aggiornamento dell'ePolicy è la Commissione Innovazione Digitale.

## 1.6. Integrazione dell'ePolicy con regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'ePolicy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

# 2. FORMAZIONE E CURRICOLO

## 2.1. Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali".

Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico" ("[Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente](#)", C189 pag.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale.

Le competenze digitali richiamano diverse dimensioni sulle quali sarà possibile lavorare in classe, in un'ottica che integra la dimensione tecnologica con quella cognitiva ed etica (Calvani, Fini e Ranieri 2009):

- dimensione tecnologica: è importante far riflettere i più giovani sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana, onde evitare automatismi che abbiano conseguenze incerte, attraverso un'adeguata comprensione della "grammatica" dello strumento;
- dimensione cognitiva: fa riferimento alla capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità;
- dimensione etica e sociale: la prima fa riferimento alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui, e di usare le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri. La seconda, invece, pone

un po' più l'accento sulle pratiche sociali e quindi sullo sviluppo di particolari abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online;

I documenti più importanti per progettare e implementare un buon curriculum sulle competenze digitali a cui fare riferimento sono:

-Piano Nazionale Scuola Digitale (PNSD), in particolar modo il paragrafo 4.2. su "Competenze e contenuti";

-Sillabo sull'Educazione Civica Digitale: ha lo scopo di inquadrare il corpus di temi e contenuti che sono alla base dello sviluppo di una piena cittadinanza digitale degli studenti attraverso il percorso educativo;

-DigComp 2.1.: "Il quadro di riferimento per le competenze digitali dei cittadini", con otto livelli di padronanza ed esempi di utilizzo;

-Raccomandazione del Consiglio europeo relativa alle competenze chiave per l'apprendimento permanente, in particolare al paragrafo 4 dell'allegato (C189, p. 9).

L'Istituto ha seguito nell'a.s. 2019-2020 il progetto Generazioni Connesse e sa di poter usufruire dei materiali e di tutti gli altri contenuti (ad es. il corso di formazione per la redazione di questa ePolicy) offerti dal sito [www.generazioniconnesse.it](http://www.generazioniconnesse.it) e di poter fare riferimento al relativo canale Youtube per video pensati per bambini/e e ragazzi/e.

## 2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica

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

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

L'Istituto, attraverso il Collegio dei Docenti, riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola (ad es. con l'aiuto dell'animatore digitale) dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti (anche online), purché restino coerenti con il piano di formazione.

Fondamentale è l'attenzione all'uso delle TIC nella didattica: un loro utilizzo strutturato e integrato non solo può rendere gli apprendimenti motivanti, coinvolgenti ed inclusivi, ma permette al docente di guidare studenti e studentesse rispetto alla fruizione dei contenuti online, ormai la modalità naturale di apprendimento al di fuori della scuola. Inoltre, permettono di sviluppare capacità che sono sempre più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza e il confronto fra pari in modalità asincrona. Per questo si è provveduto ad attivare da diversi anni la GSuite d'Istituto: tutti i docenti e gli studenti hanno accesso ad una serie di servizi, tra i quali e-mail personale con spazio d'archiviazione illimitato; Drive, che permette di archiviare online tutti i tipi di file, senza limiti di spazio, e ne permette la condivisione collaborativa;



Classroom, per avere una classe virtuale nella quale lavorare attivamente e ricevere materiale.

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

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

Si immagina di avviare un programma che consideri il triennio scolastico, in un'ottica di vera e propria programmazione, con azioni specifiche, a partire dall'a. s. 2019/20 che ha visto i membri della Commissione Innovazione Digitale seguire il percorso di redazione della ePolicy d'Istituto, e il coinvolgimento di alcuni colleghi nello stesso corso di formazione. Si pensa in seguito di:

- analizzare il fabbisogno formativo degli insegnanti sull'uso sicuro della Rete;
- promuovere la partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse";
- monitorare le azioni svolte per mezzo di specifici momenti di valutazione;
- organizzare incontri con professionisti della scuola o con esperti esterni, enti/associazioni, etc.

### **2.4. Sensibilizzazione delle famiglie e Patto di corresponsabilità**

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del Regolamento di disciplina, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

## 3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE TIC DELLA E NELLA SCUOLA

### 3.1. Protezione dei dati personali

“Le scuole sono chiamate ogni giorno ad affrontare la sfida più difficile, quella di educare le nuove generazioni non solo alla conoscenza di nozioni basilari e alla trasmissione del sapere, ma soprattutto al rispetto dei valori fondanti di una società. Nell'era di Internet e in presenza di nuove forme di comunicazione questo compito diventa ancora più cruciale. È importante riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino”.

(cfr. <http://www.garanteprivacy.it/scuola>).

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il “corretto trattamento dei dati personali” a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni.

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato in vigore il 19 settembre 2018.

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori. A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali.

### 3.2. Accesso ad Internet

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



l'accesso alla società dell'informazione e fare in modo che il «diritto a Internet» diventi una realtà, a partire dalla scuola”.

Già da alcuni anni a seguito di partecipazione a Bandi PON in tutti i plessi è reso disponibile l'accesso ad Internet via LAN e WIFI.

Su un'altra linea l'accesso è garantito allo stesso modo per gli uffici amministrativi.

### 3.3. Strumenti di comunicazione online

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

L'accesso a internet è garantito a tutti i pc e dispositivi della scuola, via LAN e/o WIFI.

L'accesso per gli studenti è sempre mediato da un adulto di riferimento.

Strumenti di comunicazione online riconosciuti dall'Istituto sono:

- il registro elettronico in uso alla primaria e alla secondaria (account creati per docenti e famiglie);
- il sito internet (con area riservata ai docenti)
- la Gsuite for Education (account creati per tutti i docenti di ruolo, per i docenti con incarico annuale, su richiesta ad educatori e tirocinanti, per tutti gli studenti della primaria e della secondaria, a richiesta dei docenti per gli alunni dell'infanzia, anche attivato a livello di sezione)

### 3.4. Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/le studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento.

La presente ePolicy è coerente con le 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").

L'Istituto consente l'accesso a Internet dai dispositivi personali dei docenti, purché utilizzati a scopo didattico; alle stesse condizioni è consentito agli alunni purché con la mediazione di un adulto di riferimento, seguendo le procedure indicate nel Regolamento Internet.

## 4. RISCHI ON LINE: CONOSCERE, PREVENIRE E RILEVARE

### 4.1. Sensibilizzazione e prevenzione

Il rischio online si configura come la possibilità per il minore di:

- commettere azioni online che possano danneggiare se stessi o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e contenerli. È importante che bambini/e e ragazzi/e abbiano gli strumenti idonei per riconoscere possibili situazioni di rischio e segnalarle ad un adulto di riferimento.

Gli strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio si configurano come interventi di sensibilizzazione e prevenzione:

- nel caso della sensibilizzazione si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare;
- nel caso della prevenzione si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.

### 4.2. Cyberbullismo: che cos'è e come prevenirlo

La legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", nell'art. 1, comma 2, definisce il cyberbullismo:

"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo".

La stessa legge e le relative Linee di orientamento per la prevenzione e il contrasto del cyberbullismo indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie;
- nomina del Referente per le iniziative di prevenzione e contrasto che:
  - ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
  - potrà svolgere un importante compito di supporto al Dirigente scolastico e alle figure preposte alla revisione/stesura di Regolamenti, atti e documenti (PTOF, PdM, RAV).

### 4.3. Hate speech: che cos'è e come prevenirlo

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, etc.) ai danni di una persona o di un gruppo.

L'Istituto prende atto che tale fenomeno, purtroppo, è sempre più diffuso e che è estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

## 4.4. Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

## 4.5. Sexting

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti medialmente sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

Considerato che tale fenomeno emerge laddove risulta carente un'adeguata educazione affettiva, già da diversi anni l'Istituto ha attivato un progetto specifico di educazione all'affettività con personale esterno per gli studenti della scuola secondaria.

## 4.6. Adescamento online

Il grooming (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i/le bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di teen dating (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies - l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

## 4.7. Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti,

concrete o simulate o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

La legge n. 269 del 3 agosto 1998 "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella legge n. 38 del 6 febbraio 2006 "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet", segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 - Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito [www.generazioniconnesse.it](http://www.generazioniconnesse.it) alla sezione "Segnala contenuti illegali" ([Hotline](#)). Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete.

I due servizi messi a disposizione dal Safer Internet Centre sono il "[Clicca e Segnala](#)" di Telefono Azzurro e "[STOP-IT](#)" di Save the Children.

## 5. SEGNALAZIONE E GESTIONE DEI CASI

### 5.1. Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.



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. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).

Nelle procedure:

- sono indicate le **figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso.**
- la scuola **individua nel Referente al Cyberbullismo** la figura preposta 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.**

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

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 minorenni 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 la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via 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.

Segnaliamo, 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.

## 5.2. Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ma si estende a tutte le altre attività educative.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due 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.
- 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 cyberbullismo, sexting o adescamento online.

Per tutti i dettagli fare riferimento 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 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 -per studenti secondaria-;
- docente referente per il cyberbullismo.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito [1.96.96](tel:1.96.96).

## **5.3. Gli attori sul territorio per intervenire**

Talvolta, nella gestione dei casi, può essere necessario rivolgersi ad **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.

Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

A seguire **i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti** che una problematica connessa all'utilizzo di Internet può presentare.

#### **Servizi socio-assistenziali Amministrazione Comunale di Rescaldina:**

Via Matteotti 8 - 0331.467831/833/834/870/877  
servizisociali@comune.rescaldina.mi.it

**Azienda Socio Sanitaria Territoriale:** fornisce supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete

<http://www.asst-ovestmi.it/home/stlegnano>

Indirizzi e recapiti strutture dipartimento salute mentale e delle dipendenze:

- Centro psicosociale (CPS) via Ronchi 103 Legnano - 0331.1776001
- Neuropsichiatria Infantile (NPIA) via Ferraris 33 Legnano - 0331.1776061
- Servizi Territoriali per le Tossicodipendenze (SERT) via Spagliardi 19 Parabiago - 0331.1776260 - 266



S.O.S. LUDOPATIA

800 318 318 (gratuito da rete fissa)

02 3232 3325 (da rete mobile, a pagamento secondo il piano tariffario)

**Comitato Regionale Unicef:** su delega della regione svolge un ruolo di difensore dei diritti dell'infanzia

Comitato Unicef Lombardia Via Marsala, 8 - 20121 - Milano 02 4654771

comitato.lombardia@unicef.it

**Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.

CORECOM Grattacielo Pirelli Via F. Filzi, 22 Milano 02. 67482300

corecom@consiglio.regione.lombardia.it

www.corecomlombardia.it/

**Ufficio Scolastico Regionale:** supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.

UFFICIO SCOLASTICO REGIONALE Via Polesine, 13 Milano 02. 5746271

drlo@postacert.istruzione.it

drlo.urp@istruzione.it

http://usr.istruzione.lombardia.gov.it/

**Polizia Postale e delle Comunicazioni:** accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.

POLIZIA POSTALE E DELLE COMUNICAZIONI

Compartimento Milano, Via Moisè Loria, 74 - 02. 43333011

compartimento.polposta.mi@pecps.poliziadistato.it

www.commissariatodips.it/

**Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico:** segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.

Garante per l'infanzia e l'adolescenza della Lombardia

Consiglio Regionale Via Fabio Filzi, 22 - Milano 02. 67486290

garanteinfanziaeadolescenza@consiglio.regione.lombardia.it

**Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori

Tribunale per i Minorenni di Milano - Via Leopardi, 18 - 02. 46721

tribmin.milano@giustizia.it