



MINISTERO DELL'ISTRUZIONE
E DEL MERITO

TERME
VIGLIATORE
FALCONE
OLIVERI



ISTITUTO COMPRENSIVO
TERME VIGLIATORE

Viale delle Terme, 5 - 98050 Terme Vigliatore (ME)
Tel. 090 9781254 - Fax 090 9783472
Cod. Meccanografico MEIC85700X - C.F. 83001910831
PEO: meic85700x@istruzione.it - PEC: meic85700x@pec.istruzione.it
Sito WEB: www.ictermevigliatore.edu.it

All. 16 del Regolamento Interno d'Istituto (Allegato al PTOF vigente)

Documento di e-Policy interna



Approvato dal C.I. del 16/05/2025
Aggiornato dal C.I. del 27/11/2025

L'ePolicy è un documento programmatico autoprodotta dalla scuola per promuovere lo sviluppo delle competenze digitali ed un uso responsabile delle tecnologie digitali dell'informazione e della comunicazione (TIC), sia da parte degli alunni/e che degli adulti coinvolti nel processo educativo.

La nostra ePolicy interna rimanda ad altri documenti e regolamenti della scuola, definendo un sistema di norme comportamentali, buone prassi di azione e misure di prevenzione e gestione di problematiche connesse ad un uso non consapevole delle tecnologie digitali.

Il presente Documento di ePolicy è approvato dal Collegio Docenti e dal Consiglio di Istituto ed è parte integrante del PTOF della scuola

Indice

1. Presentazione dell'ePolicy

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

2. Formazione e curriculum

- 2.1 Curriculum sulle competenze digitali per gli studenti
- 2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
- 2.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
- 2.4 Sensibilizzazione delle famiglie e Patto di corresponsabilità

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

- 3.1 Protezione dei dati personali e GDPR
- 3.2 Accesso ad Internet, strumenti di comunicazione online e 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

Capitolo 1 - Introduzione al documento di ePolicy

1.1 Scopo dell'ePolicy

L' ePolicy interna prevede:

- a) misure atte a facilitare e promuovere l'utilizzo delle TIC nella didattica;
- b) misure di prevenzione e di gestione di situazioni problematiche relative all'uso di Internet e delle tecnologie digitali;
- c) misure di monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento (Piani d'azione)

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. Sono individuati i seguenti ruoli e le principali responsabilità correlate:

➤ Il Dirigente scolastico (DS)

- Segue corsi di formazione e di aggiornamento sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del Ministero dell'istruzione e delle sue agenzie.
- Promuove la cultura della **e-safety** (sicurezza online) – anche attraverso il documento di epolicy – e fornisce il proprio contributo all'organizzazione, insieme ad altre figure di sistema (ad es. Animatore digitale, Docente referente per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo...), di corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC.
- Presiede il Team per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo. Interviene nei casi bullismo, cyberbullismo ed uso improprio delle tecnologie digitali. Gestisce in prima persona, in collaborazione con i referenti e i docenti dei Consigli di classe, i casi gravi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali da parte degli alunni.
- Garantisce l'esistenza all'interno della scuola di un Tavolo permanente di monitoraggio per la prevenzione del bullismo e cyberbullismo e un Codice Interno per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo

➤ Il Direttore amministrativo (DSGA):

- Assicura, nei limiti delle risorse finanziarie, l'acquisto di nuove dotazioni tecnologiche e garantisce la realizzazione di interventi di manutenzione di tutte le tecnologie informatiche utilizzate a scuola al fine di garantirne il funzionamento, la sicurezza e la tutela da un uso improprio.
- Interviene sulla definizione delle modalità e dei mezzi del trattamento dei dati, elabora dati per conto del titolare del trattamento e ha il compito di predisporre un sistema interno di gestione e monitoraggio dell'organizzazione interna della Privacy e di supervisionare gli adempimenti relativi alla privacy, per garantire le misure minime di sicurezza previste dal Codice della Privacy, così come aggiornate dalle modifiche apportate dalla normativa vigente.

➤ I Docenti

- Integrano parti del curriculum disciplinare con approfondimenti sull'uso responsabile delle TIC e della RETE (il c.d. "curriculum digitale") servendosi delle tecnologie digitali nella didattica (LIM o altri dispositivi tecnologici);
- sviluppano le competenze digitali degli allievi facendo sì che gli stessi conoscano e seguano le

- norme di sicurezza digitale nell'utilizzo del web;
 - rispettano l'obbligo di riservatezza dei dati personali trattati e non, in conformità alla normativa vigente;
 - segnalano prontamente alle famiglie eventuali problematiche emerse in classe nell'utilizzo del digitale e stabiliscono linee comuni di intervento educativo;
 - segnalano al Dirigente scolastico/suoi collaboratori o al Referente antibullismo qualunque violazione, anche online, del Regolamento di Istituto secondo la procedura stabilita;
 - nell'uso dei propri account di social media, devono fare attenzione affinché le proprie opinioni o giudizi su eventi, cose o persone non possano essere scambiati per comunicazioni istituzionali e attribuibili all'Ente di appartenenza.
- In ogni caso, il dipendente deve astenersi da qualsiasi intervento o commento online che possa danneggiare il prestigio, il decoro o l'immagine dell'ente di appartenenza o della pubblica amministrazione in generale (DPR 81/2023, art.11)
- L'uso degli account istituzionali è consentita solo per lo svolgimento dei compiti istituzionali e senza compromettere né la sicurezza né la immagine dell'ente di appartenenza. I dipendenti devono firmare i messaggi di posta elettronica che inviano, sono responsabili del loro contenuto e dai messaggi si deve potere risalire al dipendente mittente, che peraltro deve indicare il suo recapito istituzionale.
 - Tutto il personale è consapevole che è sanzionabile una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali.
 - Per le comunicazioni ufficiali online utilizzano le piattaforme istituzionali disponibili. Ai docenti che decidessero, nella loro autonomia, di avvalersi di gruppi whatsapp tra docenti e studenti, si suggerisce di circoscrivere la finalità del gruppo alle sole comunicazioni di natura didattica, con l'assenso genitoriale.

➤ **L'Animatore Digitale e il Team per L'innovazione Digitale**

L'Animatore Digitale è un docente interno che ha il compito di coordinare la diffusione dell'innovazione digitale e della cultura della Cybersicurezza all'interno della scuola.

Si tratta quindi di una figura di sistema e non di supporto tecnico (su quest'ultimo aspetto, nell'ambito di un Istituto Comprensivo, è buona prassi creare un Team "Pronto Soccorso Tecnico" di docenti/ ata/ esperti), anche se può fornire indicazioni al personale scolastico da un punto di vista tecnico-informativo.

L'Animatore digitale è il **Referente e-policy** d'Istituto e fa parte del **Team per l'innovazione digitale**; partecipa anche al **Tavolo permanente di monitoraggio per la prevenzione del bullismo e cyberbullismo** e, in base ai casi che si possono presentare, il suo intervento può essere necessario all'interno del **Team Antibullismo e Cyberbullismo** e del **Team per l'Emergenza**

L'Animatore Digitale ha il compito di sviluppare progettualità sui seguenti 3 ambiti:

1) formazione interna; 2) coinvolgimento della comunità scolastica; 3) creazione di soluzioni innovative.

Una delle tematiche più urgenti di cui deve occuparsi l'animatore digitale è quella dell'**educazione alla sicurezza informatica (Cybersicurity)** in riferimento ai rischi online e alla protezione e gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale".

L'animatore monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e ha il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione)..

Non c'è un compenso *ad personam* per l'Animatore Digitale; può ricevere un compenso in veste di formatore, per le ore di formazione programmate ed effettuate, se la formazione non viene affidata a soggetti esterni.

Nell'ambito della Contrattazione di Istituto si può prevedere un compenso forfettario per le attività di pianificazione/organizzazione svolte ai fini della diffusione dell'innovazione digitale e della cultura della Cybersicurezza e prevedere che il ruolo di animatore digitale rientri tra le funzioni di un Docente Funzione Strumentale.

Il **Team per l'innovazione tecnologica** (in breve "**Team Digitale**") supporta l'Animatore Digitale/docente Funzione Strumentale area "Innovazione Tecnologica", promuove non solo il processo di digitalizzazione della scuola ma anche di diffusione di politiche legate all'innovazione didattica connessa all'uso delle TIC e delle RETE e alla Cybersicurezza.

Il **Team digitale** della nostra scuola è composto da:

- Dirigente scolastico -DS
- Direttore amministrativo – DSGA
- N.1 Assistente amministrativo
- Animatore Digitale
- N.3 Docenti

Compiti:

- supporta il personale scolastico in riferimento ai rischi online, alla protezione e gestione dei dati personali;
- promuovono percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (PNSD)
- supporta l'Animatore digitale nel monitoraggio e rilevazione di eventuali episodi o problematiche connesse all'uso delle TIC a scuola;

➤ **Il team antibullismo-cyberbullismo e il team per l'emergenza**

Il team antibullismo-cyberbullismo:

- coadiuva il dirigente scolastico e il Referente antibullismo nella definizione degli interventi di prevenzione e nella gestione dei casi di bullismo e cyberbullismo che si possono presentare;
- promuove il coinvolgimento di genitori, alunni e di tutto il personale scolastico e comunica l'esistenza del team, a cui poter fare riferimento per segnalazioni o richieste di informazioni sul tema;
- promuove la redazione e l'applicazione della ePolicy interna e monitora le segnalazioni

Il team per l'emergenza interviene (come gruppo ristretto) nelle situazioni di accertamento di bullismo

➤ **Il Personale ata**

All'interno dei singoli regolamenti d'Istituto, il personale ATA, in collaborazione con il Dirigente e con il personale docente tutto, è coinvolto nelle pratiche di prevenzione (incluso il processo di definizione e implementazione dell'ePolicy di Istituto) ed è tenuto a

- collaborare nel reperire, verificare e valutare informazioni inerenti possibili casi di bullismo/cyberbullismo;
- segnalare comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.
- Nell'uso dei propri account di social media, devono fare attenzione affinché le proprie opinioni o giudizi su eventi, cose o persone non possano essere scambiati per comunicazioni istituzionali e attribuibili all'Ente di appartenenza.

In ogni caso, il dipendente deve astenersi da qualsiasi intervento o commento online che possa danneggiare il prestigio, il decoro o l'immagine dell'ente di appartenenza o della pubblica amministrazione in generale (DPR 81/2023, art.11)

- L'uso degli account istituzionali è consentita solo per lo svolgimento dei compiti istituzionali e senza compromettere né la sicurezza né la immagine dell'ente di appartenenza. I dipendenti

devono firmare i messaggi di posta elettronica che inviano, sono responsabili del loro contenuto e dai messaggi si deve potere risalire al dipendente mittente, che peraltro deve indicare il suo recapito istituzionale.

- Tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile

➤ **Alunni e alunne**

Agli studenti è richiesto di :

- utilizzare con responsabilità le tecnologie digitali uniformandosi alle indicazioni dei docenti nonché al rispetto delle norme codificate nei regolamenti di istituto (chiaramente, ogni giorno tutto è così veloce, fluido e dinamico che non è facile “fissare” regole e un'etichetta che vale per tutti e per sempre). A scuola le situazioni sono molteplici, le sensibilità pure. **Le regole spesso vanno riscritte** giorno dopo giorno, attraverso ciò che avviene in rete e soprattutto imparando dagli errori;
- rispettare le regole di **e-safety** le buone pratiche di sicurezza in rete per evitare situazioni di rischio per sé e per gli altri;
- partecipare attivamente alle iniziative che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso percorsi di peer education;
- saper distinguere, con l'aiuto dei docenti, le fonti di informazione attendibili in rete;
- segnalare ai docenti situazioni di difficoltà nell'utilizzo delle tecnologie digitali o possibili casi di bullismo/cyberbullismo;

➤ **I genitori/tutori/adulti di riferimento**

I Genitori, in continuità con la scuola, sono coinvolti nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali (pc, smartphone ecc.) da parte di infratredicenni/quattordicenni. 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 a comunicare con i docenti circa i problemi rilevati quando i propri figli non usano responsabilmente le tecnologie digitali.

Ad essi è richiesto di:

- accettare e condividere quanto scritto nell'ePolicy interna, nel Regolamento d'istituto e nel Patto di Corresponsabilità in un'ottica di collaborazione reciproca;
- partecipare alle iniziative di sensibilizzazione e formazione organizzate dall'Istituto sull'uso consapevole delle TIC e della RETE, nonché sull'uso responsabile dei device personali
- sostenere i docenti nell'azione educativa diretta al corretto utilizzo delle tecnologie digitali
- educare (vigilando sui propri figli) al corretto utilizzo delle tecnologie digitali sia in ambiente domestico sia a scuola, fissando regole comportamentali e di utilizzo, in particolare in caso di attività di didattica a distanza;
- collaborare con i docenti nell'adozione di linee di intervento coerenti per contrastare l'uso non responsabile, scorretto o pericoloso delle tecnologie digitali.
 - segnalare agli insegnanti possibili casi di bullismo/cyberbullismo

Si promuove il coinvolgimento dei rappresentanti di genitori/adulti di riferimento all'interno del percorso di definizione e implementazione dell'ePolicy

➤ **Soggetti esterni pubblici e privati e le Associazioni**

Ai Soggetti esterni e al mondo dell'associazionismo che entrano in relazione con la scuola si chiede di:

- conformarsi alla politica interna della scuola riguardo all'uso consapevole della Rete e delle TIC;
- attivare procedure e comportamenti sicuri, la sicurezza online e la protezione degli studenti durante le attività che si svolgono insieme.

Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto

Tutti gli attori che entrano in relazione educativa con gli alunni/e devono:

- mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.
- Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.
- Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse.
- Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, **in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).**
- Le attività progettuali o di formazione a carattere seminariale, devono essere preventivamente autorizzate dal Dirigente scolastico, con modalità e tempi concordati; a tal proposito, al fine di verificare preventivamente il contenuto da somministrare o dibattere con la scolaresca, i soggetti esterni forniranno un dettagliato programma delle attività con narrazione sintetica della scaletta al fine di essere autorizzato dalla Dirigenza.

Per quanto non espressamente indicato sui ruoli e sulle responsabilità delle figure presenti all'interno dell'Istituzione scolastica, si rimanda: all'art. 21, comma 8, Legge 15 marzo 1997, n. 59; all'art. 25 della Legge 30 marzo 2001, n. 165; al CCNL in vigore; al D.P.R. 8 marzo 1999, n. 275; alla Legge 13 luglio 2015, n. 107; al Piano Nazionale Scuola Digitale; a quanto stabilito in materia di **culpa in vigilando, culpa in organizzando, culpa in educando.**

1.3 Integrazione dell'ePolicy con Regolamenti esistenti

Nel nostro istituto il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'ePolicy, così come anche il Patto di Corresponsabilità e il Ptof, in coerenza con le Linee Guida Miur e le indicazioni normative in materia

1.4 Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

Il documento di ePolicy viene condiviso con tutta la comunità educante, ponendo al centro gli alunni/e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli alunni/e ecc.) si faccia a sua volta promotore del documento.

L'ePolicy viene condivisa e comunicata a tutta la comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;

- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie (prevedendo anche la sottoscrizione sulla piattaforma UNICA, se applicabile) e rilasciato alle stesse all'inizio dell'anno scolastico;
- la presentazione del documento in tutte le classi, all'inizio dell'anno; in occasione dell'illustrazione del Regolamento di Istituto e del Patto di corresponsabilità, i docenti presenteranno anche una sintesi della e-policy interna;
- l'integrazione dei contenuti dell'e-policy nel curriculum sulle competenze digitali;
 - l'utilizzo di risorse online sull'ePolicy e l'e-Safety messe a disposizione dal SIC Safer Internet Centre - Italia - Generazioni Connesse; Telefono Azzurro; Save the Children Italia; Unicef Italia ecc.)
 - L'organizzazione di specifici incontri informativi, nel corso dell'anno, per rinnovare le raccomandazioni relative a e-Policy e e-Safety, cogliendo l'opportunità delle giornate nazionali (**Safer internet day, legalità** ecc.) alla presenza di personale specializzato e Forze dell'ordine

Tutti gli alunni/e saranno informati che la rete, l'uso di internet e di ogni dispositivo digitale a scuola saranno controllati dai docenti e utilizzati solo con la loro autorizzazione e supervisione, nel rispetto delle regole di condotta da tenere in Rete per la sicurezza on-line.

L'animatore digitale predispone delle versioni sintetiche del documento, all'interno delle quali sono individuati gli elementi principali del documento: una versione è diretta agli alunni ed una alle famiglie, con un linguaggio chiaro ed adeguato. La versione degli alunni è inserita all'interno del curriculum di educazione civica; la versione per le famiglie è pubblicata sul registro elettronico e analizzata durante gli incontri scuola-famiglia.

Sarà favorito sempre un approccio collaborativo nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione di incontri scuola-famiglia assembleari, collegiali e individuali al fine di sensibilizzare le famiglie sui temi dell'uso delle TIC. Sarà condiviso materiale informativo aggiornato per implementare la presente e-policy.

1.5 Gestione delle infrazioni alla ePolicy

La scuola gestirà le infrazioni all'ePolicy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

Disciplina degli alunni

Le potenziali infrazioni in cui potrebbero incorrere gli alunni, relativamente alla fascia di età considerata, nell'utilizzo delle tecnologie digitali e di internet durante la didattica sono le seguenti:

- impedire a qualcuno di esprimersi o partecipare
- esprimersi in modo volgare usando il turpiloquio
- invio incauto o senza permesso di foto o altri dati personali (indirizzo di casa, numero di telefono)
- condivisione online di immagini o video di compagni/e e del personale scolastico senza il loro esplicito consenso o che li ritraggono in pose offensive e denigratorie
- condivisione di immagini intime e a sfondo sessuale/ modificate con IA
- invio di immagini o video volti all'esclusione di compagni/e
- comunicazione incauta e senza permesso con sconosciuti
- collegamenti a siti web non adeguati e non indicati dai docenti

L'azione educativa prevista per gli alunni è rapportata alla fascia di età e al livello di sviluppo e maturazione personale. Infatti in alcuni casi i comportamenti sanzionabili sono dovuti a uno

sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, di cui gli educatori devono tenere conto per il raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno. Pertanto sono previsti interventi gradualmente in base all'età e alla gravità delle violazioni:

- richiamo verbale
- richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante)
- richiamo scritto con annotazione sul diario e sul registro
- convocazione dei genitori
- sospensione dalle lezioni con obbligo di frequenza e di svolgere attività rieducative;
- eventuale segnalazione alle autorità competenti

Contestualmente sono previsti interventi educativi di rinforzo rispetto a comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza, di prevenzione e gestione positiva dei conflitti, di pro- socialità, di conoscenza e gestione delle emozioni. E' inoltre importante intervenire su tutto il contesto classe con attività specifiche educative e di sensibilizzazione.

Disciplina del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono diverse e alcune possono determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli allievi:

- utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di docenza o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiale non idoneo
- utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale
- trattamento dei dati personali e dei dati sensibili degli alunni non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi
- diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi
- carente istruzione preventiva degli alunni sull'uso corretto e responsabile delle TIC e di internet
- vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili rischi connessi
- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, al Team Digitale.

Il Dirigente scolastico può disporre il controllo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola. I materiali non adeguati o non autorizzati vanno cancellati dal sistema informatico della scuola e, se necessario, se ne conserva una copia per eventuali approfondimenti successivi.

Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio dei procedimenti che possono avere carattere organizzativo-gestionale, disciplinare, amministrativo, penale, a seconda del tipo e della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

Disciplina dei genitori

In considerazione dell'età degli studenti e delle studentesse e della loro dipendenza dagli adulti, anche talune condizioni e condotte dei genitori medesimi possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli allievi a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico. Gli atteggiamenti da parte della famiglia meno favorevoli sono:

- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non corre rischi
- una posizione del computer in una stanza o in una posizione non visibile e controllabile dall'adulto
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'uso di cellulare o smartphone
- un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei a minori
- un utilizzo di cellulari e smartphone in comune con gli adulti che possono conservare in memoria indirizzi di siti o contenuti non idonei a minori

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per altri (*culpa in educando e in vigilando*).

I genitori devono rendersi conto degli effetti negativi dell'uso eccessivo e non responsabile delle TIC. L'accesso a un bacino immenso di informazioni e relazioni di qualsiasi genere pone la complessa questione di come salvaguardare le giovani generazioni da effetti negativi e situazioni potenzialmente pericolose che ne possono derivare. Secondo il Centro per la Salute Mentale del Bambino, un uso protratto delle TIC può generare diversi conseguenze negative sulla salute fisica e mentale di piccoli e adolescenti.

1.6 Monitoraggio dell'implementazione della e-Policy e suo aggiornamento (Piani d'azione)

L'ePolicy interna viene implementata attraverso Piani di azione annuali e pluriennali deliberati dal Collegio docenti e dal Consiglio di Istituto ed inseriti nel PTOF.

I Piani di azione (rivolti ad alunni, personale, famiglie) contengono:

- la rilevazione dei bisogni (che, purtroppo, si manifestano nel corso dell'anno e non sempre esplicitamente fin dall'inizio delle lezioni);
- le iniziative informative e formative (organizzazione/partecipazione ad eventi sul tema, utilizzo di risorse online del SIC Safer Internet Centre - Italia - Generazioni Connesse; Telefono Azzurro; Save the Children Italia; Unicef Italia ecc.);
- il monitoraggio e la valutazione delle azioni (laddove possibile, anche all'interno del RAV).

L'ePolicy viene aggiornata periodicamente in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con il Collegio docenti e con il Consiglio d'Istituto.

Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

Il monitoraggio e la revisione della e-Policy sarà svolta annualmente e /o qualora si verifichino cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno dell'Istituto. L'aggiornamento del documento di e-Policy sarà curato dal del Team per l'innovazione digitale e dal Team antibullismo.

Capitolo 2 - Formazione docenti e curriculum

2.1. Curriculum sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più “intuitivo” ed “agile” rispetto agli adulti, ma non per questo sono dotati di maggiori “competenze digitali”. Essere “nati nativi” (i “nativi digitali” sono nati dal 1994 al 2010) non vuol dire possedere le competenze civili e civiche connesse al digitale: bisogna saper distinguere tra i concetti di “nativi/nati digitali” “sapienti digitali” e “consapevoli digitali”

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

Riconoscere la caratteristica degli studenti quali “nati digitali” non esclude la necessità di impegnarsi per far loro sviluppare **le competenze digitali** (attualmente le 21 competenze connesse al digitale, definite dal nuovo Quadro DigComp 2.2 delle competenze digitali dei cittadini) e accompagnarli dall’essere “analfabeti/inconsapevoli digitali” all’essere “sapienti/consapevoli digitali”. Piuttosto è importante **individuare quale sia il loro livello di partenza** (bisogna partire sempre dalla rilevazione dei bisogni) perché è da lì che occorre partire e fissare gli obiettivi da raggiungere, obiettivi che devono essere differenziati a seconda del livello di scuola e della classe.

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 competente, consapevole e responsabile delle tecnologie digitali, inclusi i sistemi di IA.

Ciò avviene attraverso la progettazione e l’implementazione del CURRICOLO DIGITALE VERTICALE, allegato al PTOF, e redatto utilizzando le risorse e le fonti normative a disposizione a livello nazionale e internazionale.

La stesura del curriculum digitale d’Istituto è conforme ai documenti europei Digcomp 2.2, Digcompedu e al dettato della Legge 233 del 29 dicembre 2021 relativamente alle competenze digitali, declinate secondo le **cinque aree del quadro di riferimento DIGCOM** (Quadro comune di riferimento europeo per le competenze digitali) indicate nella seguente tabella:

Area 1: Alfabetizzazione su informazioni e dati

- 1.1 Navigare, ricercare e filtrare dati, informazioni e contenuti digitali
- 1.2 Valutare dati, informazioni e contenuti digitali
- 1.3 Gestire dati, informazioni e contenuti digitali

Area 2: Comunicazione e collaborazione

- 2.1 Interagire attraverso le tecnologie digitali
- 2.2 Condividere informazioni attraverso le tecnologie digitali
- 2.3 Esercitare la cittadinanza attraverso le tecnologie digitali
- 2.4 Collaborare attraverso le tecnologie digitali
- 2.5 Netiquette
- 2.6 Gestire l'identità digitale

Area 3: Creazione di contenuti digitali

- 3.1 Sviluppare contenuti digitali
- 3.2 Integrare e rielaborare contenuti digitali
- 3.3 Copyright e licenze
- 3.4 Programmazione

Area 4: Sicurezza

- 4.1 Proteggere i dispositivi
- 4.2 Proteggere i dati personali e la privacy
- 4.3 Proteggere la salute e il benessere
- 4.4 Proteggere l'ambiente

Area 5: Risolvere problemi (*problem-solving*)

- 5.1 Risolvere problemi tecnici
- 5.2 Individuare fabbisogni e risposte tecnologiche
- 5.3 Utilizzare in modo creativo le tecnologie digitali
- 5.4 Individuare divari di competenze digitali

Il Quadro (Framework) europeo DigComp 2.2 è organizzato in 21 competenze, suddivise in 5 aree. Ogni competenza viene declinata a 8 livelli di padronanza.

<https://repubblicadigitale.gov.it/portale/documents/20122/967347/DigComp+2.2+Italiano+marzo.pdf/3be86d9b-cc83-6d29-c55b-2489c27edb33?t=1679493691038>

Sono individuati **8 livelli di padronanza**: Base, Intermedio, Avanzato, Altamente specializzato (ciascuno suddiviso in due livelli). E inoltre parlare di competenza digitale è una semplificazione: DigComp individua **5 aree e 21 distinte competenze**. Ventun competenze che possono essere possedute, ciascuna, a otto diversi livelli.

Gli obiettivi generali del curriculum digitale d'Istituto sono:

- promuovere competenze digitali strutturate e l'utilizzo di Kit didattici aggiornati
- allineare l'istruzione digitale alle 5 aree di competenza del DigComp 2.2
- rendere gli alunni cittadini digitali consapevoli e rispettosi
- coinvolgimento, informazione/formazione sul campo delle famiglie

La scuola, declinando la competenza digitale seguendo il framework DigComp mira a raggiungere i seguenti obiettivi: almeno il Base 1 entro la Primaria e il Base 2 entro la conclusione della Secondaria di primo grado.

Le finalità formative delle TIC possono essere sintetizzate nei seguenti punti:

- Favorire la conoscenza dello strumento pc e/o tablet a scopo didattico
- Sostenere l'alfabetizzazione informatica
- Favorire la trasversalità delle discipline
- Facilitare il processo di apprendimento
- Favorire il processo di inclusione
- Fornire nuovi strumenti a supporto dell'attività didattica
- Promuovere situazioni collaborative di lavoro e di studio
- Sviluppare creatività e capacità di lavorare in gruppo
- Promuovere azioni di cittadinanza attiva
- Utilizzare in modo critico, consapevole e collaborativo la tecnologia.

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

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo. Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

Il Collegio docenti riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola, sia quelle liberamente scelte dai docenti (anche online) purché restino coerenti con il piano di formazione, come meglio indicato nel PTOF. L'attenzione all'uso delle TIC nella didattica rende gli apprendimenti più motivanti, coinvolgenti ed inclusivi, con una funzione di guida da parte del docente; inoltre, permette di sviluppare capacità che sono sempre più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza ed il confronto fra pari in modalità asincrona. La competenza digitale -oggi- è imprescindibile sia per i docenti sia per gli alunni e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa ed in grado di venire incontro ai nuovi stili di apprendimento.

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.

2.4. – Prevenzione e Sensibilizzazione delle famiglie; integrazioni al 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 scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

Capitolo 3 – Gestione dell'infrastruttura e della strumentazione ICT della e nella scuola

3.1 Protezione dei dati personali e GDPR

Ogni giorno a scuola vengono trattati numerosi dati personali del personale scolastico, degli alunni e delle rispettive famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali, e dati giudiziari. 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.

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8).

Le principali normative di riferimento sono:

- il D.lgs 196/2003 “Codice in materia di protezione dei dati personali” conosciuto come “Codice Privacy italiano”;
- il Regolamento UE Generale sulla Protezione dei dati n. 679/2016, noto anche come **GDPR** (General Data Protection Regulation);
- il D.Lgs. 10 agosto 2018, n. 101, Disposizioni attuative per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo
- Il GDPR prevale sul Codice Privacy italiano (quando un regolamento europeo entra in attuazione le leggi nazionali, nella parte in cui sono in contrasto col regolamento europeo, non possono essere applicate. Si chiama disapplicazione).

Definizione di dato personale:

“Qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale”.

Tipologia di dati:

- **Dati sensibili:** rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale (i dati relativi alla salute e alla vita sessuale sono detti “supersensibili”).
- **Dati comuni:** tutte quelle informazioni idonee a rivelare informazioni, come nome, cognome, codice fiscale, partite I.V.A, indirizzo, posta elettronica, numero di telefono, numero patente, e documento di identità.
- **Dati giudiziari:** informazioni idonee a rivelare provvedimenti in materia di casellario giudiziale, anagrafe delle sanzioni amministrative dipendenti da reati o carichi pendenti.

Soggetti responsabili e/o incaricati del trattamento dei dati personali in forma analogica (cartacea) e digitale (a mezzo strumenti informatici) - Privacy ed e-Privacy

- **Il titolare del trattamento:** persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali (art. 4 GDPR). Per la comunità scolastica il titolare del trattamento è l'Istituzione scolastica stessa, nella figura del Dirigente Scolastico.
- **Responsabile esterno del trattamento (art.28 del GDPR):** nelle scuole viene stipulato un contratto con un soggetto esterno, fornitore specializzato di servizi web e software gestionali, previa specifica delibera del Consiglio di Istituto.
- **Responsabile della Protezione dei Dati personali** (RPD o DPO= Data Protection Officer): con l'entrata in vigore del GDPR nelle scuole deve essere stipulato un contratto

- con un soggetto esterno che svolge questa funzione, previa specifica delibera del Consiglio di Istituto.
- **Referente interno in materia di protezione dei dati personali** (ex figura del Responsabile interno del trattamento, in base al D.lgs 196/2003): per la comunità scolastica è la figura del Direttore amministrativo (Dsga), che interviene sulla definizione delle modalità e dei mezzi del trattamento dei dati, elabora dati per conto del titolare e ha il compito di supportarlo nell'organizzazione e nel monitoraggio dell'organizzazione interna della privacy, di supervisionare gli adempimenti privacy e di aggiornare il DPS (Documento Programmatico Sicurezza) entro il 31 marzo di ogni anno o in occasione di modifiche significative ai fini della sicurezza dei dati trattati.
 - **Incaricato del trattamento**: la persona fisica autorizzata dal titolare o dall'Incaricato di I livello (ex Responsabile del trattamento) a compiere materialmente il trattamento.
 - **L'interessato**: la persona fisica a cui si riferiscono i dati stessi.

La gestione della Privacy e dell'e-Privacy del nostro Istituto ottempera tutte le indicazioni del D.lgs 196/2003 e del GDPR:

- nomina DPO
- definizione organigramma privacy
- rilascio informativa (famiglie, dipendenti, fornitori/altri soggetti) al momento della raccolta dei dati
- tenuta di un registro dei trattamenti dei dati personali per mezzo di sistemi di protocollazione/archiviazione elettronica

3.2 Accesso ad Internet, agli strumenti di comunicazione online e alla strumentazione personale

Al fine di garantire una gestione il più possibile corretta delle dotazioni tecnologiche, il nostro Istituto definisce e adotta il Regolamento interno "Sicurezza informatica a scuola e PUA - Politica di Uso Accettabile e sicuro della rete" (in sintesi **Regolamento PUA**"), a cui si rimanda integralmente. Il Documento PUA è parte integrante del DPS (Documento Programmatico della Sicurezza) e del PTOF della scuola (sezione Regolamenti d'Istituto).

In base al DPS e al Regolamento PUA d'Istituto, le principali strategie attuate sono:

- Il sistema informatico delle TIC della scuola viene regolarmente controllato in base alle norme di sicurezza
- E' predisposta una separazione fisica tra la rete didattica e quella amministrativa;
- Il sistema informatico della scuola è provvisto di un software antivirus aggiornato periodicamente;
- La connessione WiFi ad Internet dalle scuole è regolata da un meccanismo di autenticazione-autorizzazione;
- L'uso dei **computer presenti** e l'utilizzo dei **Kit laboratoriali informatici mobili** è regolamentato come descritto nel presente documento.
- L'uso delle dotazioni tecnologiche della scuola è funzionale al superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.

Si ribadisce che sono attivate, altresì, strategie di informazione/formazione sull'uso consapevole della rete:

- formazione del personale scolastico (inclusa l'auto-formazione tramite materiale informativo) sull'uso consapevole delle TIC e l'integrazione delle TIC nella didattica;
- sensibilizzazione delle famiglie e Patto di corresponsabilità
- costante e aggiornata informazione agli utenti sui pericoli della rete in relazione all'evoluzione delle tecnologie (anche in collegamento con le Forze di polizia e con gli Enti esterni pubblici e privati preposti);
- controllo (una tantum e/o all'evenienza di episodi dubbi) del sistema informatico (cronologia, temp, cookies, ecc.) da parte dei docenti che svolgono l'attività informatica;
- utilizzo di firewall e proxy;
- settaggio delle macchine in modo che agli utenti non sia consentito di scaricare e/o installare da Internet alcun tipo di software.

Nel regolamento PUA si fa riferimento anche al BYOD "Bring Your Own Device", ovvero all'uso della strumentazione personale. Come è noto, con la **nota n. 5274 del 11/07/2024 del MIM è stato introdotto il divieto dell'uso dello smartphone anche a fini didattici.**

Come stabilito dal Ministero dell'istruzione nel I Ciclo d'istruzione (dalla scuola d'infanzia fino alla secondaria di primo grado) è vietato l'utilizzo a scuola (all'interno dell'edificio e in tutte le sue pertinenze) di qualsiasi tipo di cellulare/smartphone **anche a fini educativi e didattici** (o tecnologia equivalente: orologi, occhiali, penne ecc. abilitati alla ricezione e trasmissione di dati ovvero alla memorizzazione di dati, quindi idonei alla trasmissione di dati anche se spenti). All'orario di entrata a scuola i docenti controlleranno che gli alunni ripongano il proprio cellulare spento in appositi spazi CONTENITORI posti nell'aula. Il cellulare potrà essere ripreso solo a fine giornata, al termine di tutte le lezioni.

Sono previste restrizioni equilibrate, e concordate con i genitori, nell'uso dello smartphone anche durante lo svolgimento di attività scolastiche al di fuori della scuola (viaggi d'istruzione, visite guidate ecc.)

I genitori e i docenti devono esercitare un costante controllo sull'uso degli smartphone che, in caso ci sia la necessità di portarli a scuola, devono rimanere chiusi negli zaini e spenti per tutto il periodo di permanenza a scuola (si declina ogni responsabilità riguardo a eventuali danni ai dispositivi elettronici portati in classe contravvenendo alle regole), e a promuovere un uso consapevole e responsabile della tecnologia in classe.

Gli alunni devono impegnarsi a:

- utilizzare in modo consapevole e corretto la RETE e i dispositivi telematici, nel rispetto della privacy e della dignità propria e altrui;
- rispettare le consegne dei docenti;
- non scaricare materiali e software senza autorizzazione;
- non utilizzare unità rimovibili personali senza autorizzazione;
- segnalare immediatamente materiali inadeguati ai propri genitori e ai propri insegnanti.

Capitolo 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:

- 4.1.1 commettere azioni online che possano danneggiare se stessi o altri;
- 4.1.2 essere una vittima di queste azioni;
- 4.1.3 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, ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. Ciò è possibile lavorando su aspetti di ampio raggio che possano permettere una riduzione dei fattori di rischio e di conseguenza una minore probabilità che i ragazzi si trovino in situazioni non piacevoli. È importante che 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 Codice interno per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo

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"*.

Al fine di intervenire preventivamente ed efficacemente e al fine di evitare, arginare ed eliminare possibili manifestazioni di comportamenti antisociali di bullismo e Cyberbullismo, il nostro Istituto definisce e adotta un **Codice interno per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo**, come previsto dalla Legge 17 maggio 2024, n. 70., allegato al PTOF, a cui si rimanda integralmente per informarsi sulle procedure interne /esterne di gestione e segnalazione di possibili casi di bullismo/cyberbullismo (su cosa va segnalato, con quali strumenti e a chi).

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.

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.

- Comitato Regionale Unicef: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- 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.
- Ufficio Scolastico Regionale: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- 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.
- Aziende Sanitarie Locali: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- 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.
- Tribunale per i Minorenni: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.
- Ufficio scolastico provinciale supporta le scuole della provincia per realizzare progetti di prevenzione, coordina le attività di rete per eventuali seminari e corsi di formazione, coordina le attività legate alla giornata mondiale sulla sicurezza in Internet.

4.3 Hate speech dentro e fuori la Rete: che cos'è e come prevenirlo

Il fenomeno di "incitamento all'odio" o "discorso d'odio" dentro e fuori la Rete si riferisce a parole, immagini, meme, video, commenti o post violenti che vengono usati per ferire le persone. Le **parole/immagini d'odio** mirano a svalutare, attaccare o addirittura incitare alla violenza contro un determinato gruppo di persone o un individuo.

Insulti e minacce colpiscono quotidianamente non solo sui social, ma sui giornali, in tv, nei film, nei testi musicali (rap/ trap pieni zeppi di insulti e parolacce), nelle manifestazioni e nelle piazze; vi sarà capitato di leggere o di ricevere insulti, se non addirittura ricevere minacce, dopo aver commentato una notizia sui social, soprattutto sui temi caldi: il rischio c'è per tutti.

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, eccetera) ai danni di una persona o di un gruppo.

Nello specifico è un comportamento e/o epiteti dispregiativi e offensivi (slurs) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischia di provocare reazioni violente, a catena.

Tale fenomeno, purtroppo, è sempre più diffuso ed è estremamente importante affrontarlo anche a livello educativo e scolastico, per cui il nostro Istituto ha inserito questa tematica nel curriculum di Italiano, Tecnologica, Arte e Immagine, Musica ed Educazione civica.

Insulti e offese fanno da sempre parte della storia dell'uomo e le parolacce non si sono poi così tanto evolute rispetto ai tempi di Dante ma gli insulti che oggi si scambiano sui social sono più pericolosi, servono per "zittire" o "ferire" le persone davanti a tantissime altre persone, a volte sono incitati appositamente, in altri casi la scintilla è innescata da notizie o *fake news*.

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.

L'Istituto ha inserito questa tematica nel curriculum di Scienze e di Educazione civica, e promuove azioni di prevenzione attraverso percorsi sul benessere digitale.

Inoltre, all'interno dell'Istituto operano docenti orientatori/mentor/coach che costituiscono uno "Sportello di Ascolto", al fine di supportare pedagogicamente gli alunni in difficoltà.

Il bilanciamento tra opportunità e rischi negli ambienti mediali e in relazione ai più giovani, richiede una costante e attenta negoziazione tra opportunità e rischi.

Occorre una linea condivisa con la famiglia per stabilire mezzi e modalità durante lo studio domestico, con tempi stabiliti e controllo attivo di genitori (Parental Control) durante la navigazione in 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 mediali 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.

La Legge 19 luglio 2019 n. 69, all'articolo 10, ha introdotto in Italia il reato di "revenge porn", ossia la diffusione illecita di immagini o di video sessualmente espliciti.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psico- sessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro e depressione.

Il nostro Istituto attiva percorsi di Educazione all'affettività al fine di informare ed accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) alle relazioni interpersonali positive. Inoltre, all'interno dell'Istituto operano docenti orientatori/mentor/coach che costituiscono uno "Sportello di Ascolto", al fine di supportare pedagogicamente gli alunni in difficoltà

4.6 - Adescamento online

Il **grooming** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenzialmente abusanti utilizzano per indurre i 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).

Il nostro Istituto attiva percorsi di Educazione all'affettività al fine di informare ed accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) alle relazioni interpersonali positive. Inoltre, all'interno dell'Istituto operano docenti orientatori/mentor/coach che costituiscono uno "Sportello di Ascolto", al fine di supportare pedagogicamente gli alunni in difficoltà.

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