Documento di ePolicy

FOIC81500Q

IC GAMBETTOLA

VIA GRAMSCI 37 - 47035 - GAMBETTOLA - FORLI'-CESENA (FO)

Giuliana Massaro

Capitolo 1 - Introduzione al documento di 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 E-policy, 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'E-policy, 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'E-policy 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 (ICT) 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.

Argomenti del Documento

Perché è importante dotarsi di una E-policy?

Attraverso l'E-policy 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’ E-policy 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.

Attraverso l'elaborazione del documento in questione, l’Istituto Comprensivo di Gambettola intende coinvolgere tutte le componenti della Comunità scolastica (personale della scuola, alunni/e e famiglie), proponendo uno strumento operativo ed accessibile a tutti, con lo scopo di diffondere l'uso critico e consapevole delle tecnologie digitali, in ambito didattico e, auspicabilmente, nella quotidianità.

La redazione dell'e-policy di istituto è avvenuta in conformità con le “Linee di orientamento per azioni di contrasto al bullismo e al cyberbullismo” del 15 aprile 2015 e successiva nota Miur prot. n. 482, “Linee di orientamento per la prevenzione del bullismo e del cyberbullismo” del 18 febbraio 2021.

L’obiettivo che ci si propone, innanzitutto, è quello di informare l'utenza sui rischi connessi all'impiego di Internet, al fine di dotare gli alunni di quelle competenze utili per la prevenzione delle problematiche derivanti da un utilizzo inadeguato delle tecnologie digitali. L'e-policy integra il Regolamento d’Istituto, con lo scopo di disciplinare e gestire eventuali infrazioni e stabilire le misure per la segnalazione di situazioni di rischio legate ad un uso improprio e scorretto delle tecnologie digitali nella scuola. Il presente documento è altresì parte integrante del PTOF e le azioni sottoscritte costituiscono indicazioni e buone prassi di azione e prevenzione in materia di bullismo e cyberbullismo.

La progettazione, gestione e monitoraggio delle iniziative formative promosse nell'ambito dell'e-policy saranno sviluppate nelle modalità ritenute compatibili a tempi, disponibilità professionali e vincoli economici dell'Istituto Comprensivo.

1.2 - Ruoli e responsabilità

Affinché l’E-policy 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 garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica; promuove la cultura della sicurezza online e, insieme

ai docenti referenti sulle tematiche del bullismo/cyberbullismo, favorisce la partecipazione a corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC. Il Dirigente Scolastico ha inoltre la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali, con eventuali segnalazioni alle autorità competenti.

L'Animatore digitale

L'Animatore digitale supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali. Inoltre 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); riceve segnalazioni in merito ad 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).

Il Referente bullismo e cyberbullismo

Il Referente bullismo e cyberbullismo ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo, non solo in ambito scolastico, ma anche in quello extrascolastico. Ha un ruolo di mediatore tra docenti e Dirigente Scolastico, informando tempestivamente quest'ultimo, nel caso in cui si verifichino episodi di bullismo o cyberbullismo.

I Docenti

I Docenti hanno un ruolo centrale nel diffondere la cultura dell'utilizzo responsabile delle TIC e della Rete, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica. I docenti accompagnano e supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'impiego della LIM o di altri dispositivi tecnologici che si connettono alla 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.

Il personale Amministrativo, Tecnico e Ausiliario (ATA)

Il personale ATA, così come previsto dal regolamento d'Istituto, è coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e nella raccolta di informazioni inerenti possibili casi di bullismo/cyberbullismo.

Gli Studenti e le Studentesse

Gli Studenti e le Studentesse utilizzano al meglio, in relazione al proprio grado di maturità e consapevolezza raggiunta, le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola imparano 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; segnalano ad un adulto eventuali episodi di bullismo o cyberbullismo di cui vengono a conoscenza.

I Genitori

Il Genitori, in continuità con l'Istituto scolastico, partecipano attivamente ai momenti di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali; si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicano con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet in ambito scolastico. È estremamente importante che accettino e condividano 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 sono chiamati a conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC; dovrebbero, inoltre, promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

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

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse 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).

Tutti gli attori esterni, inoltre, sono tenuti a prendere visione dell'e-Policy d'Istituto.

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

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.

L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

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.

La condivisione e la comunicazione del documento agli studenti e alle studentesse avviene attravero i percorsi trasversali di Educazione Civica, promossi dal Curricolo d'Istituto. Essi mirano a diffondere e consolidare l'uso consapevole e maturo dei dispositivi e della tecnologia informatica; regole condivise di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici; elementi per poter riconoscere e quindi prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e.

La condivisione e la comunicazione del documento al personale scolastico avviene durante i principali momenti collegiali, in modo da poter orientare tutte le figure sui temi in oggetto, a partire da un uso corretto dei dispostivi e della Rete in linea anche con il codice di comportamento dei pubblici dipendenti. Il Dirigente Scolastico condivide con gli interessati i relativi ambiti di competenza riferibili al presente documento

La condivisione e la comunicazione del documento ai genitori avviene tramite pubblicazione sul sito istituzionale della scuola, nonché tramite momenti di formazione specifici e durante gli incontri scuola-famiglia.

1.5 - Gestione delle infrazioni alla ePolicy

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

A seconda dell'età dello studente o della studentessa, è molto importante intervenire 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. È opportuno, inoltre, valutare la natura delle infrazioni all'ePolicy ed, eventualmente, comunicarne la gravità al Dirigente Scolastico, al fine di considerare la necessità di denunciare l'episodio o di garantire immediato supporto psicologico allo/la

studente/ssa attraverso i servizi predisposti, qualora ciò fosse necessario.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

L'aggiornamento del Regolamento sarà subordinato all'approvazione del Collegio dei Docenti e del Consiglio d'Istituto.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

Tali obiettivi riguardano prioritariamente la promozione delle competenze digitali e dell'uso delle TIC nei percosi educativi e didattici e la prevenzione e la gestione dei rischi online.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.

- Organizzare 1 evento di presentazione dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione dell'ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione dell'ePolicy rivolto ai genitori

Azioni da svolgere nei prossimi 3 anni:

- Organizzare uno o più eventi o attività volti a consultare i docenti sul monitoraggio dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori

Capitolo 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", C189/9, p.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.

Nel Curricolo disciplinare del nostro istituto, la competenza digitale viene trattata in maniera interdisciplinare e trasversalmente ai vari ordini scolastici. L'alunno, al termine del primo ciclo, distingue i diversi device e li utilizza correttamente, rispetta i comportamenti nella rete e naviga in modo sicuro. Comprende il concetto di dato e individua le informazioni corrette o errate, anche nel confronto con altre fonti.
Sa distinguere l'identità digitale da un'identità reale e sa applicare le regole sulla privacy tutelando se stesso e il bene collettivo.
Prende piena consapevolezza dell'identità digitale come valore individuale e collettivo da preservare. Argomenta attraverso diversi sistemi di comunicazione.
È consapevole dei rischi della rete e del come riuscire a individuarli.

Di seguito si riporta il curricolo trasversale sulle competenze digitali per gli studenti, elaborato dal team di tutti i docenti dell'istituto, dei vari gradi scolastici.

SCUOLA DELL'INFANZIA

	Campi d'esperienza	Traguardi	Obiettivi	Contenuti
Sezione tre anni	Tutti i campi di esperienza: **IL SE' E L'ALTRO** **IL CORPO E IL MOVIMENTO** **IMMAGINI, SUONI E COLORI** **I DISCORSI E LE PAROLE** **LA CONOSCENZA DEL MONDO**	Conosce e utilizza i primi strumenti tecnologici.	Utilizzo delle strumentazioni tecnologiche per la fruizione di contenuti audio e video inerenti alle tematiche trattate	Utilizziamo i dispositivi presenti a scuola per ascoltare canzoni e visionare immagini e filmati inerenti ai contenuti trattati
Sezione quattro anni	//	Conosce e utilizza i primi strumenti tecnologici.	Utilizzo delle strumentazioni tecnologiche per la fruizione di contenuti audio e video inerenti alle tematiche trattate	Utilizziamo i dispositivi presenti a scuola per ascoltare canzoni e visionare immagini e filmati inerenti ai contenuti trattati
Sezione cinque anni	//	Si avvia ad utilizzare con il supporto dell'insegnante i dispositivi multimediali in modo corretto.	Primo utilizzo dei dispositivi digitali (pc o tablet) per attività programmate e giochi didattici, sotto la guida attenta dell'insegnante	Progetto "Il mio amico computer": utilizzo del computer, conoscenza delle sue parti e del loro utilizzo; Costruiamo percorsi con le frecce direzionali (indicatori topologici)

SCUOLA PRIMARIA

	Monte ore annuo indicativo	**Traguardi**	**Obiettivi**	**Contenuti**
Classe prima	Tutti gli ambiti disciplinari	Utilizza in modo corretto e consapevole dispositivi digitali a scopi didattici. Inizia a comprendere la differenza tra mondo reale e virtuale.	Utilizzare i computer e i software didattici per attività e giochi di apprendimento con la guida e le istruzioni dell'insegnante.	Svolgimento di giochi didattici con la guida dell'insegnante. Attività di gioco e riflessione sulla differenza tra mondo virtuale e reale.
Classe seconda	Tutti gli ambiti disciplinari	Utilizza in modo corretto e consapevole i primi dispositivi digitali.	Conoscere le regole fondamentali di comportamento in ambiente digitale (regolamento della DDI)	Condivisione delle regole per la DDI (uso delle chat, del microfono, comportamento davanti alla telecamera).
Classe terza	8 ore	Utilizza le nuove tecnologie in modo sicuro e consapevole delle potenzialità e dei rischi.	Ricercare correttamente le informazioni sul WEB	Le principali funzioni dei dispositivi digitali.
Classe quarte	7 ore	Interagisce attraverso alcune tecnologie digitali.	Usare in modo consapevole gli strumenti digitali.	Utilizzo di software per la creazione di mappe concettuali interattive
Classe quinta	4	Usa in modo consapevole le nuove tecnologie nell'esercizio di una reale cittadinanza digitale.	Utilizzare in modo consapevole le nuove tecnologie.	Utilizzo delle TIC e delle principali funzioni dei dispositivi digitali per elaborare dati testi ed immagini. Riflessione in merito alle potenzialità del web ma anche ai rischi e ai pericoli nella ricerca e nell'impiego di fonti.

SCUOLA SECONDARIA DI I° GRADO				
	Discipline	Traguardi	Obiettivi	Contenuti
Classe prima	Italiano, Storia e Geografia	Avviamento all'utilizzo di vari device, in relazione dell'identità digitale come valore individuale e collettivo.	Conseguire padronanza nell'uso dei linguaggi e assumere	Cyberbullismo; gestione degli strumenti Google Workspace per la didattica.
	Matematica e Scienze	Capacità di ricercare correttamente informazioni sul web, interpretandone l'attendibilità.	-Riconoscere situazioni lesive dei diritti propri ed altrui ed assumere atteggiamenti di tutela. -Saper analizzare le informazioni ricevute valutandone l'utilità e distinguendo fatti e opinioni.	-L'uso consapevole della rete e nelle ricerche storiche -Le fake news -Uso responsabile dei social.
	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.

La professione docente è complessa e pertanto richiede competenze diverse ed integrate, fra queste anche quelle di tipo digitale. Le TIC, infatti, integrano la didattica al fine di progettare, sviluppare, utilizzare, gestire e valutare più efficacemente i processi di insegnamento e apprendimento di tutti gli studenti e le studentesse della classe, anche delle persone con Bisogni Educativi Speciali (in chiave inclusiva).

Di conseguenza, gli insegnanti dovrebbero raggiungere un buon livello di formazione ed aggiornarsi in merito all'utilizzo e l'integrazione delle TIC nella didattica, tenendo presente l'immagine che fornisce in merito il DigComp: "imparare a nuotare nell'oceano digitale". La metafora fornita dal documento indica che è necessario sapersi destreggiare, partendo dai compiti semplici (es.: individuare i fabbisogni informativi; trovare dati, informazioni e contenuti attraverso una semplice ricerca in ambienti digitale etc.) per arrivare ai compiti complessi che presentano molti fattori di interazione (ad es.: creare nuove app o piattaforme per navigare, ricercare e filtrare portali e offerte).

È su tali premesse che 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 dalle agenzie del territorio, sia quelle liberamente scelte dai docenti (anche online), purché restino coerenti con il piano di formazione.

Fondamentale, infatti, che vi sia 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. Le TIC permettono, inoltre, di sviluppare capacità che sono sempre più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza, il confronto fra pari in modalità asincrona e il problem solving.

La competenza digitale, oggi, è imprescindibile per i docenti così come per studenti e studentesse e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa e 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.

Nell'ottica di creare ulteriore sinergia fra scuola, studenti/studentesse e famiglie, di promuovere la condivisione di buone pratiche nell'utilizzo consapevole delle TIC e di prevenire e contrastare ogni forma di discriminazione, offesa, denigrazione e lesione della dignità dell'altro, nonché fenomeni di bullismo e cyberbullismo, è necessario e auspicabile che i docenti tutti dell'Istituto scolastico seguano un percorso formativo specifico ed adeguato che abbia ad oggetto non solo l'uso responsabile e sicuro della Rete ma anche i rischi legati a quest'ultime.

Formare i docenti sulle tematiche in oggetto vuol dire non pensare esclusivamente all'alfabetizzazione ai media ma anche considerare la sfera emotiva e affettiva degli studenti e delle studentesse che usano le nuove tecnologie. Essi/e, infatti, comunicano, esprimono se stessi e sviluppano l'identità personale e sociale, anche attraverso i dispositivi tecnologici che sempre di più consentono loro di poter entrare in contatto con il mondo che li circonda. Prestare attenzione a questi aspetti significa dare loro gli strumenti per poterli educare alle emozioni in contesto onlife e quindi modulare e gestire i propri ed altrui comportamenti, favorendo e promuovendo forme di convivenza civile.

I momenti di formazione e aggiornamento sono pensati e creati innanzitutto a partire dall'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica; dall'analisi del fabbisogno conoscitivo circa particolari argomenti che si sentono come più cogenti per i docenti e l'Istituto; dall'analisi delle richieste che provengono dagli studenti e dalle studentesse.

Si potrebbe anche pensare ad un cronoprogramma che consideri il triennio scolastico, in un'ottica di vera e propria programmazione, con azioni specifiche. Per esempio:

1. **Analizzare il fabbisogno formativo degli insegnanti sull'uso sicuro della Rete.**
2. **Promuovere la partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse".**
3. **Organizzare incontri con professionisti della scuola o con esperti esterni, enti/associazioni, etc.**
4. **Monitorare le azioni svolte per mezzo di specifici momenti di valutazione.**

Sul sito istituzionale della scuola, è incluso il link e i materiali informativi del progetto

"**Generazioni connesse**", dove trovare ulteriori approfondimenti, spunti aggiornamenti e strumenti didattici utili da usare con gli studenti e le studentesse, per ciascun grado di scuola.

2.4. - Sensibilizzazione delle famiglie e 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.

Il "Patto di Corresponsabilità" è un documento centrale per ogni istituzione scolastica e per la comunità educante tutta. Esso punta a "rafforzare il rapporto scuola/famiglia in quanto nasce da una comune assunzione di responsabilità e impegna entrambe le componenti a condividerne i contenuti e a rispettarne gli impegni" (Linee di indirizzo "Partecipazione dei genitori e corresponsabilità educativa"). I genitori sono dunque informati sulle condotte che si dovranno adottare a scuola, ciò in continuità anche con l'art. 5 (comma 2) della legge 29 maggio 2017, n.71 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" che prevede l'integrazione, oltre che del regolamento scolastico, anche del "Patto di Corresponsabilità".

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023)

- Effettuare un’analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un’analisi del fabbisogno formativo del corpo docente sull’utilizzo e l’integrazione delle TIC nella didattica.
- Effettuare un’analisi del fabbisogno formativo di tutto il personale scolastico sull’utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere il Consiglio d'Istituto per individuare i temi di maggiore interesse nell’ambito dell’educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri/seminari in base all'analisi dei bisogni formativi emersi.

AZIONI (da sviluppare nell’arco dei tre anni scolastici successivi)

- Organizzare e promuovere per il corpo docente incontri formativi sull’utilizzo e l’integrazione delle TIC nella didattica.
- Organizzare e promuovere per il personale scolastico incontri formativi sull’utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i genitori sull’educazione alla cittadinanza digitale.

Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT 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 lo scorso 19 settembre.

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.

La diffusione sempre maggiore di smartphone tra i giovanissimi, l'uso di tablet a scopo didattico, la condivisione online di contenuti didattici, l'uso del registro elettronico, l'eventualità di gruppi whatsapp tra studenti/esse, genitori, docenti o tra insegnanti e studenti/esse, obbliga la scuola ad avere un'attenzione particolare non solo alla privacy in generale, ma anche alla gestione della privacy legata all'uso dei nuovi dispositivi. La velocità, l'immediatezza con cui si risponde ai messaggi o si condividono foto o video, può far perdere il controllo di dati personali e mettere a rischio la reputazione e la sicurezza dei soggetti coinvolti.

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc.

Fra questi, particolarmente importanti sono:

- i dati che permettono l'identificazione diretta di una persona, come i dati anagrafici (ad es. nome e cognome);
- i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad es. il codice fiscale, l'indirizzo IP, il numero di targa);
- i dati rientranti in particolari categorie: si tratta dei dati cosiddetti sensibili, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale di una persona. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;
- i dati relativi a condanne penali e reati: si tratta dei dati cosiddetti giudiziari, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad es. i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto o obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Con l'evoluzione delle tecnologie digitali, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via Internet o telefono) e quelli che consentono la geo-localizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti di una persona.

Le parti "in gioco", quando si parla di dati personali, sono:

- L'interessato è la persona fisica alla quale si riferiscono i dati personali (art. 4, paragrafo 1, punto 1), del Regolamento UE 2016/679);
- Il titolare è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico, privato o l'associazione che adotta le decisioni sugli scopi e sulle modalità del trattamento (art. 4, paragrafo 1, punto 7), del Regolamento UE 2016/679);
- Il responsabile è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo del trattamento dei dati (art. 4, paragrafo 1, punto 8), del Regolamento UE 2016/679). Il Regolamento medesimo ha introdotto la possibilità che un responsabile possa, a sua volta e secondo determinate condizioni, designare un altro soggetto c.d. sub-responsabile (art. 28, paragrafo 2).

Con "Trattamento dei dati" si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o insiemi di dati personali (art. 4, par. 1, punto 2, del Regolamento (UE) 2016/679).

I soggetti che procedono al trattamento dei dati personali altrui devono adottare particolari misure per garantire il corretto e sicuro utilizzo dei dati.

Le istituzioni scolastiche pubbliche possono trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali, oppure quelli espressamente previsti dalla normativa di settore. Per tali trattamenti non sono tenute a chiedere il consenso degli/lle studenti/esse.

Alcune categorie di dati personali degli/lle studenti/esse e delle famiglie, come quelli sensibili e giudiziari, devono essere trattate con estrema cautela, nel rispetto di specifiche norme di legge, verificando in primis non solo la pertinenza e completezza dei dati, ma anche la loro indispensabilità rispetto alle "finalità di rilevante interesse pubblico" che si intendono perseguire.

Esempi di violazione sono il trattamento dei dati senza aver fornito all'interessato un'adeguata informativa o senza aver ottenuto uno specifico e libero consenso, qualora previsto.

In tali casi la persona interessata (studente/essa, professore, etc.) può presentare al Garante per la Protezione dei dati personali un'apposita "segnalazione" gratuita o un "reclamo" (più circostanziato rispetto alla semplice segnalazione e con pagamento di diritti di segreteria).

Le scuole, sia pubbliche che private, hanno l'obbligo di informare (tramite apposita informativa) gli interessati delle caratteristiche e modalità del trattamento dei loro dati, indicando i responsabili del trattamento.

Il nostro Istituto, in conformità al Regolamento UE 2016/679, si fa carico di:

- Valutarei rischi sulla privacy: (definita nel regolamento Data Protection Impact

Assessment o PIA) relativamente ad alcune tipologie di trattamento dei dati sensibili. Le istituzioni scolastiche pubbliche e private possono trattare anche dati sensibili, come ad esempio dati relativi alle origini razziali per favorire l'integrazione degli/lle alunni/e, dati relativi alle convinzioni religiose, al fine di garantire la libertà di culto, e dati relativi alla salute per adottare misure di sostegno degli/lle alunni/e, come i dati vaccinali con le Asl.

- Analizzare il processo sulla raccolta/gestione del consenso: occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio, all'interno di modulistica o sul proprio sito web istituzionale.
- Analizzare il sito web istituzionale di riferimento con proposte volte a migliorare la sicurezza e la protezione dei dati trattati.
- Mettere in sicurezza la intranet scolastica attraverso:

a) L'utilizzo di un proxy (un server che, ad esempio, si interpone nel flusso di comunicazione fra un computer e un sito Internet, eliminando il collegamento diretto fra il client e il server di destinazione. Permette di fornire un maggiore anonimato durante la navigazione in Rete, funziona da antivirus e memorizza una copia locale degli elementi web).

b) L'uso di un firewall hardware (componente hardware che, utilizzando un certo insieme di regole predefinite, permette di filtrare ed eventualmente bloccare tutto il traffico da e verso una qualsiasi rete di computer, lasciando passare solo tutto ciò che rispetta determinate regole).

La scuola prevede una liberatoria indirizzata alle famiglie e richiedente l'autorizzazione alle riprese fotografiche e video, per finalità eccedenti alla didattica (concorsi, progetti, iniziative sportive, ecc.).

Famiglie e studenti hanno il diritto di conoscere quali informazioni sono trattate dall'Istituto scolastico, farle rettificare se inesatte, incomplete o non aggiornate.

3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi*

operativi e applicazioni anche distribuite.

5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il 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.*

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

Il diritto di accesso a Internet è dunque 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".

Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

L'uso delle TIC è disciplinato da un'apposita sezione presente nel regolamento d'Istituto. Esso è un documento condiviso con la comunità scolastica, anche attraverso la sua pubblicazione sul sito della scuola.

Il suddetto documento stabilisce che, per gli studenti e le studentesse della Scuola dell'Infanzia e Primaria, non è consentito introdurre in ambiente scolastico i cellulari.

Tutti gli studenti si impegnano a:

- *utilizzare la rete nel modo corretto;*
- *rispettare le consegne dei docenti;*
- *non scaricare materiali e software senza autorizzazione;*
- *non utilizzare unità removibili personali senza autorizzazione;*
- *segnalare immediatamente materiali inadeguati ai propri insegnanti;*
- *tenere spento lo smartphone al di fuori delle attività didattiche che ne prevedano l'utilizzo (Scuola Secondaria di Primo Grado);*
- *durante le attività che prevedono lo smartphone, utilizzarlo esclusivamente per svolgere le attività didattiche previste (Scuola Secondaria di Primo Grado).*

I docenti si impegnano a:

- *utilizzare la rete nel modo corretto;*
- *non impiegare device personali se non per uso didattico;*
- *formare gli studenti all'uso della rete;*
- *dare consegne chiare e definire gli obiettivi delle attività;*
- *monitorare l'uso che gli studenti fanno delle tecnologie a scuola.*

La scuola informerà che si farà carico di tutte le precauzioni necessarie per garantire agli/lle studenti/esse l'accesso a materiale appropriato, ma che allo stesso tempo non può essere responsabile per l'accesso autonomo da parte degli/lle studenti/esse a materiali inadeguati e potenzialmente dannosi trovati online.

Le informazioni sull'e-Safety a scuola sono fornite ai genitori all'interno del Patto di Corresponsabilità.

Anche il personale scolastico prende visione del regolamento, consapevole che l'uso improprio di Internet verrà segnalato.
Per attuare la cybersecurity il nostro Istituto provvede a:

- Mantenere separate le reti didattica e segreteria;
- Aggiornare, ogni qualvolta si renda necessario, software e Sistema operativo;
- Definire la programmazione di backup periodici;
- Garantire formazione adeguata allo staff, incluso il corpo docente;
- Preparare piani di azione in risposta ai problemi più seri;
- Definire una policy sulle password: non usare password facilmente identificabili (nomi dei figli, compleanni, etc.), non memorizzare le password nei dispositivi scolastici, non condividere le password con nessuno, non utilizzare la stessa password su siti differenti;
- Minimizzare i privilegi amministrativi.

La pianificazione che riguarda l'acquisizione, la gestione e il mantenimento dell'infrastruttura di rete tiene in considerazione due aspetti:

- **lo status quo**, cioè la disponibilità attuale di tecnologia nella scuola e come rendere l'infrastruttura sicura, accessibile ma anche funzionante e adatta allo scopo.
- **l'analisi dei bisogni della scuola** (o del plesso), in relazione alle reali esigenze didattiche e agli obiettivi prefissati.

La scuola chiede ai genitori degli/lle studenti/esse minori di 16 anni di età il consenso all'uso della piattaforma Google Workspace.

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.

Nella comunicazione mediata dalle tecnologie non condividiamo lo stesso spazio e lo stesso contesto comunicativo con i nostri interlocutori. Il cosiddetto feed-back non tangibile e l'impossibilità di accedere ai segnali non verbali del nostro interlocutore, così come la distanza e la separazione mediante lo schermo, ci rendono meno empatici e quindi meno attenti a emozioni e potenziali reazioni dell'altra persona. Inoltre, la comunicazione che viaggia online, generalmente, si avvale di messaggi scritti che possono essere memorizzati, diffusi e permangono nel tempo.

D'altro canto, grazie agli strumenti di comunicazione online, possiamo usufruire dell'interattività del mezzo, superare le barriere spazio-temporali, usare un linguaggio multimediale, ipertestuale e accattivante, promuovere la partecipazione e il coinvolgimento dei diversi attori in gioco nel processo educativo.

Gli strumenti di comunicazione - interna ed esterna - dell'istituto sono: il registro elettronico, il sito web istituzionale, le risorse della piattaforma Google Workspace ed e-Twinning.

Il registro elettronico, in particolare, permette di gestire la comunicazione con le famiglie, le quali attraverso di esso possono visualizzare molte informazioni utili, interagendo con la scuola, in modo differente a seconda dei diversi ordini scolastici dell'Istituto.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle 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. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente ***ePolicy*** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

Alla luce del quadro normativo e di indirizzo di riferimento, i docenti non possono fare uso, per scopi personali, di smartphone o altri dispositivi digitali.

Nel Decreto del Presidente della Repubblica 21 Novembre 2007, n. 235 "Regolamento recante modifiche ed integrazioni al decreto del Presidente della Repubblica 24 giugno 1998, n. 249", concernente lo statuto delle studentesse e degli studenti della scuola secondaria, che si introduce il Patto educativo di corresponsabilità e giornata della scuola (Art. 3) che definisce, attribuendole, le responsabilità fra istituzione scolastica e famiglia. Oggi, il Patto va letto anche in riferimento all'educazione dei ragazzi e delle ragazze all'uso dei nuovi dispositivi tecnologici, inclusi tablet e smartphone sia a scuola che a casa.
Riguardo il Codice della Privacy, D. Lgs. 196/2003, modificato e integrato dal D. Lgs. 101/2018 recependo il regolamento UE 2016/679 e art.10 del Codice Civile, ricordiamo che "Spetta comunque agli istituti scolastici decidere nella loro autonomia come regolamentare o se vietare del tutto l'uso dei cellulari. Non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese. È bene ricordare che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere lo studente in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati.
Stesse cautele vanno previste per l'uso dei tablet, se usati a fini di registrazione e non soltanto per fini didattici o per consultare in classe libri elettronici e testi on line".
L'attenzione verso le tecnologie digitali e il loro utilizzo in classe diventa così inclusivo e creativo, nel senso che le stesse vengono riproposte come strumenti da inserire nella didattica e nelle sperimentazioni laboratoriali. L'uso viene consentito per scopi prettamente didattici, sotto il controllo e la responsabilità del docente che pianifica l'attività didattica.

"La scuola digitale, in collaborazione con le famiglie e gli enti locali, deve aprirsi al cosiddetto BYOD (Bring Your Own Device), ossia a politiche per cui l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficace".

BYOD letteralmente significa "porta il tuo dispositivo" ed è un'espressione che descrive quelle politiche aziendali che in tutto il mondo consentono agli impiegati di utilizzare i propri dispositivi personali in ambiente di lavoro.

In tal senso, gli smartphone, i tablet e i pc personali possono essere integrati nel

lavoro nelle classi quando ben progettato e calibrato per discipline e obiettivi formativi e didattici: si pensi, a titolo di esempio, agli student response systems ossia alla possibilità degli studenti e delle studentesse di rispondere a quiz e sondaggi utilizzando direttamente il proprio smartphone come telecomando sempre sotto la guida e il controllo dell'insegnante.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).

- Organizzare un evento volto a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare una o più attività volte a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).

Verrà individuata una o più delle seguenti azioni, a seconda dei bisogni emergenti:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte delpersonale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto perredigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione degli studenti/studentesse suindicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamentisull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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:

- 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, 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.*

Le azioni di sensibilizzazione per essere efficaci dovranno essere chiare e mirate sullo stato attuale del tema o del problema in modo tale da:

- Accrescerne la consapevolezza nel gruppo di riferimento;
- Incoraggiare il gruppo a modificare i propri comportamenti rendendoli più

funzionali;
- Diffondere all'esterno del gruppo e quindi tra la comunità educante la coscienza rispetto all'argomento di interesse;
- Coinvolgere i soggetti esterni in modo da creare sinergie finalizzate al perseguimento di un obiettivo comune;
- Favorire la diffusione di informazioni e servizi disponibili alla collettività, in primis promuovere la conoscenza dell'ePolicy nella comunità scolastica ed educante.

Parallelamente alle azioni di sensibilizzazione si dovrà elaborare un piano di prevenzione a più livelli, partendo dal presupposto che tutti gli studenti che navigano sul WEB sono potenzialmente a rischio.

Il primo livello (prevenzione universale) comprende gli interventi non specifici diretti a produrre cambiamenti, se pur modesti, sull'intera popolazione scolastica, ad esempio progetti dedicati alle competenze emotive o alla cittadinanza digitale.

Il secondo livello (prevenzione selettiva) è dedicato ad un gruppo di studenti in cui il rischio online è stato accertato tramite precedenti indagini e/o segnalazioni fatte dalla scuola e si basa su azioni formative strutturate.

Il terzo livello (prevenzione indicata) consta di un programma di intervento ad hoc per ciascun caso specifico; è quindi pensato e strutturato per ridurre i comportamenti problematici delle studentesse e degli studenti e per dare supporto alle vittime, avvalendosi eventualmente della collaborazione della famiglia e di professionalità diverse (sportello d'ascolto, servizi sanitari).

La scuola, le famiglie, le istituzioni, le associazioni e la società civile sono responsabili dell'azione formativa e preventiva nei confronti di bambine, bambini e adolescenti e sono chiamate a collaborare ad un progetto educativo comune e condiviso.

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 per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Come previsto dalla normativa vigente, il nostro istituto ha nominato un referente che si occupa della prevenzione e del contrasto del bullismo e cyberbullismo; si propone inoltre di integrare il regolamento di istituto con norme relative alle tematiche suddette, di condividerlo con studenti e genitori e di porne un estratto in ogni singola classe dalla Primaria alla Secondaria.

Al regolamento d'Istituto è allegata una scheda di segnalazione di eventuali atti di bullismo e/o cyberbullismo in cui vengono riportate le modalità di compilazione e di consegna.

Sul sito si prevede di pubblicare una guida per i genitori, con riferimenti di siti, servizi, numeri telefonici per un supporto psicologico e legale in caso di problematiche legate al bullismo e/o cyberbullismo.

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

Tale fenomeno, purtroppo, è sempre più diffuso ed 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.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

1. Promuovere tra gli studenti i principi di solidarietà, di rispetto e di tolleranza dell'altro;

2. Riconoscere l'importanza del linguaggio come strumento per negare o sostenere i diritti degli altri;

3. Apprezzare l'unicità di ogni individuo;

4. Accrescere l'autostima di ciascun individuo;

5. Stimolare nei bambini/e, ragazzi/e il pensiero critico, favorire la discussione e l'apprendimento cooperativo.

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 è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale?

Il nostro Istituto si propone di organizzare incontri con associazioni di professionisti del settore rivolti a genitori, insegnanti e studenti per sensibilizzare la comunità scolastica sui temi suddetti e fornire ove necessario supporto psicologico.

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*, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti.

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 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).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

Il nostro Istituto si propone di sensibilizzare gli studenti sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni. Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.

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.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito 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.

Qualora si ravvisi un rischio per il benessere psicofisico dei/lle bambini/e, ragazzi/e coinvolte nella visione di questi contenuti, sarà opportuno ricorrere a un supporto psicologico anche passando per una consultazione presso il medico di base o pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza: Consultori Familiari, Servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, etc.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023)

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi)

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.

- Promuovere incontri e laboratori per studenti e studentesse dedicati all’Educazione Civica Digitale.

Capitolo 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**.
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

Inoltre, la scuola **individua le figure che costituiranno un team** preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

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

Tali procedure sono comunicate e condivise con l'intera comunità scolastica.

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.

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

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

- **Cyberbullismo**: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online**: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting**: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere 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.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per

segnalare la presenza di materiale pedopornografico online.

Si considerano da segnalare tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o un piccolo gruppo) tramite un utilizzo irresponsabile di internet. La scuola, quindi, avrà cura di porre attenzione alla rilevazione di rischi connessi alla navigazione sul web. In modo particolare al cyberbullismo, all'adescamento online e al sexting.

In particolare si segnaleranno:

- Contenuti afferenti la violazione della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);

- Contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);

- Contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

Tutte le segnalazioni riportate dai docenti verranno registrate su apposita scheda.

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, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

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 bullismo e/o cyberbullismo, sexting o adescamento online.

Per tutti i dettagli fate 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 ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Attualmente è attivo, presso il nostro Istituto, uno sportello di ascolto psicologico per fornire supporto a chi ne fa richiesta. Il servizio è rivolto a studenti della scuola secondaria, docenti e genitori.

Si sottolinea che la rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti. Il personale scolastico, soprattutto nella componente docente, ma anche in quella del personale ATA, è invitato ad evitare atteggiamenti accusatori o intimidatori, in modo tale da riuscire a ricevere dai minori più fragili segnalazioni e confidenze circa situazioni problematiche vissute. E' fondamentale, infatti, osservare per tempo ciò che accade, per poter agire immediatamente nei confronti di atti non opportuni e in modo tale da poter scongiurare conseguenze a lungo termine ben più gravi, in quanto negative per il benessere e la crescita armonica dei minori coinvolti. La gestione dei casi rilevati andrà differenziata a seconda della loro gravità; è in ogni caso opportuna la condivisione a livello di Consiglio di Classe/Team di Docenti di ogni episodio rilevato. Alcuni avvenimenti di lieve rilevanza possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e individuare una strategia comune per affrontarlo e rimediare. Per i casi più gravi bisogna informare il

Dirigente Scolastico che nel caso di reati veri e propri effettuerà la denuncia all'autorità giudiziaria.

Come segnalare eventuali casi?
Il personale della scuola, anche con l'ausilio del personale di assistenza tecnica e dell'Animatore digitale, dovrà provvedere a conservare le eventuali tracce di una navigazione non consentita su Internet o del passaggio di materiali inidonei sui pc della scuola; la data e l'ora consentiranno di condurre più approfondite indagini; nel caso di messaggi, si cercherà di risalire al mittente attraverso i dati del suo profilo. Sia nel caso di chat che di messaggi di posta elettronica, l'insegnante dovrà copiare e stampare i messaggi per fornire le eventuali prove dell'indagine sugli abusi commessi. Tali prove saranno utili anche ad informare la famiglia dell'alunno vittima di abuso, il Dirigente Scolastico e, ove si configurino reati, la Polizia Postale e la magistratura inquirente. In ogni caso, sarà opportuna una tempestiva informazione delle famiglie in merito all'accaduto, per consentire ulteriori indagini e, in assenza di prove oggettive, raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico ed, eventualmente, alla Polizia Postale. Qualora siano coinvolti più alunni, in qualità di vittime o di responsabili della condotta scorretta, le famiglie degli alunni in questione saranno informate tempestivamente per un confronto.

In base all'entità dei fatti si provvederà a:

1) una comunicazione scritta tramite diario alle famiglie;

2) una nota disciplinare sul registro di classe;

3) una convocazione formale dei genitori degli alunni, tramite segreteria;

4) una convocazione delle famiglie da parte del Dirigente Scolastico.

Per i reati più gravi gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti). Inoltre è possibile avvalersi dei due servizi messi a disposizione dal Safer Internet Center il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children. Una volta ricevuta la segnalazione, infatti, gli operatori procederanno a coinvolgere le autorità competenti in materia.

5.3. - Gli attori sul territorio

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.

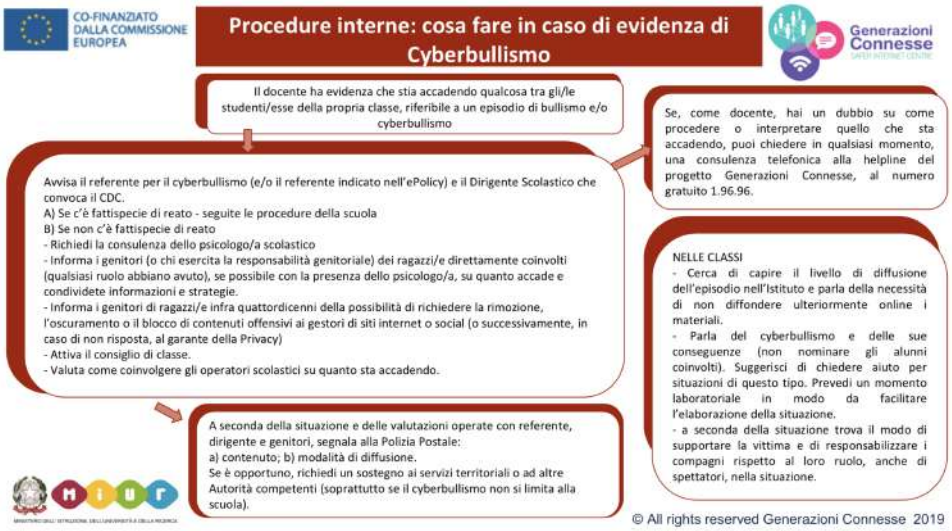
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **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.

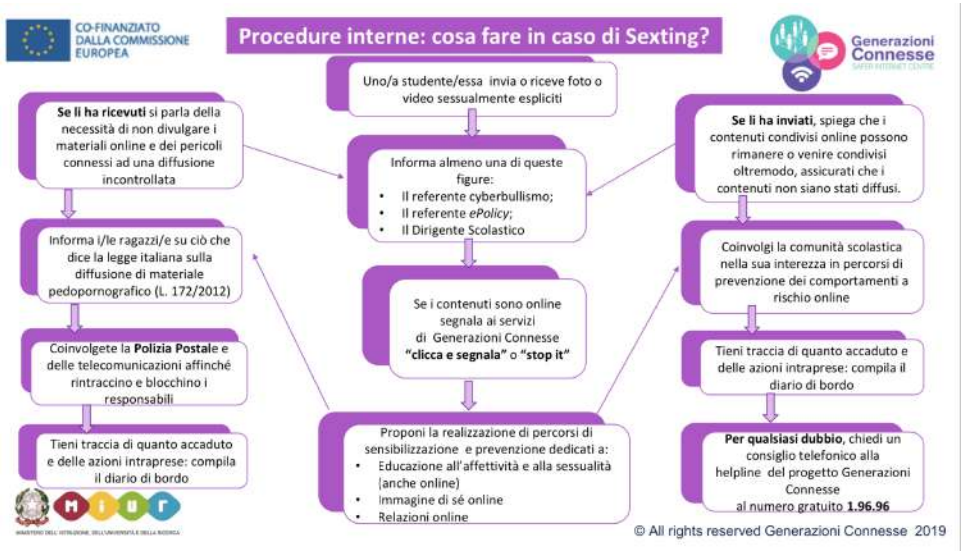
Nei casi di maggiore gravità, si valuterà anche il coinvolgimento di attori esterni quali forze dell'ordine e servizi sociali. I documenti relativi alle procedure operative e i protocolli sono da elaborare in collaborazione con i suddetti attori del territorio, con cui siglarli unitamente.

5.4. - Allegati con le procedure

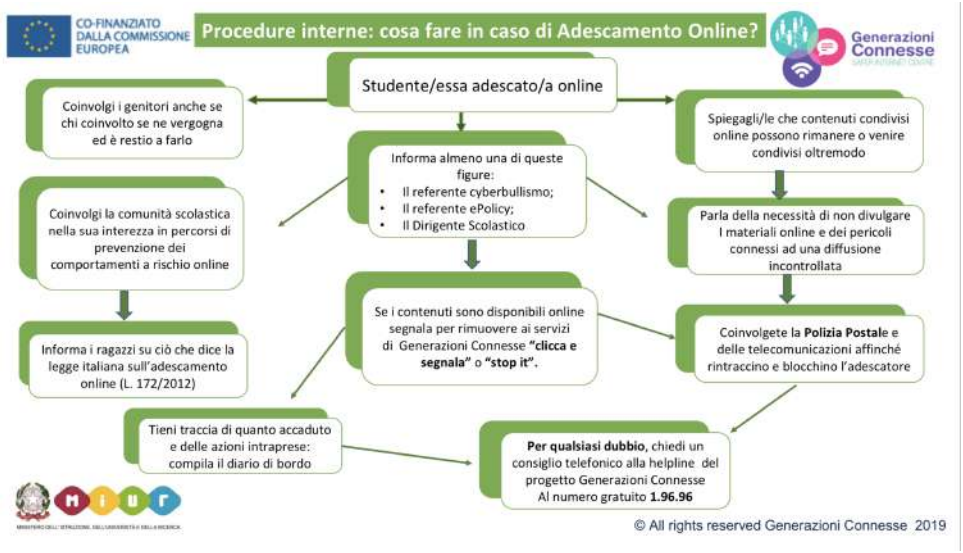
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



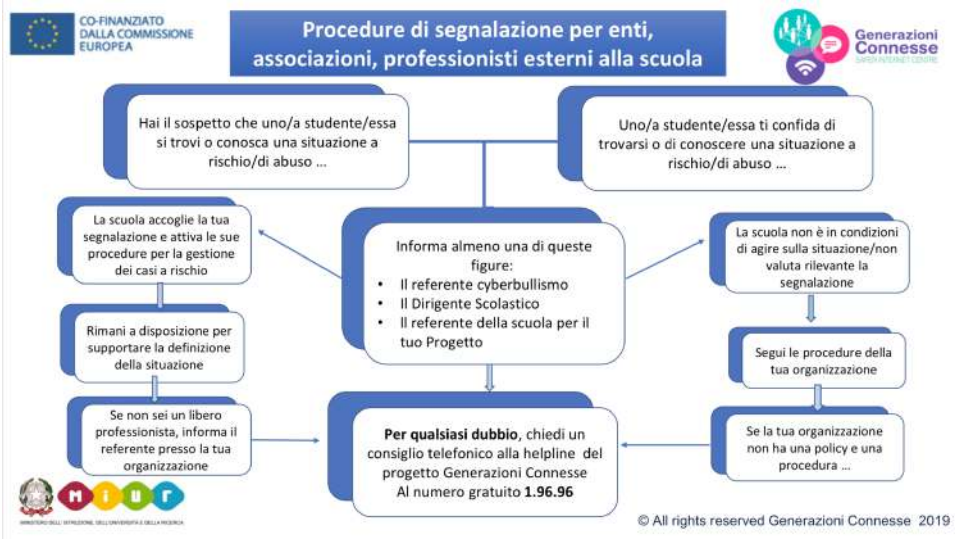
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola



Altri allegati

- Scheda di segnalazione
- Diario di bordo
- iGloss@ 1.0 l'ABC dei comportamenti devianti online
- Elenco reati procedibili d'ufficio

Il nostro piano d'azioni

Sulla base delle "Linee guida per l'uso positivo delle tecnologie digitali e della prevenzione dei rischi nelle scuole", il nostro Istituto Comprensivo assume i seguenti punti per una collaborazione sinergica tra scuola-famiglia-servizi territoriali, al fine di creare un modello composito e lineare di azioni condivise e di promuovere l'educazione adlla cittadinanza digitale.

IL NOSTRO PIANO DI AZIONI

Presentazione del documento di ePolicy

- Organizzare un evento di presentazione dell'ePolicy rivolto agli studenti;
- Organizzare un evento di presentazione dell'ePolicy rivolto ai docenti;
- Organizzare un evento di presentazione dell'ePolicy rivolto ai genitori;

Analisi dei bisogni

- Effettuare un’analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un’analisi del fabbisogno formativo del corpo docente sull’utilizzo e l’integrazione delle TIC nella didattica.
- Effettuare un’analisi del fabbisogno formativo di tutto il personale scolastico sull’utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere il Consiglio d'Istituto per individuare i temi di maggiore interesse nell’ambito dell’educazione alla cittadinanza digitale.

Formazione

- Organizzare e promuovere per il corpo docente incontri/seminari in base all'analisi dei bisogni formativi emersi.
- Organizzare uno o più eventi o attività volti a formare la comunità scolastica sui temi delle tecnologie digitali, della protezione dei dati personali, dell’accesso ad Internet e dell’uso sicuro delle tecnologie digitali (cybersecurity).

Sensibilizzazione e Prevenzione

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all’utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, ai genitori e ai docenti con il coinvolgimento di esperti.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all’Educazione Civica Digitale.