POLO STATALE D'ISTRUZIONE SECONDARIA SUPERIORE "MATTARELLA - DOLCI"
Castellammare del Golfo - Alcamo

Documento di ePolicy

TPIS008004

IS "P.MATTARELLA-D.DOLCI" C/MARE GOLFO

VIA FLEMING N.19 - 91014 - CASTELLAMMARE DEL GOLFO - TRAPANI (TP)

Caterina Agueci

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.

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.

Dirigente Scolastico

Il Dirigente Scolastico garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica; promuovere la cultura della sicurezza online e collabora all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC.

Il Dirigente Scolastico ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

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, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto per la promozione della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche in relazione all'educazione civica).

L'animatore digitale, inoltre, 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).

Referente bullismo e cyberbullismo

"Ogni Istituto scolastico, nell'ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo" (Art. 4 Legge n.71/2017, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo". Tale figura ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del

bullismo e del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio.

Il Referente può coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

Docenti

I Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. I Docenti possono integrare parti del curriculum della propria disciplina con approfondimenti ad hoc, 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'uso 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 Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il dirigente scolastico e con il personale docente tutto. Si occupano ciascuno per le proprie mansioni, del funzionamento dell'Istituto scolastico che passa anche attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola.

Il personale ATA è coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

Gli Studenti e le Studentesse

Gli Studenti e le Studentesse devono, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola 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 farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

I Genitori

I Genitori, in continuità con l'Istituto scolastico, devono essere partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali; 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. I Genitori accettano e condividono quanto scritto nell'ePolicy dell'Istituto.

Enti educativi esterni e le associazioni

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola si conformano alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC; promuovono comportamenti sicuri, la sicurezza online e assicurano la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

Gli Enti educativi esterni e le associazioni accettano e condividono quando espresso nella sezione specifica dell'ePolicy per gli attori esterni.

Per un approfondimento sui ruoli e le responsabilità delle figure presenti a scuola: Legge 59/97, Art. 21 CO° 8; Legge N.165/2001 Art. 25; CCNL; DPR n. 275/99; Legge n.107/2015; Piano Nazionale Scuola Digitale.

Esiste una corresponsabilità educativa e formativa che riguarda sia i genitori che la scuola nel percorso di crescita degli studenti e delle studentesse. A tal proposito il 2° comma dell'art. 2048 c.c. così recita: "I precettori e coloro che insegnano un mestiere o un'arte sono responsabili del danno cagionato dal fatto illecito dei loro allievi e apprendisti nel tempo in cui sono sotto la loro vigilanza". Per i genitori, invece, bisogna considerare: il 1° comma dell'art. 30 della Costituzione "è dovere e diritto dei genitori mantenere, istruire ed educare i figli, anche se nati fuori del matrimonio"; il 1° comma dell'art. 2048 c.c. ai sensi del quale "il padre e la madre o il tutore sono responsabili del danno cagionato dal fatto illecito dei figli minori non emancipati o delle persone soggette alla tutela, che abitano con essi (…)"; l'art. 147 del c.c. "l'obbligo di mantenere, istruire, educare e assistere moralmente i figli, nel rispetto delle loro capacità, inclinazioni naturali e aspirazioni (...)".

Dato questo quadro normativo, rispetto ad un profilo prettamente processuale anche in materia di bullismo e cyberbullismo (dunque non in via esclusiva), si può parlare di tre tipologie di "culpa":

- culpa in vigilando: concerne la mancata sorveglianza attiva da parte del docente responsabile verso il minore (cosi come da art. 2048 del c.c.). Tale condizione è superabile se ci si avvale di una prova liberatoria di non aver potuto impedire il fatto (recita il terzo comma dell'art. 2048 c.c.: "le persone indicate nei commi precedenti sono liberate dalla responsabilità soltanto se provano di non aver potuto impedire il fatto").
- culpa in organizzando: si riferisce ai provvedimenti previsti e presi dal Dirigente Scolastico ritenuti come non soddisfacenti e quindi elemento favorevole al verificarsi dell'eventuale incidente.
- culpa in educando: fa capo ai genitori i quali hanno instaurato una relazione educativa con il/la figlio/a, ritenuta come non adeguata, insufficiente o comunque carente tale da metterlo/a nella situazione di poter recare danno a terzi.

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 i soggetti esterni che erogano attività in ambito scolastico vengono sensibilizzati e resi consapevoli dei rischi online che possono correre gli studenti e le studentesse e dei comportamenti corretti che devono adottare a scuola.

A tale scopo nel successivo capitolo 5 del presente documento di ePolicy è presente il modulo di Segnalazione, anche per i soggetti esterni, utile qualora si verifichino episodi che mettano in pericolo studenti e studentesse. Le procedure di segnalazione devono contenere i riferimenti interni alla scuola a cui rivolgersi in tali situazioni, a titolo di esempio, il referente cyberbullismo, il referente del progetto, il/la coordinatore/trice di classe.

L’Istituto si riserva inoltre la possibilità di richiedere agli attori esterni, eventualmente, il casellario giudiziale come fattore ulteriormente protettivo verso i minori. L’obiettivo è quello di verificare l’esistenza (o meno) di condanne per alcuni reati previsti dal Codice penale e nello specifico gli articoli 600-bis (prostituzione minorile), 600-ter (pornografia minorile), 600-quater (detenzione di materiale pornografico), 600-quinquies (iniziative turistiche volte allo sfruttamento della prostituzione minorile), 609-undecies (adescamento di minorenni), o l’irrogazione di

sanzioni interdittive all'esercizio di attività che comportino contatti diretti e regolari con i minori. L'eventuale presenza di un codice di condotta adottato dalla propria organizzazione o associazione (cooperativa, ente di formazione, servizio, etc.) è un fattore preferenziale.

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.

Oltre alla pubblicazione del documento sul sito istituzionale della scuola, sarà redatta una versione child friendly (ad es. Infografica, prodotto digitale con PowToon) del documento per la comunicazione e la sensibilizzazione degli studenti e delle studentesse.

Tramite la pubblicazione sul sito web della scuola si considerano informate le famiglie e la comunità scolastica.

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.

Nel capitolo 5, verranno analizzati, nello specifico, alcuni dei principali rischi connessi ad un uso poco consapevole delle tecnologie digitali e verranno anche esposte le relative procedure di segnalazione e gestione delle infrazioni (anche in riferimento agli specifici regolamenti in materia).

Segue, a titolo esemplificativo, un elenco di infrazioni alle quali farà seguito il documento:

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

In funzione della natura e gravità di quanto accaduto si potrà **considerare la necessità di denunciare l'episodio** (con il coinvolgimento ad es. della Polizia Postale) o di garantire immediato supporto psicologico allo/la studente/ssa attraverso i servizi predisposti, qualora ciò fosse necessario.

Anche il personale scolastico può incorrere nelle relative procedure di segnalazione e gestione delle infrazioni, ad esempio in caso di improprio utilizzo di device o della Rete, nonché in caso di non intervento nella segnalazione di condotte improprie dei/lle propri/ie studenti/studentesse.

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.

La scuola si impegna ad aggiornare i propri regolamenti alla luce del documento redatto di ePolicy.

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.

Ai fini del monitoraggio lo strumento che si utilizzerà sarà un Google moduli o similare.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti

Azioni da svolgere nei prossimi 3 anni:

- 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
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy 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.

L'Istituto si impegna a progettare e implementare il curricolo sulle competenze digitali. Come già evidente nella definizione iniziale delle Raccomandazioni Europee, le competenze digitali richiamano diverse dimensioni sulle quali sarà possibile lavorare in classe, in un'ottica che integra la dimensione tecnologica con quella cognitiva ed etica (Calvani, Fini e Ranieri 2009):

- **dimensione tecnologica**: è importante far riflettere i più giovani sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana, onde evitare automatismi che abbiano conseguenze incerte, attraverso un'adeguata comprensione della "grammatica" dello strumento.
- **dimensione cognitiva:** fa riferimento alla capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità.

- **dimensione etica e sociale**: la prima fa riferimento alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui, e di usare le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri. La seconda, invece, pone un po' più l'accento sulle pratiche sociali e quindi sullo sviluppo di particolari abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online.

Il curricolo sulle competenze digitali dell'Istituto, il cui comune obiettivo è quello di Esercitare i principi della cittadinanza digitale, con competenza e coerenza rispetto al sistema integrato di valori che regolano la vita democratica, è incentrato sulle seguento tematiche:

(per il primo biennio)

1. La Dichiarazione dei diritti in Internet;
2. Le Netiquette per comunicare e condividere in rete;
3. La (dis)informazione naviga sul Web;
4. Le trappole del Web e non solo.

(per il secondo biennio)

1. La cybersecurity;
2. Tutelare la privacy;
3. I Social Network;
4. Le tecnologie digitali al servizio del cittadino.

(per il V anno)

1. Il cittadino digitale;
2. L'informazione tra realtà e menzogna;
3. La cultura naviga sul Web.

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.

L'attenzione all'uso delle TIC nella didattica risulta fondamentale: un loro utilizzo strutturato e integrato non solo può rendere gli apprendimenti motivanti, coinvolgenti ed inclusivi, ma permette al docente di guidare studenti e studentesse rispetto alla fruizione dei contenuti online, ormai la modalità naturale di apprendimento al di fuori della scuola. Inoltre, permettono di sviluppare capacità che sono sempre più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza e il confronto fra pari in modalità asincrona.

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

La formazione farà riferimento al DigComp, al Piano di formazione dell'Istituto e all'offerta formativa dell'Ambito 27.

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.

I momenti di formazione e aggiornamento sono pensati e creati 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 in modo, poi, da riutilizzare nel loro lavoro di educatori (attraverso le modalità che il docente indica e ritiene più

confacente alla classe) quanto appreso durante la formazione ricevuta.

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022)

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.

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

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.

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”, come si legge nelle Linee di indirizzo *Partecipazione dei genitori e corresponsabilità educativa*, 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”.

In continuità 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*, l'Istituto ha integrato sia il regolamento scolastico che il “Patto di Corresponsabilità” con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari “commisurate alla gravità degli atti compiuti”, al fine di meglio regolamentare l’insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione al fenomeno.

Per informare i genitori sulle condotte da adottare a scuola e, in generale, per offrire loro consigli da mettere in pratica con i propri figli, l'Istituto ha

- **elaborato regole sull’uso delle tecnologie digitali** da parte dei genitori nelle comunicazioni con la scuola e con i docenti (es. mail, gruppo whatsapp, sito della scuola ecc.) e li ha informati adeguatamente anche riguardo alle regole per gli studenti e le studentesse;
- **fornito ai genitori consigli o linee guida sull’uso delle tecnologie digitali nella comunicazione** con i figli e in generale in famiglia (a tal fine sul sito web dell'Istituto sono presenti i link a moige.it, al booklet-genitori di moige e alla sezione dedicata ai genitori del sito generazioniconnesse.it).

Il “Patto di corresponsabilità” e il Regolamento Scolastico, integrati con specifici riferimenti alle tecnologie digitali e all’ePolicy, saranno consultabili sul sito dell'Istituto.

Il nostro piano d'azioni

AZIONI (da sviluppare nell’arco dell’anno scolastico 2021/2022)

- 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 consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare e promuovere per il corpo docente incontri formativi sull’utilizzo e l’integrazione delle TIC nella didattica.

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.

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

- 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 del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze 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.

Quali sono i "dati personali"?

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica, 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.

A tal proposito, sono importanti:

- 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 (art. 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 (art. 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.
- dati 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.

Soggetti coinvolti nella "protezione dei dati personali"

- **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).

Cosa si intende per "trattamento dei dati"?

Trattamento è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, ad esempio: la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, la cancellazione, la distruzione, ecc. (art. 4, par. 1, punto 2, del Regolamento (UE) 2016/679).

Chi tratta dati personali altrui deve adottare particolari misure per garantire il corretto e sicuro utilizzo dei dati.

Obblighi della scuola in tema di "protezione dei dati personali"?

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).

La scuola informa (tramite apposita informativa) gli interessati delle caratteristiche e modalità del trattamento dei loro dati, indicando i responsabili del trattamento. Gli interessati non sono solo gli/le studenti/esse, ma anche le famiglie e gli stessi professori. La scuola verifica i loro trattamenti, controllando se i dati siano eccedenti rispetto alle finalità perseguite.

Cosa fa la scuola per essere compliant al Regolamento UE 2016/679:

- Redige e mantiene un registro dei trattamenti dei dati: sia per il titolare che per il responsabile dei trattamenti.
- Valuta i rischi sulla privacy: (definita nel regolamento Data Protection Impact Assessment o PIA) relativamente ad alcune tipologie di trattamento dei 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.
- Analizza il processo di raccolta/gestione del consenso: verifica 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. La formula utilizzata per chiedere il consenso deve essere comprensibile, semplice e chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali, ma devono ad esempio adeguare tutta la modulistica al Regolamento UE 2016/679 e predisporre una lettera di incarico per il trattamento dei dati al personale ATA, ai collaboratori scolastici e ai docenti.

- mette in sicurezza la Intranet scolastica:

  a) interviene sulle reti Wi-fi installate;

  b) utilizza le white list per la navigazione (sistemi di filtraggio dei contenuti);

  c) usa un firewall hardware;

  f) istituire corsi di formazione destinati ai responsabili, agli incaricati ed eventualmente ai sub-incaricati del trattamento.

Quali dati deve contenere la liberatoria?

La scuola non è tenuta a richiedere alle famiglie l'autorizzazione alle riprese fotografiche e video (ad es. in caso di gite scolastiche o recite) solo se esse sono realizzate a fini personali e non a fini di pubblicazione o divulgazione; in caso contrario se è prevista la pubblicazione nel sito web della scuola, ma anche nelle pagine Facebook o tramite whatsapp poiché si tratta di divulgazione è necessaria l'autorizzazione degli interessati.

In generale, il Garante per la protezione dei dati personali stabilisce che “le scuole devono rendere noto alle famiglie e ai ragazzi, attraverso un’adeguata informativa, quali dati raccolgono e come li utilizzano.

La scuola si impegna a far conoscere alle famiglie quali informazioni sono trattate dall’Istituto scolastico e a farle rettificare se inesatte, incomplete o non aggiornate.

I modelli di liberatoria che l’Istituto utilizza in materia di protezione dei dati personali sono disponibili sul sito istituzionale all'indirizzo: www.mattarelladolci.edu.it.

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.

Per garantire l'accesso ad Internet la scuola valuterà:

- lo status quo, cioè la disponibilità attuale di tecnologia e le caratteristiche dell'infrastruttura per renderla sicura, accessibile, ma anche funzionante e adatta allo scopo;
- i bisogni della scuola (o del plesso), in relazione alle reali esigenze didattiche e agli obiettivi prefissati. Questo permetterà di pianificare e di cogliere eventuali occasioni che possono presentarsi sotto forma di bandi, donazioni o finanziamenti.
- le caratteristiche dell'ambiente online: La scuola considera l'ambiente online alla stregua dell'ambiente fisico e ne valuta tutti gli aspetti legati alla sicurezza nel momento in cui permette ai propri studenti e docenti l'accesso alla rete tramite i dispositivi della scuola, tramite la rete scolastica o tramite i dispositivi personali nel caso del BYOD (Bring your own device).In termini di sicurezza la scuola terrà in considerazione sia la safety che la security. Nello specifico, si muoverà sul piano della prevenzione dei rischi (safety), preparando gli utenti ad un uso consapevole delle tecnologie digitali, ma interverrà anche sulla security, cioè sulle risorse tecnologiche che rendono sicuro l'ambiente digitale, dall'antivirus al firewall, da un protocollo di trasmissione dei dati sicuro (https) all'aggiornamento di software e sistemi operativi. In riferimento alla security si presterà attenzione non solo all'infrastruttura hardware e alla rete (wireless e non), ma anche alla sicurezza di tutti gli aspetti che riguardano la gestione degli account degli utenti (in modo differenziato tra studenti, insegnanti e personale amministrativo), il filtraggio dei contenuti (possibilmente in modo differenziato in base all'età) e gli aspetti legali in relazione prevalentemente alla privacy.

Se la tecnologia non funziona: cosa fare?

Per superare la diffidenza nei confronti delle tecnologie a scuola e il divario nell'accesso, è necessario andare oltre la possibile prima barriera che ne inibisce un uso efficace da parte di tanti docenti: i problemi tecnici e la scarsa familiarità con la strumentazione.

La scuola, per affrontare proattivamente la problematica, si impegna:

- a pianificare interventi periodici di manutenzione; inoltre, implementerà un registro delle problematiche incontrate per poter stilare una classifica dei problemi più frequenti. Tutto ciò al fine di permettere agli insegnanti di affrontare e, si spera, risolvere in autonomia tutte quelle situazioni e casistiche di mal funzionamento dei dispositivi che si possono presentare nella

quotidianità;

- a formazione i docenti non solo sull'uso delle tecnologie digitali nella didattica, ma anche sul funzionamento e sull'uso stesso della tecnologia in sé. La parola d'ordine per quanto riguarda le tecnologie è sempre: "Formazione". La formazione dovrebbe anche aiutare a familiarizzare con i dispositivi, laddove ci fossero incertezze e difficoltà

Il regolamento sull'uso delle tecnologie a scuola

Le regole sull'utilizzo della strumentazione tecnologica della scuola, ovvero le azioni che docenti, personale scolastico e studenti/esse possono e non possono compiere quando si connettono alla Rete e/o accedono a un device sono riportate nel regolamento d'istituto, nel patto di corresponsabilità, nel regolamento d'uso degli smartphone a scuola e in modo specifico ed analitico nei regolamento del laboratorio di informatica.

Nei diversi documenti si prevedere la modalità di utilizzo della strumentazione personale a scuola, sia nel caso del BYOD, qualora i docenti proponessero ai propri studenti l'uso di device personali (tablet, PC o smartphone) in classe, ma anche le regole per quanto riguarda la presenza degli smartphone a scuola, non a supporto delle attività didattiche. In particolare stabiliscono:

In generale, i documenti prevedono una parte dedicata all'uso di Internet, in cui gli alunni si impegano a:

- utilizzare la rete in modo corretto
- rispettare le consegne dei docenti
- non scaricare i materiali e i software senza autorizzazione
- non utilizzare unità removibili personali senza autorizzazione
- tenere spento lo smartphone al di fuori delle attività didattiche che ne prevedano l'utilizzo
- di utilizzare lo smartphone esclusivamente per svolgere le attività didattiche previste
- segnalare immediatamente i materiali inadeguati ai propri insegnanti.

I docenti si impegnano a:

- utilizzare la rete nel modo corretto
- non utilizzare 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.

Informazioni sul regolamento sull'uso delle tecnologie a

scuola

La ePolicy verrà condivisa con la comunità scolastica e sul sito Istituzionale.

La scuola si impegna a che gli/le studenti/esse e i loro esercenti la responsabilità genitoriale ne prendano visione. Si impegna altresì a fornire ai genitori informazioni sulla sicurezza in internet a scuola e sull'importanza di un'azione di accompagnamento da parte di adulti competenti rispetto al mondo online, con l'obiettivo di aiutare i discenti a sviluppare le competenze digitali necessarie alla convivenza civile e al loro futuro lavorativo.

Anche il personale scolastico visionerà il regolamento e informato che l'uso di Internet verrà monitorato e segnalato.

Agli insegnanti, inoltre, saranno fornite informazioni concernenti i diritti d'autore.

La scuola chiederà ai genitori degli/lle studenti/esse minori di 16 anni di età il consenso all'uso di Internet da parte dei loro figli e per la pubblicazione dei loro lavori e delle fotografie. Gli/Le studenti/esse che hanno un'età superiore a 16 anni (o maggiorenni), non hanno bisogno del consenso scritto dei genitori. In ogni caso, la scuola può richiedere il consenso genitoriale a tutti i minorenni.

Eventuali commenti o suggerimenti connessi al regolamento potranno essere inviati al Dirigente Scolastico o al responsabile del gruppo di lavoro dell'ePolicy.

Contenuti dannosi e materiali non adatti

L'accesso a Internet è un diritto. Pertanto la scuola adotta tutte le necessarie precauzioni per evitare, all'interno della scuola, l'accesso online da parte di studenti e studentesse a materiali non adatti a loro. Questo attraverso l'adozione di sistemi di filtraggio software e hardware.

Cloud computing e strumenti online

La scuola prevede account personali per l'accesso ai computer e un indirizzo email per gli studenti, oltre che per gli insegnanti. Questo facilita le comunicazioni tra docenti e studenti, abbatte i costi per la scuola, permettendo di accedere a una grande quantità di programmi attraverso Internet, senza bisogno di acquistare e installare programmi localmente. Permette, altresì, un risparmio rispetto alla manutenzione, in quanto il software viene gestito sui server ed è costantemente aggiornato. La scuola, grazie al cloud computing, deve unicamente occuparsi di aggiornare il sistema operativo e il browser. Inoltre, i file salvati sono accessibili agli studenti anche da casa, dove possono proseguire il lavoro iniziato in classe, sotto la guida dell'insegnante. Infine, il cloud non dipende dalla piattaforma, per cui può funzionare con Linux, Windows, Mac e Android.

Rispetto all'uso del cloud o di strumenti di comunicazione online la scuola si doterà di una netiquette.

Norme che la scuola rispetta o si impegna a rispettare per la cybersecurity

- Mantenere separate le reti didattica e segreteria: importante per garantire maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le due reti grazie al firewall.
- Aggiornare periodicamente software e Sistema operativo: garantire che il sistema sia aggiornato lo protegge dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo.
- Definire la programmazione di backup periodici: cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi (possibilmente anche una copia offline).
- Garantire formazione adeguata allo staff, incluso il corpo docenti: la formazione deve riguardare la gestione dei dispositivi, la conoscenza delle regole basilari sulla sicurezza.
- Testare regolarmente le possibili vulnerabilità.
- Preparare piani di azione in risposta ai problemi più seri: è importante non dover improvvisare nel momento in cui si verifica un problema serio, ma avere un protocollo di azione.
- Predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo: se non è previsto uno stand-by, il dispositivo resta accessibile nel caso in cui qualcuno dimentichi di spegnerlo, con il rischio potenziale di accesso da parte di persone non autorizzate.
- Impostare il browser per l'eliminazione dei cookies alla chiusura: in questo modo si evita che qualcuno possa avere accesso ad account altrui senza autorizzazione.
- Definire una policy sulle password (le password devono essere forti):
    - Richiedere password complesse con almeno otto (8) caratteri con numeri, maiuscole e minuscole e caratteri speciali.
    - Sensibilizzare rispetto al non uso di password facilmente identificabili (nomi dei figli, compleanni, etc.).
    - Non memorizzare le password nei dispositivi scolastici.
    - Non condividere le password con nessuno.
- Minimizzare i privilegi amministrativi: solo poche persone autorizzate hanno privilegi amministrativi. Studenti e la maggior parte dei docenti possono accedere con account con permessi limitati.
- Sviluppare il regolamento sull'uso delle tecnologie a scuola (policy di uso accettabile): deve riguardare chiunque abbia accesso alla Rete, studenti/esse, docenti, amministrazione e segreteria, includere i dispositivi della scuola e quelli personali, anche in caso di BYOD.

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.

La sfida, allora, è quella di conoscere al meglio tali strumenti, sfruttarne le potenzialità e come sempre prevenire eventuali rischi correlati ad un uso poco consapevole degli stessi.

Le caratteristiche della comunicazione mediata dalle tecnologie

A tal proposito la scuola fa riferimento agli studi sulla Computer mediated communication per comprendere come la comunicazione online si differenzi sostanzialmente dalla cosiddetta comunicazione face to face e per poter stabilire delle regole. Nello specifico la comunicazione online ha le seguenti caratteristiche:

1. nella comunicazione mediata dalle tecnologie non condividiamo lo stesso spazio e lo stesso contesto comunicativo con i nostri interlocutori. Per questo, talvolta, può accadere che si forniscano cornici interpretative molto diverse ai messaggi e ai contenuti scambiati;
2. essa generalmente non ci permette di accedere ai cosiddetti segnali della comunicazione non verbale (tono della voce, espressione del volto, gesti del corpo, pause…etc.) e non siamo in grado di vedere ed ascoltare direttamente gli effetti della nostra comunicazione sull'interlocutore. Ciò comporta che difficilmente potremo adeguare il nostro comportamento a partire da tali segnali;
3. essa ci rende meno empatici e meno attenti ad emozioni e potenziali reazioni dell'altra persona; non disponiamo infatti del cosiddetto feed-back non tangibile;
4. la comunicazione che viaggia online, generalmente, si avvale di messaggi scritti che possono essere memorizzati, diffusi e permangono nel tempo. È sempre bene tenerlo a mente.
5. gli strumenti di comunicazione online, consenono di 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 (dai ragazzi ai genitori).

Strumenti di comunicazione online che la scuola utilizzare

A tale proposito è importante effettuare una distinzione preliminare fra comunicazione

interna e comunicazione esterna. Diversi strumenti di comunicazione online possono essere utilizzati dalla scuola, sia per raggiungere target esterni, al fine di valorizzare e promuovere le attività portate avanti dall'Istituto (rivolgendosi ad esempio a istituzioni, famiglie, studenti non ancora iscritti, associazioni etc.) sia per far circolare all'interno della scuola informazioni di servizio o contenuti importanti fra i diversi attori scolastici (docenti, studenti, genitori, collaboratori scolastici etc.).

Fra gli strumenti di comunicazione esterna, troviamo in primis il sito web della scuola, i profili sui social network (Facebook, Instagram, Youtube). Tali strumenti, vengono utilizzati anche per fornire informazioni di servizio rivolte a studenti o genitori.

Fra gli strumenti di comunicazione interna, abbiamo le email istituzionali, nella disponibilità sia dei docenti che degli studenti, il registro elettronico con tutte le sue funzionalità, whatsapp, applicativi e piattaforme di lavoro condiviso e collaborativo come Google Docs, Classroom, Drive, ecc utilizzati anche per facilitare e rendere più partecipata la didattica e la comunicazione a scuola.

La scuola utilizza gli strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne nel rispetto del cosiddetto "Diritto alla disconnessione" (art. 22 del CCNL 2016/2018).

Le chat informali fra colleghi, o fra docenti e genitori, non hanno una regolamentazione e per tale ragione è fondamentale, a partire dal buon senso e da una riflessione sulle peculiarità del mezzo, che si elaborino regole condivise sull'uso delle stesse. Fra queste, ad esempio, suggeriamo:

- mettere in chiaro fin dall'inizio, comprendere e rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità;
- usare sempre un linguaggio adeguato e il più possibile chiaro e preciso (come già sottolineato la comunicazione online si presta spesso a non pochi fraintendimenti);
- evitare di affrontare in chat argomenti troppo complessi e controversi (la comunicazione online in una chat di gruppo non è adatta per la gestione di problematiche di questo tipo, che certamente è più opportuno affrontare in presenza o in un Consiglio di classe);
- evitare discussioni di questioni che coinvolgono due o pochi interlocutori, onde evitare di annoiare e disturbare gli altri componenti del gruppo;
- non condividere file multimediali troppo pesanti;
- evitare il più possibile di condividere foto di studenti in chat;
- indirizzare solo domande precise e chiare, a cui si possano dare risposte altrettanto brevi e precise;
- evitare messaggi troppo spezzettati, cercando il più possibile di essere brevi ed esaustivi allo stesso tempo.

Altro strumento centrale nella nostra scuola è il registro elettronico. Esso è utilizzato per la gestione di assenze, presenze, valutazioni, prenotazioni di incontri e

comunicazioni con le famiglie. Queste ultime per mezzo del registro possono visualizzare molte informazioni utili riguardanti:

- andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);
- risultati scolastici (voti, documenti di valutazione);
- udienze (prenotazioni colloqui individuali);
- eventi (agenda eventi);
- comunicazione varie (comunicazioni di classe, comunicazioni personali).

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.

La scuola promuove l'utilizzo delle tecnologie nella didattica nell'ottica di potenziare le competenze di cittadinanza digitale (azione #15 del PNSD scenari innovativi per lo sviluppo di competenze digitali applicate).

La scuola condivide con tutta la comunità il decalogo del MI per l'uso dei dispositivi mobili a scuola, (BYOD) che stabilisce delle regole sulla didattica integrata tramite l'uso dei dispositivi personali in classe e per la sicurezza delle interazioni e delle relazioni fra pari tramite le tecnologie digitali;

La scuola ha integrato/modificato i Regolamenti già esistenti per disciplinare l'utilizzo delle TIC al suo intero e stabilito specifiche procedure per rilevare e gestire le diverse problematiche.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

Scegliere almeno 1 di queste azioni:

- 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 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).

Scegliere almeno 1 di queste azioni:

- 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 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 campagne di **sensibilizzazione** possono avere come obiettivo di mettere in luce una determinata problematica oppure chiedere ad una determinata utenza di attivarsi per una causa.

Gli interventi di sensibilizzazione possono interessare l'intera comunità scolastica

(alunni e famiglie) oppure gruppi più ristretti, come ad esempio alunni di una certa fascia di età.

I benefici di un'attività di sensibilizzazione sono molteplici:

- accrescere la consapevolezza nel gruppo target di riferimento circa un determinato tema/bisogno/problema che potrebbe presentarsi in quel gruppo;
- incoraggiare il gruppo a modificare i propri comportamenti rendendoli più funzionali;
- diffondere all'esterno del gruppo di riferimento e quindi tra l'opinione pubblica una certa consapevolezza rispetto all'argomento di interesse;
- facilitare il coinvolgimento di soggetti esterni in modo da mettere insieme diverse idee per lavorare ad un obiettivo comune.
- favorire la diffusione di informazioni e servizi disponibili all'utilità collettiva (ad esempio, si può pensare ad un intervento di sensibilizzazione per promuovere la conoscenza dell'ePolicy nella comunità scolastica).

Per far sì che un intervento di sensibilizzazione sia efficace, è importante fornire ai beneficiari informazioni chiare su quello che è lo stato attuale del tema che vogliamo trattare, per es.: violazione della riservatezza dei dati, cyberbullismo, adescamento on line, incitamento all'odio. In questo modo gli utenti avranno tutte le informazioni necessarie per avere una fotografia chiara del contenuto che stiamo trattando e del perché è necessario impegnarsi verso un cambiamento.

In sintesi, è opportuno tenere in considerazione i seguenti aspetti:

- spingere le persone a desiderare un cambiamento;
- porre in evidenza la possibilità di generare un cambiamento;
- individuare le azioni che consentono di produrre il cambiamento.

Si potrebbero proporre dei brevi video che contengano informazioni sul tema da trattare oppure racconti di esperienze di ragazzi che hanno subito azioni on line che li hanno danneggiati o semplicemente disturbati.

Parlando di prevenzione in ambito digitale si potrebbe tradurre quanto appena detto con 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.

Se il problema della "sicurezza" è difficilmente riconducibile esclusivamente all'esistenza in sé di alcuni rischi, più o meno gravi e insidiosi, appare chiaro dunque come le migliori strategie di intervento siano di carattere prevalentemente preventivo.

Si può utilizzare la classificazione proposta dall'Institute of Medicine che distingue tre livelli di prevenzione:

1. Prevenzione Universale. Un programma di questo tipo parte dal presupposto che tutti gli studenti siano potenzialmente a rischio. Si tratta quindi di interventi diretti al grande pubblico o a un intero gruppo di una popolazione che non è stato identificato sulla base del rischio individuale.

2. Prevenzione Selettiva. Un programma dedicato ad un gruppo di studenti in cui il rischio online è presente. In questo caso la presenza del rischio è stata individuata tramite precedenti indagini, segnalazioni fatte dalla scuola, oppure dalla conoscenza della presenza di fattori di rischio in quel determinato territorio.

3. Prevenzione Indicata. Un programma di intervento sul caso specifico e quindi pensato e strutturato per adattarsi agli studenti con l'obiettivo di ridurre i comportamenti problematici, oppure dare supporto alle vittime. Per la sua natura questo tipo di intervento si avvale di professionalità diverse perché spesso affronta problemi legati alla salute mentale del minore per cui è opportuno coinvolgere anche la famiglia del/lla ragazzo/a.

Ai fini preventivi la scuola implementa un progetto con le seguenti finalità:

- formare ad un corretto utilizzo di Internet (aspetti relazionali e aspetti sociali);

- informare sui rischi: cyberbullismo, pornografia, pedopornografia, stalking; virus e spam; informare sulle leggi vigenti in fatto di privacy, diritti d'autore, furto di dati personali, furto di denaro; sui siti illegali (che inneggiano all'odio, alla violenza), sui rischi da dipendenza online.

- fornire formazione sui sistemi per prevenire ed evitare i rischi

- collaborare alla raccolta di dati statistici per monitorare l'evoluzione degli stili di utilizzo del web da parte di ragazzi e famiglie;

- aiutare nella costruzione di competenze che possano sostenere un uso consapevole e creativo dei media al fine di coglierne le opportunità e prevenirne gli abusi.

La scuola cerca di dare una risposta il più possibile integrata, collaborando (anche prevedendo accordi specifici) con la rete dei servizi locali (per es. le ASL e la Polizia Postale), con istituzioni e associazioni, oltre che con la famiglia, con la quale ogni anno viene rinnovato il patto educativo.

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).

Nel bullismo tradizionale, solitamente, la vittima che viene presa di mira è percepita come più debole e incapace di difendersi. Mentre nel bullismo tradizionale il potere presenta connotati ben precisi, ad esempio di tipo fisico (legato alla forza o alla statura) o sociale (legato alla popolarità), il potere online può derivare semplicemente dal possesso di specifiche competenze o di alcuni contenuti (immagini, video, confessioni) che potrebbero essere utilizzati per danneggiare la vittima.

Solitamente, quando si parla di cyberbullismo o di bullismo è necessario che vittima e bullo/cyberbullo siano minori o comunque adolescenti (sono esclusi, quindi, dalla definizione episodi di prevaricazione che avvengono fra adulti o fra un adulto e un minore).

Come sottolinea la Willard i tratti specifici del bullismo online sono correlati all'impatto che le tecnologie digitali hanno nella vita dei ragazzi e alle caratteristiche stesse della Rete:

- **L'impatto**: la diffusione di materiale tramite Internet è incontrollabile e non è possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online e continuare a diffondersi). Un contenuto offensivo e denigratorio online può, quindi, diventare virale e distruggere in alcuni casi la reputazione della vittima. Nelle situazioni più gravi, le vittime di cyberbullismo si trovano costrette a dover cambiare scuola o addirittura città, ma questo spesso non le aiuta in quanto la Rete, si sa, è ovunque.

- **La convinzione dell'anonimato**: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile. Sentendosi protetti dall'anonimato ci si sente liberi e più forti nel compiere atti denigratori, senza il timore di essere scoperti. È importante tenere bene a mente, però, che quello dell'anonimato è un "falso mito della Rete". Ogni nostra azione online è, infatti, rintracciabile e riconducibile a noi con gli strumenti opportuni o con l'intervento della Polizia Postale. L'anonimato del cyberbullo, inoltre, è anche uno dei fattori che stanno alla base del forte stress percepito dalla vittima, la quale molte volte non può dare né un nome né un volto al proprio aggressore;

- **L'assenza di confini spaziali:** il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio.

La vittima può essere raggiungibile anche a casa e vive nella costante percezione di non avere vie di fuga. Spegnere il cellulare o il computer non basta, così come cancellare tutti i propri profili social. Il solo pensiero che eventuali contenuti denigratori continuino a diffondersi online è doloroso e si accompagna ad un senso costante di rabbia e impotenza.

- **L'assenza di limiti temporali:** può avvenire a ogni ora del giorno e della notte.

- **L'indebolimento dell'empatia:** esistono cellule chiamate neuroni specchio che ci permettono di "leggere" gli altri quando li abbiamo di fronte, capirli e di provare emozioni simile a quelle che loro provano, proprio come se fossimo di fronte ad uno specchio. Tale sensazione è data dall'attivazione di una particolare area del cervello. Quando le interazioni avvengono prevalentemente online la funzione speciale di questi neuroni viene meno (mancando la presenza fondamentale dell'altro che è sostituito dal dispositivo). La riduzione di empatia che ne consegue può degenerare nei comportamenti noti messi in atto dai cyberbulli.

- **Il feedback non tangibile:** il cyberbullo non vede in modo diretto le reazioni della vittima e, ancora una volta, ciò riduce fortemente l'empatia e il riconoscimento del danno provocato.

Per questo non è mai totalmente consapevole delle conseguenze delle proprie azioni. L'impossibilità di vedere con i propri occhi l'eventuale sofferenza e umiliazione provata dalla vittima fa sì che il tutto venga percepito come "uno scherzo" divertente a cui partecipare, di cui ridere o a cui essere indifferenti. Inoltre, il cyberbullismo non lascia segni fisici evidenti sulla vittima e si consuma in un contesto virtuale che spesso viene percepito dai ragazzi come non "reale", come un mondo ludico a sé stante.

A ciò si aggiungono altre convinzioni o tendenze frequenti nell'uso della Rete sia da parte dei giovani che degli adulti:

- Percezione che online non ci siano norme sociali da rispettare: fra i giovani spesso vige la falsa convinzione secondo cui la Rete sia uno spazio virtuale lontano dalla realtà, in cui vige libertà assoluta e in cui regole e norme sociali della vita quotidiana non valgono;

- La sperimentazione online di identità e personalità multiple: la Rete è per i minori il luogo virtuale per eccellenza in cui mettersi in gioco "fingendo di essere ciò che non si è" per il semplice gusto di sperimentare nuove forme di identità e comportamento;

- Il contesto virtuale come un luogo di simulazione e giochi di ruolo: “la vita sullo schermo” e tutti i comportamenti messi in atto online vengono percepiti solo come un gioco.

- Diffusione di responsabilità: tutti quelli che partecipano anche solo con un like o un commento diventano, di fatto, corresponsabili delle azioni del cyberbullo facendo accrescere la portata dell’azione; mettere un “like” su un social network, commentare o condividere una foto o un video che prende di mira qualcuno o semplicemente tacere pur sapendo, mette ragazzi e ragazze nella condizione di avere una responsabilità.

È possibile suddividere gli atti di cyberbullismo in due grandi gruppi:

1. cyberbullismo diretto: il bullo utilizza strumenti di messaggistica istantanea che hanno un effetto immediato sulla vittima, poiché diretti esclusivamente a lei.

2. cyberbullismo indiretto: il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico.

Come riconoscere casi di cyberbullismo?

Alcuni segnali generali che può manifestare la potenziale vittima di cyberbullismo possono essere i seguenti; la vittima:

- Appare nervosa quando riceve un messaggio o una notifica;

- Sembra a disagio nell’andare a scuola o finge di essere malata (ha spesso mal di stomaco o mal di testa);

- Cambia comportamento ed atteggiamento in modo repentino;

- Mostra ritrosia nel dare informazioni su ciò che fa online;

- Soprattutto dopo essere stata online, mostra rabbia o si sente depressa;

- Inizia ad utilizzare sempre meno Pc e telefono (arrivando ad evitarli);

- Perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;

- Il suo rendimento scolastico peggiora.

Chi compie atti di bullismo e cyberbullismo può anche essere responsabile di reati penali e danni civili.

L'atto di bullismo può violare sia la legge penale, sia quella civile, quindi può dar vita a due processi, l'uno penale e l'altro civile.

Le responsabilità per atti di bullismo e cyberbullismo compiute dal minorenne possono ricadere anche su:

- i genitori: devono educare adeguatamente e vigilare, in maniera adeguata all'età del figlio, cercando di correggerne comportamenti devianti. Questa responsabilità generale persiste anche per gli atti compiuti nei tempi di affidamento alla scuola (culpa in educando).

- gli insegnanti e la scuola: nei periodi in cui il minore viene affidato all'Istituzione scolastica il docente è responsabile della vigilanza sulle sue azioni e ha il dovere di impedire comportamenti dannosi verso gli altri/e ragazzi/e, insegnanti e personale scolastico o verso le strutture della scuola stessa. A pagare in primis sarà la scuola, che poi potrà rivalersi sul singolo insegnante. La responsabilità si estende anche a viaggi, gite scolastiche, manifestazioni sportive organizzate dalla scuola (culpa in vigilando).

- esiste poi una culpa in organizzando, che si ha quando la scuola non mette in atto le azioni previste per la prevenzione del fenomeno o per affrontarlo al meglio (così come previsto anche dalla normativa vigente).

Gli insegnanti potranno essere chiamati a rispondere personalmente solo in caso di azione di rivalsa per dolo o colpa grave, da parte dell'amministrazione. L'insegnante ha un dovere di vigilanza e di conseguenza viene addebitata, in caso di comportamento illecito del minore affidato, una colpa presunta, cioè una "culpa in vigilando", come inadempimento dell'obbligo di sorveglianza sugli allievi. Di questa colpa/responsabilità si può essere liberati dimostrando di non aver potuto impedire il fatto. Si tiene conto in questi casi dell'età e del grado di maturità dei ragazzi, della concreta situazione ambientale, etc. Inoltre, l'insegnante deve dimostrare di aver adottato in via preventiva le misure idonee ad evitare la situazione di pericolo.

L'insegnante è responsabile per tutto il tempo dell'affidamento dell'alunno alla scuola. Quindi, non soltanto le ore delle attività didattiche, ma anche tutti gli altri momenti della vita scolastica, compresa la ricreazione, la pausa pranzo, la palestra, le uscite e i viaggi di istruzione etc.

Come previsto dalla Legge 71/2017 e dalle relative "Linee di orientamento per la

prevenzione e il contrasto del cyberbullismo", che indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo, la scuola dovrà occuparsi di:

- 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;

  La scuola ha già dei referenti per le iniziative di prevenzione e contrasto che:

- hanno il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, si avvalgono della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
- Svolgono un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

  Salvo che il fatto costituisca reato, il Dirigente Scolastico qualora venga a conoscenza di atti di cyberbullismo deve informare tempestivamente i genitori dei minori coinvolti (art.5).

Alcune indicazioni operative da tenere presenti sono le seguenti:

- per intervenire efficacemente è necessario capire se si tratta effettivamente di cyberbullismo o di altra tipologia di comportamenti violenti o disfunzionali. Oltre al contesto, altri elementi utili ad effettuare questa valutazione sono le modalità in cui avvengono (alla presenza di un "pubblico"? Tra coetanei? In modo cronico e intenzionale? etc.) e l'età dei protagonisti.
- valutare circa l'eventuale stato di disagio vissuto dalle persone minorenne/i

coinvolte, per cui potrebbe essere necessario rivolgersi ad un servizio deputato ad offrire un supporto psicologico o di mediazione. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza (ad esempio: spazio adolescenti, se presente, del Consultorio Familiare, servizi di Neuropsichiatria Infantile, centri specializzati sulla valutazione o l'intervento sul bullismo o in generale sul disagio giovanile, i comportamenti a rischio in adolescenza, etc.).

- 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. Il Garante ha pubblicato nel proprio sito il modello per la segnalazione/reclamo in materia di cyberbullismo da inviare a: cyberbullismo@gpdp.it.

- Parallelamente, nel caso in cui si ipotizzi che ci si possa trovare di fronte ad una fattispecie di reato (come, ad esempio, il furto di identità o la persistenza di una condotta persecutoria che mette seriamente a rischio il benessere psicofisico del bambino o adolescente coinvolto in qualità di vittima) si potrà far riferimento agli uffici preposti delle Forze di Polizia per inoltrare la segnalazione o denuncia/querela e permettere alle autorità competenti l'approfondimento della situazione da un punto di vista investigativo. È in tal senso possibile far riferimento a queste tipologie di uffici:

  Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato – Commissariato on line (attraverso il portale http:// www.commissariatodips.it).

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.

Le principali caratteristiche dell’hate speech possono essere riassunte così:

- Il discorso d’odio procura sofferenza. La parola ferisce, e a maggior ragione l’odio! Il discorso può violare i diritti umani. Il discorso d’odio online non è meno grave della sua espressione offline, ma è più difficile da individuare e da combattere.

- Gli atteggiamenti alimentano gli atti. Il discorso dell’odio è pericoloso anche perché può condurre a più gravi violazioni dei diritti umani, e perfino alla violenza fisica. Può contribuire a inasprire le tensioni razziali e altre forme di discriminazione e di violenza.

- L’odio online non è solo espresso a parole. Internet ci permette di comunicare rapidamente e in modi svariati, ad esempio mediante i social media e i giochi online, molto spesso in maniera anonima. L’odio online può esprimersi sotto forma di video e foto, come pure, più solitamente, di contenuto testuale. Le forme visive o multimediali hanno sovente un impatto più forte sugli atteggiamenti consci e inconsci.

- L’odio prende di mira sia gli individui che i gruppi. L’odio online può prendere di mira dei gruppi che spesso sono già vulnerabili sotto altri aspetti, come i richiedenti asilo, le minoranze religiose o le persone con disabilità. Tuttavia, anche i singoli individui sono sempre maggiormente oggetto di attacchi. Le conseguenze sono talvolta fatali, come dimostrato da numerosi fatti di cronaca riferiti dai media, riguardanti giovani vittime di cyberbullismo che sono state spinte al suicidio.

- Internet è difficilmente controllabile. La diffusione di messaggi di incitamento all'odio è maggiormente tollerata su Internet rispetto al mondo offline ed è sottoposta a minori controlli. È ugualmente più facile (e comporta meno rischi) insultare o molestare online, perché le persone spesso si esprimono sotto la copertura dell'anonimato.

- Ha radici profonde. Gli atteggiamenti e le tensioni sociali che suscitano sentimenti di odio online affondano le loro radici nella società, e non sono diversi, in genere, da quelli che alimentano il discorso dell'odio offline.

- Impunità e anonimato. Sono le due presunte caratteristiche delle interazioni sociali in rete che abbassano le remore etiche. In realtà, però, qualsiasi azione compiuta sul web consente di rintracciare il suo autore.

È utile prendere in considerazione alcuni aspetti dell'hate speech:

Il contenuto e il tono

Certe espressioni di odio sono più estreme, utilizzano termini più insultanti e possono perfino istigare altri ad agire. All'altra estremità della scala, troviamo insulti più moderati o generalizzazioni eccessive, che presentano certi gruppi o individui sotto una cattiva (e perfino sotto falsa) luce.

I bersagli potenziali

Alcuni gruppi, o individui, possono essere più vulnerabili di altri alle critiche. Può dipendere dal modo in cui sono globalmente considerati nella società, o da come sono rappresentati nei media, oppure dalla loro situazione personale, che non permette loro di difendersi efficacemente. La stessa espressione, applicata a gruppi diversi, può avere un impatto molto diverso.

Il contesto

Il contesto di una particolare espressione di odio è legato talvolta a circostanze storiche e culturali specifiche. Può includere altri fattori, come il mezzo utilizzato e il gruppo preso di mira, le tensioni o i pregiudizi esistenti, l'autorità del suo autore, etc.

L'impatto o l'impatto potenziale

L'impatto reale o potenziale esercitato sugli individui, sui gruppi o sull'insieme della società è una delle principali considerazioni da tenere presenti. Spesso, le ripercussioni negative subite dall'individuo o dal gruppo si rivelano più importanti della valutazione dell'episodio da parte di osservatori esterni.

L'intervento che la scuola propone per fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, e

promuovere la partecipazione civica e l'impegno, si basa su attività di analisi e produzione mediale, finalizzate soprattutto a:

- 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;
- realizzare contenuti multimediali sul contrasto ai messaggi violenti e discriminatori presenti sulla rete;
- far acquisire agli studenti la competenza di presentare se stessi attraverso profili che non diano possibilità di fraintendimenti, prestando attenzione ai post che poi vengono condivisi da un canale all'altro;
- far acquisire e/o migliorare la capacità dei ragazzi di entrare in relazione con gli altri, apprezzando e rispettando le altrui differenze, ignorando le offese invece di ribattere subito parola su parola e valutando quando sia il caso di rispondere..

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?

La dipendenza da Internet, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica che deve attenzionare il fenomeno e fornire gli strumenti agli studenti e alle studentesse

affinché questi siano consapevoli dei rischi che comporta l'iperconnessione.

La scuola ha la possibilità di fare formazione e di indicare strategie per un uso più consapevole delle tecnologie per favorire il "benessere digitale", cioè la capacità di creare e mantenere una relazione sana con la tecnologia.

Gli elementi che contribuiscono al benessere digitale sono:

- la ricerca di equilibrio nelle relazioni anche online
- l'uso degli strumenti digitali per il raggiungimento di obiettivi personali
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile
- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche)

Questo è un argomento trasversale, se ne può parlare quando si parla di cittadinanza digitale, di cyberbullismo, di uso integrativo e non sostitutivo dei dispositivi e della Rete; tanto più può essere utile dedicare al tema un momento specifico e riflettere con studenti e studentesse per fare in modo che la tecnologia sia strumento per raggiungere i propri obiettivi e non sia solo distrazione o addirittura ostacolo.

La scuola si propone di integrare la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online; la scuola promuove riflessioni su che ruolo ha e deve avere la tecnologia (internet o il gioco) nella propria vita, chiedendosi quando la tecnologia è un valore aggiunto.

Si rende necessario strutturare regole condivise e stipulare con gli alunni una sorta di "patto" d'aula, proponendo delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d'aula

È importante non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli studenti e delle studentesse, stabilendo chiare e semplici regole di utilizzo.

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.

I contenuti sessualmente espliciti possono diventare materiale di ricatto assumendo la forma di “revenge porn” letteralmente “vendetta porno”, fenomeno quest’ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l’altra parte (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).

La diffusione di contenuti personali si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo o la ragazza soggetto della foto/del video sia colui/coloro che hanno contribuito a diffonderla generando ripercussioni negative sulla vittima in termini di autostima, di credibilità, di reputazione sociale off e on line.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia negli altri e depressione.

La scuola intende sensibilizzare genitori e alunni contro la diffusione del sexting, per esempio attraverso un manifesto in cui si riportino consigli contro questa forma di bullismo e riferimenti (mail, telefono, etc.) di associazioni, centri di ascolto e istituzioni a cui rivolgersi nei casi in cui ci si ritenga vittima di sexting.

Alcuni consigli da riportare potrebbero essere i seguenti:

- Verificare periodicamente le impostazioni di privacy dei propri account e sui social network
- cambiare periodicamente le password e non condividerle mai, neanche con amici fidati
- non dare l'amicizia sui social a persone sconosciute, anche se risultano amici di amici
- non lasciare incustodito lo smartphone
- non condividere foto e video che potrebbero essere usati impropriamente da altri

- non usare il proprio nome e cognome e non scrivere i propri dati personali in chat o su messaggerie (numero di telefono, indirizzo, codice fiscale, email ecc.)
- fare uno screenshot dei post o messaggi offensivi
- copiare il link completo del profilo di chi utilizza impropriamente un'immagine, perché per una denuncia non basta il nome
- non rispondere ai messaggi di persone sconosciute e non rispondere a messaggi provocatori
- bloccare gli account che mandano post sgradevoli
- segnalare immediatamente al gestore del sito la diffusione di un contenuto privato senza il proprio consenso.

Un successivo momento di contrasto al sexting potrebbe essere l'organizzazione di incontri tra le famiglie e psicologi o persone con esperienza sulla tematica citata.

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 miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e, perché no, della sessualità.

La scuola ritiene di fondamentale importanza l'attivazione di un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy, la gestione dell'immagine e dell'identità online e la capacità di gestire adeguatamente le proprie relazioni online (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è).

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.

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.

Risulta utilissima l'attività educativa sull'affettività e le relazioni, sottolineando sempre la necessità di rivolgersi ad un adulto quando qualcosa online mette a disagio. I più giovani devono acquisire quelle competenze in grado di orientarli e guidarli nelle loro scelte anche online; per questo motivo l'educazione, compresa l'educazione all'affettività, riveste un ruolo fondamentale.

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.

La scuola intende porre in essere un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico attraverso progetti specifici di prevenzione dell'abuso sessuale realizzati da persone esperte; inoltre, potrà programmare attività da realizzare in classe per avviare una prevenzione efficace, con l'obiettivo primario di rafforzare i fattori protettivi e facilitare l'acquisizione e il mantenimento di competenze sociali e

benessere emozionale, in un clima sereno e cooperativo, basato sul rispetto reciproco, offrendo sostegno in particolare agli alunni che manifestano un disagio.

Se si ravvisa un rischio per il benessere psicofisico dei ragazzi, 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, centri specializzati sull'abuso e il maltrattamento dei minori, etc.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022).

□ Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

□ 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.

□ Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

□ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

□ Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

□ Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

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

□ Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

☐ 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.

☐ 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.

☐ Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

☐ Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.

☐ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

☐ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

☐ Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

☐ Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

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.

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.

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.

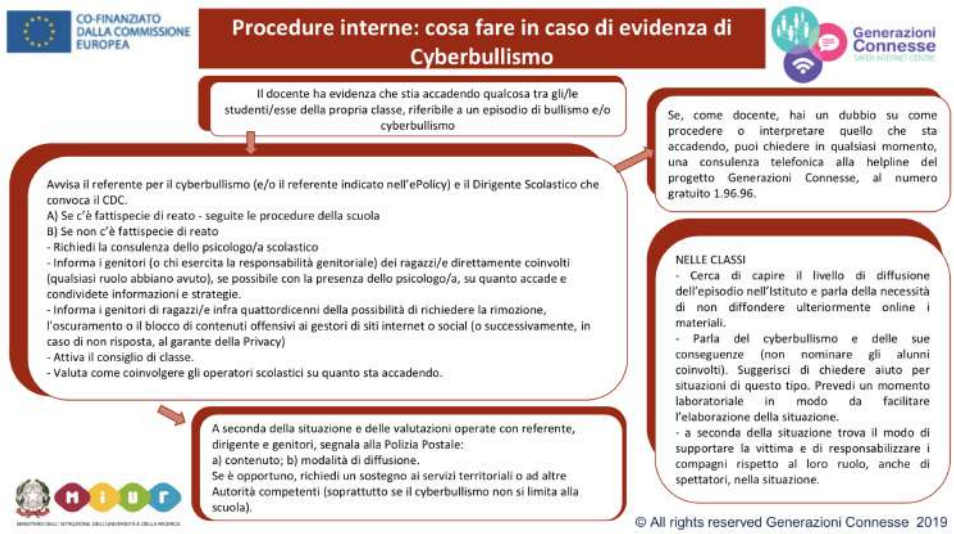
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **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.

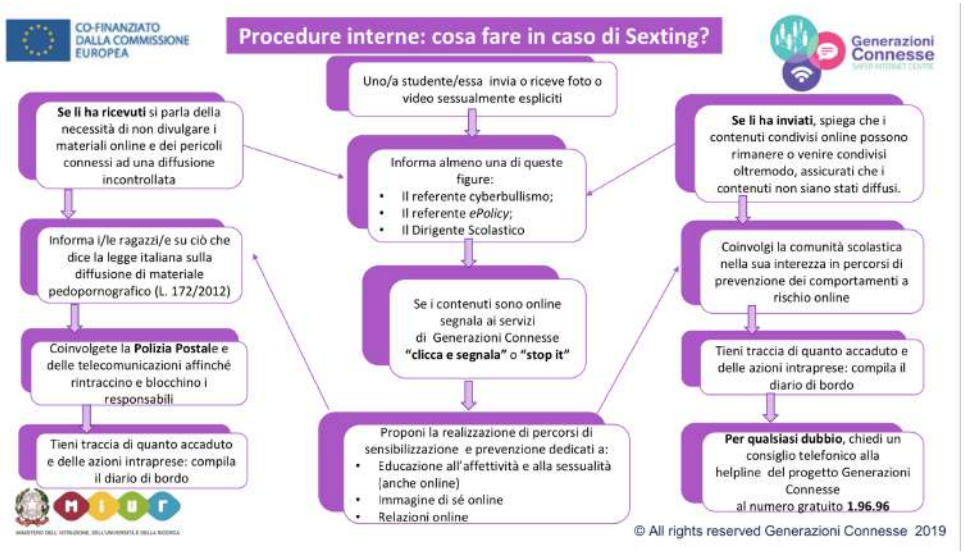
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

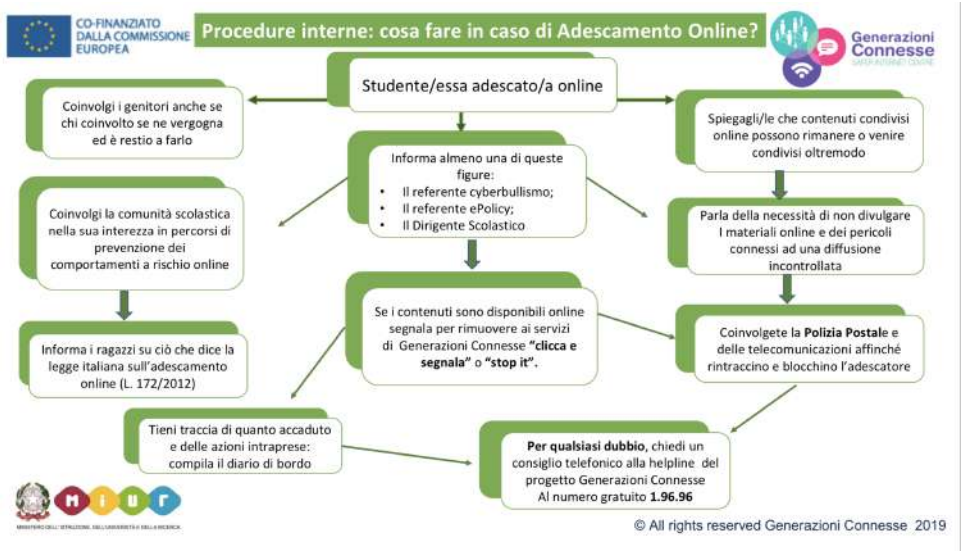
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



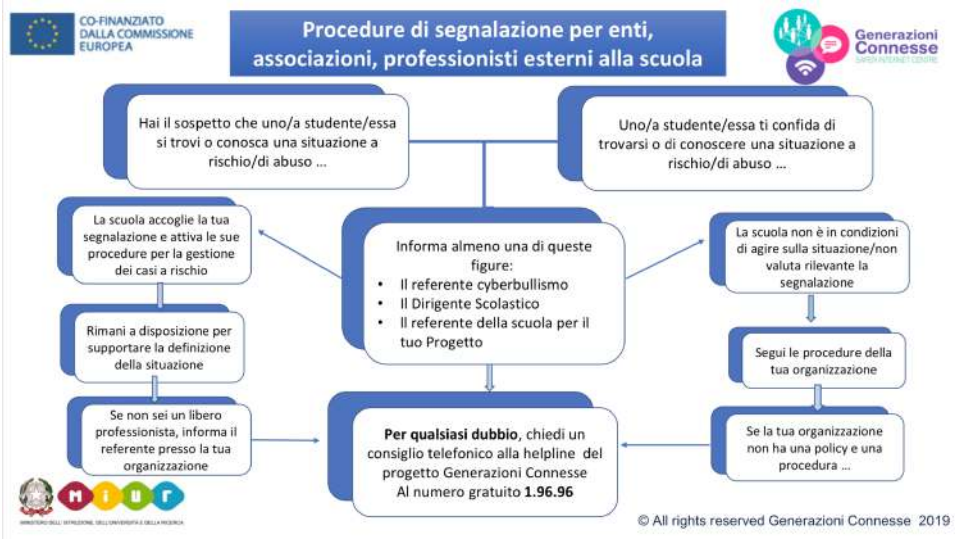
Procedure interne: cosa fare in caso di sexting?



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

Rendere edotta la comunità scolastica in merito a cosa deve segnalare, agli strumenti e alle procedure cui fare riferimento.