Documento di ePolicy

TOIC8BD00X

I.C. ILARIA ALPI

CORSO NOVARA 26 - 10152 - TORINO - TORINO (TO)

AURELIA PROVENZA

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.

Il nostro istituto ha manifestato in questi anni la volontà di sperimentare l'utilizzo delle nuove tecnologie nella didattica, ottenendo in molti casi diversi benefici nei processi di insegnamento/apprendimento.
Per contro, la diffusione delle nuove tecnologie e dei nuovi sistemi di apprendimento richiede sempre più una riflessione e un approfondimento in merito alle nostre responsabilità educative, in termini di consapevolezza e sicurezza.
È nata pertanto la necessità di dotare l'istituto di un documento E-POLICY, ossia un documento programmatico volto a regolamentare all'interno dello stesso le tematiche legate all'uso delle TIC.

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.

Nell' ambito dell'E-policy sono individuati i seguenti ruoli e le principali responsabilità correlate:

Il Dirigente Scolastico
• è garante della sicurezza, anche online, di tutti i membri della comunità scolastica;
• promuove la cultura della sicurezza online attivando, con la collaborazione del Referente di Istituto per il bullismo/cyberbullismo, percorsi di formazione per la sicurezza e le problematiche connesse all'utilizzo della RETE sia online che offline;
• garantisce l'esistenza di un sistema/protocollo per il monitoraggio e il controllo interno della sicurezza online;
• gestisce e interviene nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

Il Direttore dei Servizi Generali e Amministrativi
• assicura, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta

a uso improprio o a dannosi attacchi esterni;
• garantisce il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet;
• assicura la riservatezza dei dati personali trattati ai sensi della normativa vigente.

L' Animatore digitale
• con i componenti del team per l'innovazione 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 promotore di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale";
• coinvolge la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale";
• dovrebbe inoltre, monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e avere il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti.

Il Referente bullismo e cyberbullismo
• ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, si avvale della collaborazione delle Forze di Polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Fondamentale, dunque, il suo ruolo non solo in ambito scolastico ma anche in quello extra-scolastico, in quanto (ove possibile) può coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

Il Personale Docente e ogni figura educativa in affiancamento
• si informano e si aggiornano sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
• garantiscono che le modalità di utilizzo corretto e sicuro delle TIC e della Rete siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
• sviluppano le competenze digitali degli allievi facendo sì che gli stessi conoscano e seguano le norme di sicurezza nell'utilizzo del web sia per attività in presenza sia per attività didattiche extracurricolari; nelle lezioni in cui è programmato l'utilizzo della Rete, guidano gli alunni a siti controllati e verificati come adatti per il loro uso e controllano che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
• assicurano che gli studenti abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete, ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
• garantiscono che le comunicazioni digitali dei docenti con studenti e genitori siano

svolte nel rispetto del codice di comportamento professionale ed effettuate attraverso i canali scolastici ufficiali;
• assicurano la riservatezza dei dati personali trattati ai sensi della normativa vigente;
• comunicano ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
• segnalano qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informatico all'Animatore digitale e al team per l'innovazione digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
• segnalano al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli studenti in relazione all'utilizzo delle tecnologie digitali o della rete, per l'adozione delle procedure previste dalle norme.

Il Personale ATA.
• ha un'adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e le relative buone pratiche;
• segnala qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'animatore digitale;
• mantiene tutte le comunicazioni digitali con studenti e genitori/tutori a livello professionale e le realizza esclusivamente attraverso i canali scolastici ufficiali.

Gli studenti e le studentesse.
• devono essere responsabili, in relazione al proprio grado di maturità e di apprendimento, nell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
• prendono coscienza delle potenzialità offerte dalle Tecnologie dell'Informazione e della Comunicazione (TIC) per la ricerca di contenuti e materiali, ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
• comprendono l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;
• partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e si fanno promotori di quanto appreso anche attraverso percorsi di peer education.
• adottano condotte rispettose degli altri anche quando si comunica in rete;
• esprimono domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

I genitori
• sostengono la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;
• partecipano alle iniziative di sensibilizzazione e formazione organizzate dall'Istituto

sull'uso consapevole delle TIC e della RETE, nonchè sull'uso responsabile dei device personali; condividono con i docenti le linee educative relative alle TIC e alla RETE, al Regolamento di Istituto e al patto di corresponsabilità educativa;
• seguono gli studenti nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet;
• concordano con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet;
• fissano delle regole per l'utilizzo del computer e tengono sotto controllo l'uso che i figli fanno di internet e del telefonino in generale;
• fanno un uso appropriato delle immagini e dei video digitali acquisiti in occasione di eventi scolastici, anche al di fuori delle aule;
• fanno un uso appropriato dell'accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico.

Gli Enti educativi esterni e le associazioni.
• si conformano alla politica della scuola riguardo all'uso consapevole della Rete e delle TIC;
• inoltre, promuovono comportamenti sicuri online e garantiscono la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

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

1.3 - 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).

Per questo motivo è importante la predisposizione di un'informativa sintetica sull'ePolicy sottoscritta e condivisa anche da eventuali soggetti esterni che chiarisca anche le modalità di segnalazione in caso di episodi che mettano in pericolo la sicurezza degli studenti e delle studentesse.

I soggetti esterni che sono responsabili di iniziative educative e formative nell'Istituto dunque

- prendono visione della politica dell'Istituto riguardo all'uso consapevole e responsabile della rete e delle TIC
- promuovono la sicurezza on-line durante le attività di cui sono titolari
- segnalano ai docenti preposti e al Dirigente Scolastico eventuali comportamenti problematici o casi di abuso nell'uso della rete e delle TIC.

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.

Riguardo a ciò è necessario ricordare che:

rendere partecipi gli alunni del contenuto dell'ePolicy permette di svolgere un'azione educante nei loro confronti volta a far comprendere loro le corrette modalità di utilizzo della tecnologia sia all'interno che all'esterno della scuola anche per riconoscere e prevenire comportamenti a rischio.

condividere il documento con tutto il personale scolastico permette di sensibilizzarlo sia sui rischi delle azioni online ma anche sulle grandi possibilità didattiche ed educative delle TIC.

la condivisione attraverso i canali ufficiali della scuola (sito, incontri, scuola famiglia, etc….) del documento ai genitori è fondamentale per rendere veramente organica l'azione di tutta la comunica educante.

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.

Le infrazioni alla policy possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori a docenti/ATA, alla dirigenza.
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 caso in cui una violazione al regolamento di istituto si configuri come atto di bullismo/cyberbullismo o più in generale come infrazione all'ePolicy d'istituto, colui che ne viene a conoscenza informa tempestivamente il Dirigente Scolastico e il referente per il bullismo/cyberbullismo.
Qualora tali infrazioni dovessero configurarsi come reato, il Dirigente Scolastico farà una tempestiva segnalazione all'autorità competente, fatto obbligo di denuncia.
Verrà valutata la gravità delle violazioni in base alla quale saranno attivate azioni

educative e, all'occorrenza, allertati i servizi predisposti (Servizi sociali, Polizia postale, Nucleo di prossimità, supporto psicologico).

Disciplina degli studenti e delle studentesse.

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

● utilizzo non autorizzato di device personali (quali smartphone, tablet) durante l'attività scolastica (lezioni, intervallo, mensa);

● uso della RETE per giudicare, infastidire, offendere, denigrare, impedire a qualcuno di esprimersi o partecipare, esprimendosi in modo volgare usando il turpiloquio;

● invio incauto o senza permesso di foto o altri dati personali (indirizzo di casa, numero di telefono);

● condivisione online di immagini o video di compagni/e e del personale scolastico senza il loro esplicito consenso o che li ritraggono in pose offensive e denigratorie;

● condivisione di immagini intime e a sfondo sessuale;

● invio di immagini o video volti all'esclusione di compagni/e, comunicazione incauta e senza permesso con sconosciuti, collegamenti a siti web non adeguati e non indicati dai docenti.

L'azione educativa prevista per gli alunni è rapportata alla fascia di età e al livello di sviluppo e maturazione personale. In alcuni casi, infatti, i comportamenti sanzionabili sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, di cui gli educatori devono tenere conto per il raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno.

Sono previsti, pertanto, interventi graduali in base all'età e alla gravità delle violazioni:

- richiamo verbale
- richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante)
- richiamo scritto con annotazione sul diario e sul registro
- convocazione dei genitori da parte dell'insegnante
- convocazione dei genitori da parte del Dirigente Scolastico.

Contestualmente sono previsti interventi educativi di rinforzo rispetto a comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza, di prevenzione e gestione positiva dei conflitti, di pro-socialità, di conoscenza e gestione delle emozioni.

È inoltre importante intervenire su tutto il contesto classe con attività specifiche educative e di sensibilizzazione.

Disciplina del personale scolastico.

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

- utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di docenza o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiale non idoneo;
- utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- trattamento dei dati personali e dei dati sensibili degli alunni non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi

-

diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi, carente istruzione preventiva degli alunni sull'uso corretto e responsabile delle TIC e di internet.

- vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili rischi connessi;
- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.
- al personale ATA, fatti salvi i momenti di pausa, non è consentito in alcun modo l'uso di strumenti tecnologici personali (pc portatili, tablet, smartphone, e-reader, cellulari...). L'uso improprio verrà sanzionato in base alla normativa vigente.

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

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

Disciplina dei genitori.

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

Gli atteggiamenti da parte della famiglia meno favorevoli sono:

- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non corre rischi;
- una posizione del computer in una stanza o in una posizione non visibile e controllabile dall'adulto;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'uso di cellulare o smartphone;

- un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei a minori;
- un utilizzo di cellulari e smartphone in comune con gli adulti che possono conservare in memoria indirizzi di siti o contenuti non idonei a minori;
- I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sè e/o dannosi per altri (culpa in educando e in vigilando).

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.

Il gruppo di lavoro del presente documento, il Team digitale ed il Dirigente si impegnano a verificare l'integrazione tra i documenti prima citati, proponendo eventuali modifiche al Collegio Docenti.

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.

Il gruppo di lavoro del presente documento, il Team digitale ed il Dirigente si impegnano ad aggiornare se necessario il presente documento, proponendo eventuali modifiche al Collegio Docenti

---

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- conoscere e utilizzare le risorse di Generazioni Connesse
- organizzare 1 evento di presentazione e conoscenza dell'e-Policy rivolto ai docenti (Collegio docenti unitario)

Azioni da svolgere nei prossimi 3 anni:

- organizzare un'attività volta all'aggiornamento dell'e-Policy con i docenti
- sensibilizzare gli studenti/studentesse e sui temi dell'e-Policy

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 ha predisposto la creazione di "Un curricolo verticale per lo sviluppo delle competenze nella scuola dell'infanzia, nella scuola primaria e secondaria di I grado", nel quale si fa riferimento ad una delle competenze chiave europee, la "competenza digitale", per permettere agli alunni di maturare le conoscenze, le abilità e le attitudini necessarie a utilizzare il web e le tecnologie digitali con dimestichezza e creatività, dimostrando il ruolo fondamentale che essi possono avere nel processo di apprendimento di ogni studente ed ogni studentessa. Il curricolo si proporrà di rispettare le indicazioni contenute nel PNSD, nel DigComp 2.1, nel Sillabario sull'Educazione Civica Digitale e sulla "Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente" per individuare le competenze digitale da attenzionare maggiormente e chiarirne i descrittori, i livelli di padronanza e le modalità valutative. Inoltre, particolare rilevanza verrà data al tema della cittadinanza digitale nella creazione delle UDA di Educazione Civica, come da indicazioni del PTOF e delle linee guida ministeriali.

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.

Le TIC sono utilizzate regolarmente dagli insegnanti ad integrazione della didattica al fine di progettare, sviluppare, utilizzare, gestire e valutare i processi di insegnamento e apprendimento di tutti gli studenti e le studentesse della classe, in un'ottica inclusiva.

Il corpo docente ha partecipato e partecipa a corsi di formazione, nello specifico:

● formazione istituzionale, organizzata dal Missione Istruzione secondo il PNSD (Piano nazionale scuola digitale) e nell'ambito delle azioni del Piano nazionale di ripresa e resilienza (PNRR), attraverso gli snodi formativi.
● proseguimento della formazione specifica di Istituto, legata alle esigenze formative rilevate dall' animatore Digitale, dal team per l'innovazione digitale e dai referenti alla formazione.
● attraverso le azioni a carattere formativo realizzate nell'ambito della programmazione della V rete di scuole Riconnessioni.

● aderisce alle iniziative formative proposte dalla piattaforma Scuola Futura rivolte al personale scolastico (docenti, ATA, DSGA DS), nell'ambito delle azioni del Piano Nazionale di ripresa e resilienza (PNRR), Missione Istruzione.

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.

Al fine di promuovere la condivisione di buone pratiche per un uso consapevole sicuro delle TIC, e di prevenire e contrastare ogni forma di bullismo, anche informatico (Legge 107 /2015, e Legge 71 del 29 maggio 2017), l'Istituto ha aderito al Progetto "Generazioni Connesse" in parternariato con il Ministero dell'Interno - Polizia Postale e delle Comunicazioni e con altre importanti associazioni per la tutela dei diritti dei minori, come Children Italia e Telefono Azzurro. Altre azioni in campo didattico, informativo e formativo e destinate a studentesse e studenti, al personale tutto dell'Istituto, alle famiglie vengono di volta in volta valutate, proposte e realizzate su indicazioni del referente per il contrasto al bullismo/cyberbullismo e sul fabbisogno dell'Istituto stesso.

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.

L'Istituto intraprende con regolarità azioni di sensibilizzazione delle famiglie sul tema dell'utilizzo consapevole delle nuove tecnologie. L'istituto darà ampia diffusione, tramite pubblicazione sul sito, del presente documento e-Policy, per consentire alle famiglie una piena conoscenza del Regolamento e dell'utilizzo delle nuove tecnologie all'interno dell'Istituto, favorendo un'attiva collaborazione tra la scuola e le famiglie sul tema della prevenzione dei rischi connessi ad un uso inappropriato del digitale.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024)

- 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.

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

- Effettuare annualmente, con uno strumento di auto-valutazione online (SELFIE), una "fotografia" delle pratiche d'uso (NON le tecnologie!) e le strategie digitali della scuola per catturare lo stato attuale e pianificare azioni future del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- 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.

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 nostra Istituzione scolastica si impegna a trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali, oppure quelli espressamente previsti dalla normativa di settore. Alcune categorie di dati personali degli/lle studenti/esse e delle famiglie, come quelli sensibili e giudiziari, saranno 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.

La scuola informerà (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 docenti. È importante, inoltre, che le scuole verifichino i loro trattamenti, controllando se i dati siano eccedenti rispetto alle finalità perseguite.

La scuola ha altresì adottato una piattaforma di servizi e tools in cloud (PrivacyLab GDPR) che permettono di gestire gli adempimenti previsti dal Reg. Europeo sulla protezione dei Dati Personali.

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.

La scuola si impegna nell' acquisizione, gestione e mantenimento delle infrastrutture e dei device necessari allo scopo. L'accesso ad Internet, a scuola, avviene considerando la prevenzione dei rischi in rete, in termini di uso consapevole delle tecnologie digitali e mediante i protocolli di sicurezza che rendono accessibile l'ambiente digitale, dall'antivirus ai firewall, all'aggiornamento di software e sistemi operativi.

Per garantire la sicurezza online, sarà necessario:

- Mantenere separate le reti didattica e segreteria;
- Aggiornare periodicamente software e sistema operativo;
- Definire la programmazione di backup periodici;
- Implementare funzionalità di protezione dati e webfilter;
- Garantire formazione adeguata a tutto il personale;
- Predisporre la disconnessione dei dispositivi, dopo un certo periodo di inutilizzo;
- Minimizzare i privilegi amministrativi nell'utilizzo dei software;
- Sviluppare il regolamento sull'uso delle tecnologie a scuola (policy di uso accettabile).

Accesso a Internet, filtri e antivirus sulla navigazione

In tutti i plessi dell'Istituto è attivato un accesso al web tramite WIFI e sono presenti connessioni cablate ai laboratori dotati di PC e ai monitor di classe (Digital Board). La banda a fibra ottica presente nei plessi dell'Istituto è di tipo FTTH; al fine di garantire una navigazione protetta la rete è filtrata alla sorgente dal CSI Piemonte (Consorzio per il Sistema Informativo). Al momento solo i docenti hanno libero accesso alla navigazione sulla rete.

Gestione accessi

Come previsto dal progetto **FESR-PON-2022 "Realizzazioni di reti locali, cablate e wireless, nelle scuole"** è stata strutturata una procedura di autenticazione univoca degli utenti per l'accesso al WIFI anche tramite dispositivi personali.

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.

Strumenti di comunicazione esterna

-Sito web

Fra gli strumenti di comunicazione esterna, troviamo in primis il sito web del nostro Istituto. Le informazioni e i contenuti di tipo didattico sono pubblicati su indicazione del Dirigente Scolastico.

-Blog scolastico

Il blog scolastico "Radionote" è un social-repository dove sono pubblicati contenuti multimediali sulla vita scolastica e le attività dell'Istituto Comprensivo Ilaria Alpi di Torino; vede come destinatari gli studenti, gli insegnanti, le famiglie e il territorio.

-Giornalino scolastico

Il gazzettino-web, "Il sasso nello stagno", è uno strumento digitale online, scritto e al servizio delle studentesse e degli studenti e delle famiglie, degli insegnanti e del personale dell'Istituto Comprensivo Ilaria Alpi di Torino.

-Registro elettronico

Per la comunicazione di avvisi, per la gestione delle presenze e delle assenze, per la valutazione degli alunni ci si avvale del registro elettronico Argo Didup. Le famiglie attraverso di esso possono visualizzare molte informazioni utili, interagendo con la scuola, su: andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari); risultati scolastici (voti, documenti di valutazione); prenotazione colloqui; comunicazione varie. I genitori ottengono dalla Segreteria le credenziali di accesso al servizio, vengono così abilitati sulla piattaforma Agro Didup Famiglia alle azioni destinate alla funzione genitoriale.

Strumenti di comunicazione interna

- Google Workspace for Education

Fra quelli di comunicazione interna, invece, troviamo il registro elettronico con tutte le sue funzionalità e la piattaforma di lavoro condiviso e collaborativo "Google Workspace for Education" che mette a disposizione app per la condivisione di materiali, comunicazioni, test, ecc.

- E-mail. Gli account di istituto e di posta elettronica sono di tre tipologie:

- **account studente**: permette l'accesso ai servizi e le applicazioni della piattaforma "Google Workspace for Education" (ad esempio l'accesso ai servizi di "Classroom") e l'indirizzo e-mail - così costruito: nominativo studente seguito dal dominio @icilariaalpitorino.edu.it. - che permette esclusivamente lo scambio di messaggistica con docenti e compagni all'interno del dominio e del Cloud protetto e riservato all'istituto. Questa tipologia di indirizzi e-mail non è dunque raggiungibile né può comunicare con l'esterno della piattaforma.
- **account docente:** permette l'accesso ai servizi della piattaforma cloud d'Istituto e il libero utilizzo - relativo al solo svolgimento dell'attività professionale - del servizio gmail.
- **account personale Ata, di segreteria e collaboratori scolastici:** permette l'utilizzo libero - relativo al solo svolgimento dell'attività professionale - del servizio Gmail e degli strumenti di deposito dei file, gli applicativi, lo strumento per le videoconferenze**.**

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.

Come stabilito dall'autonomia scolastica, è nei nostri regolamenti d'Istituto che si inseriscono le sanzioni disciplinari in caso di uso scorretto dei cellulari da parte degli alunni e dei docenti.

Si confida nella proficua collaborazione dei genitori con il nostro Istituto per educare i ragazzi ad un uso corretto e sicuro delle nuove tecnologie, per trasmettere valori quali il rispetto, la responsabilità e consapevolezza delle proprie azioni.

Per gli studenti: gestione degli strumenti personali (cellulari, tablet, ecc.)

Come espresso nel Patto di Corresponsabilità, gli alunni si impegnano a tenere spenti e custoditi nello zaino i telefoni cellulari. In caso di urgenza per comunicazioni tra gli alunni e le famiglie, su autorizzazione dei docenti e sotto il diretto controllo dei collaboratori scolastici, gli alunni possono comunicare con le famiglie tramite gli apparecchi telefonici della scuola. Non è consentito l'uso di dispositivi personali se non in situazioni di estrema urgenza e con il permesso dei docenti.

Per i docenti: gestione degli strumenti personali (cellulari, tablet, ecc.)

Durante le ore di lezione è consentito ai docenti l'uso di dispositivi elettronici personali, come il tablet, unicamente a scopo didattico e a integrazione dei dispositivi scolastici disponibili (il computer di classe), soprattutto per l'utilizzo del registro elettronico. Durante il restante orario di servizio, l'uso del cellulare è consentito solo per comunicazioni personali che rivestano carattere di urgenza, mentre l'uso di altri dispositivi elettronici personali è permesso per attività funzionali all'insegnamento.

Per il personale della scuola: gestione degli strumenti personali (cellulari, tablet, ecc.)

Durante l'orario di servizio, al restante personale scolastico, l'uso del cellulare è consentito per comunicazioni personali urgenti. L'uso di altri dispositivi elettronici personali è permesso solo per attività funzionali al servizio, e preventivamente autorizzato.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024).

- 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).

- 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 consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola

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.*

La sensibilizzazione è il primo passo per poter arrivare ad un reale cambiamento positivo e, perché questo intervento sia efficace, è necessario che l'obiettivo e la strategia da utilizzare siano ben chiari a tutti che concorrono all'operazione.

Tutti gli operatori devono condividere la motivazione al cambiamento, informarsi a

divulgare e le informazioni sulla questione su cui si vuole intervenire a cominciare dal punto di partenza e poi sull'evoluzione della situazione man mano che si procede. La nostra scuola mira all'adozione di misure prevenzione e contrasto del bullismo e del cyberbullismo quali:

- l'aumento della competenza digitale in tutti i ragazzi all'interno delle materie curricolari;

- una risposta concreta ai bisogni dell'utenza, creando contatti con la rete dei servizi territoriali locali (tra cui la Polizia Postale);

- la divulgazione di un uso positivo e consapevole delle TIC negli studenti e nelle studentesse attraverso l'adesione al progetto Generazioni Connesse e la presentazione del documento di e-Policy;

- la sensibilizzazione di tutti i componenti della scuola e dei genitori della necessità di riconsiderare la propria identità, il proprio ruolo educativo e le proprie risorse, attraverso la condivisione di un patto educativo da aggiornare in itinere.

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).

Questa legge prevede la tutela dei minori per la prevenzione e il contrasto al cyberbullismo, adottando misure prevalentemente a carattere educativo/rieducativo. Essa pone al centro il ruolo dell'Istituzione Scolastica nella prevenzione e nella gestione del fenomeno, pertanto anche il nostro Istituto I.C. Ilaria Alpi ha provveduto a individuare fra i docenti un Referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo e ha stilato un Vademecum, consultabile sul sito della scuola, che vuole essere una guida operativa finalizzata alla diffusione di strumenti conoscitivi sulle attività di prevenzione del fenomeno del cyberbullismo per tutta comunità scolastica. Le strategie messe in atto dall'Istituto, per prevenire atti riconducibili ad atteggiamenti di cyberbullismo, si muovono nella direzione di creare un clima di fiducia, di stima e di accoglienza all'interno della scuola.

Gli atti di cyberbullismo si possono distinguere in due grandi gruppi:

1. cyberbullismo diretto: il bullo utilizza strumenti di messaggistica istantanea (es. sms, mms) 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.

Esistono dei segnali che possono aiutare ad individuare una potenziale vittima di Cyberbullismo, la vittima appare:

- nervosa quando riceve un messaggio o una notifica;

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

- soggetta a variare comportamento ed atteggiamento in modo repentino;

- ritrosa nel dare informazioni su ciò che fa online soprattutto dopo essere stata online;

- arrabbiata o depressa;

- meno interessata ad utilizzare sempre meno PC e telefono (arrivando ad evitarli);

- meno interessata alle attività familiari o extra-scolastiche che prima svolgeva;

- in peggioramento il suo rendimento scolastico.

Secondo il Codice penale, i ragazzi e le ragazze che commettono azioni di bullismo rientrano nei seguenti reati penalmente perseguibili: percosse (art. 581), lesione personale (art. 582), ingiuria (art. 594), diffamazione (art. 595), violenza privata (art. 610), minaccia (art. 612), danneggiamento (art. 635).

La Scuola e la famiglia collaborano al raggiungimento di un importante obiettivo: intervenire preventivamente ed efficacemente per arginare ed eliminare possibili manifestazioni di questo tipo di comportamenti antisociali.

Le tipologie di cyberbullismo maggiormente considerate sono:

- hate speech (il fenomeno dell'incitamento all'odio, all'intolleranza verso un gruppo o una persona;

- dipendenza da internet e dal gioco online (i comportamenti patologici/dipendenze);

- sexting (scambio di contenuti mediali sessualmente espliciti);

- il grooming o adescamento online (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);

- denigration (diffusione di pettegolezzi, insulti, voci lesivi della dignità della persona);

- body shaming (prendere in giro per l'aspetto fisico).

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).

La nostra Scuola intende portare avanti ciò che Linee prevedono ossia:

- la formazione del personale scolastico, prevedendo la partecipazione di un proprio Referente;

- lo sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);

- la promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;

- la previsione di misure di sostegno e rieducazione dei minori coinvolti;

- l'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.

I casi accertati di cyberbullismo possono essere segnalati attraverso le procedure attivate dall'Istituto. Qualora i fatti venissero accertati, lo stesso, si avvale del proprio regolamento al fine di sanzionare i colpevoli.

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.

Come riconoscere e prevenire l'hate speech?

Ovviamente tutto ciò che manifesta intolleranza e malvagità verso il prossimo è condannabile ma, per poter valutare la gravità delle varie forme di manifestazione di questi sentimenti è utile prendere in considerazione alcuni aspetti:

-Il contenuto e il tono

Alcune espressioni di odio sono più estreme, utilizzano termini più insultanti epossono

perfino istigare altri ad agire mentre altri insulti sono più moderati o sono semplicemente generalizzazioni eccessive, che presentano certi gruppi o individui sotto una categoria.

-L'intenzione degli autori degli insulti

Può anche capitare di offendere gli altri senza volerlo, e magari poi di pentirsene e ritirando quanto detto; in altri casi casi, invece, le affermazioni sono intolleranti e sgradevoli e l'autore ha proprio l'intenzione di offendere e fare del male.

-Il bersaglio o i bersagli potenziali

Vi sono dei gruppi, o degli individui che possono essere più vulnerabili di altri alle critiche; questo può dipendere dal modo in cui sono considerati nella società, o da come sono rappresentati nei media, oppure dalla loro situazione personale, che non permette loro di difendersi efficacemente.

-Il contesto

Il contesto di una particolare espressione di odio è legato talvolta a circostanze storiche e culturali specifiche e 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, ecc.

-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 presente; le ripercussioni negative subite dall'individuo o dal gruppo molto spesso risultano essere più importanti della valutazione dell'episodio da parte di osservatori esterni.

Negli ultimi anni, il discorso d'odio online è diventato un fenomeno molto diffuso e preoccupante, che ha radici culturali e sociali profonde e che pone nuovi interrogativi e sfide alla questione della libertà di espressione sul Web. In questo contesto, i giovani rischiano di essere maggiormente esposti per il massiccio uso dei Social. L'educazione e la sensibilizzazione sono le strategie più efficaci per combattere e prevenire il discorso d'odio su Internet e la scuola si trova in prima linea di fronte al difficile compito di affrontare questo fenomeno, che ha senza dubbio forti ripercussioni nelle relazioni tra i pari e nella propria relazione col mondo. L'approccio metodologico per prevenirlo è la promozione dell'educazione al rispetto dell'altro, alla tutela della dignità umana e all'utilizzo di un dialogo rispettoso tra gli individui. Inoltre l'educazione all'empatia, all'utilizzo delle parole gentili, lo studio del manifesto delle parole ostili aiutano i ragazzi a capire l'importanza di quanto le parole siano importanti e se utilizzate male, possano ferire un compagno/a.

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?

Questo è un argomento trasversale, che rientra nella cittadinanza digitale, e i docenti affrontano in classe quando fanno riflettere studenti e studentesse sul fatto che la tecnologia è uno strumento positivo e che serve a raggiungere i propri obiettivi.

Come Scuola, integrando la tecnologia nella didattica in modo costruttivo e coerente, si mostra quanto il suo utilizzo sia funzionale e creativo.

Far riflettere i ragazzi sulle loro abitudini online è importante perché siano più consapevoli su come impegnare il loro tempo sulla Web in modo positivo.

I videogiochi vanno pensati in termini positivi, perché un loro uso adeguato ha sui ragazzi un effetto positivo.

Bisogna aiutarli a capire come sceglierli con contenuti adeguati all'età (classificazione PEGI) e ad utilizzarli per un tempo adeguato e non eccessivo.

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.

Tali contenuti spesso vengono diffuse attraverso il cellulare o attraverso siti, e-mail, chat. L'invio di foto che ritraggono minorenni al di sotto dei 18 anni in pose sessualmente esplicite configura, infatti, il reato di distribuzione di materiale pedopornografico. I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di "revenge porn" letteralmente "vendetta

porno". Si veda la Legge 19 luglio 2019 n. 69, art. 10.

I ragazzi vengono guidati a sviluppare un pensiero critico, che aiuta loro a capire che tra le caratteristiche del fenomeno vi sono principalmente:

La fiducia tradita: chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale).

La pervasività con cui si diffondono i contenuti: in pochi istanti e attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e infinito di persone e ad altrettante piattaforme differenti.

Il contenuto, così, diventa facilmente modificabile, scaricabile e condivisibile e la sua trasmissione è incontrollabile.

La persistenza del fenomeno: il materiale pubblicato online può permanervi per un tempo illimitato e potrebbe non essere mai definitivamente rimosso.

Un contenuto ricevuto, infatti, può essere salvato, a sua volta re-inoltrato oppure condiviso su piattaforme diverse da quelle originarie e/o in epoche successive.

A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool.

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 nell'altro/i

- depressione.

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.

È fondamentale far capire agli studenti che utilizzano i Social, che non si è in grado di sapere effettivamente chi c'è dall'altra parte dello schermo e, quindi, parlare con uno sconosciuto.

Nell'attività svolte dall'Istituto si educa i ragazzi a come creare profili privati e non pubblici; a riconoscere quando una conversazione mette a disagio; a capire quando le richieste dell'interlocutore sembrano non adeguate; a chiedere l'intervento di un adulto, quando la situazione va oltre la propria capacità di risolvere un problema.

Il miglior modo per prevenire casi di adescamento online è accompagnare ragazzi/e in un percorso di educazione (anche digitale) all'affettività. Ciò aiuta a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio. È molto importante, inoltre, che i/le ragazzi/e sappiano a chi rivolgersi in caso di necessità, anche se pensano di aver fatto un errore, se si vergognano e si sentono in colpa.

Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento di cui potersi fidare, senza sentirsi giudicati, ma compresi ed ascoltati.

Affinché ciò avvenga occorre tenere sempre aperto il canale di comunicazione reciproca sui temi dell'affettività e del digitale.

Casi di adescamento online richiedono anche l'intervento della Polizia Postale e delle Comunicazioni, a cui bisogna rivolgersi il prima possibile.

Inoltre, l'istituto ha intrapreso, all'interno dell'educazione civica, percorsi didattici finalizzati alla prevenzione del grooming accompagnando gli/le studenti/studentesse

in percorsi di educazione all'affettività.

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.

Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia. L'intento è quello di facilitare il processo di rimozione del materiale stesso dalla Rete e allo stesso tempo consentire le opportune attività investigative finalizzate ad identificare chi possiede quel materiale, chi lo diffonde e chi lo produce.

Parallelamente, se si ravvisa un rischio per il benessere psicofisico dei/delle ragazzi/e coinvolte nella visione di questi contenuti sarà opportuno ricorrere a un supporto psicologico anche passando per una consultazione presso il medico di base o pediatra di riferimento.

Le strutture pubbliche a cui rivolgersi sono i servizi sociosanitari del territorio di appartenenza:

- Consultori Familiari,

- Servizi di Neuropsichiatria infantile,

- centri specializzati sull'abuso e il maltrattamento all'infanzia, etc.

Se si è a conoscenza di tale tipologia di reato è possibile far riferimento alla:

- Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni;

- Polizia di Stato – 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 online.

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.

La pedopornografia è 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 delle hotline.

Per maggiori approfondimenti, si invita a fare riferimento al Vademecum di Generazioni Connesse.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024).

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

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

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

☐ 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 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.

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.

Prevenzione

Rischi e opportunità: La prima responsabilità degli insegnanti, osservatori privilegiati in quanto spesso confidenti o semplici spettatori delle esperienze dei loro alunni, consiste nell'imparare a riconoscere i rischi più comuni che possono derivare da un utilizzo non adeguato delle nuove tecnologie e della rete. Allo stesso tempo è compito degli insegnanti guidare gli alunni alla scoperta delle positive potenzialità delle nuove tecnologie.

Azioni: L'obiettivo che l'insegnante deve proporsi dopo avere riconosciuto il pericolo è agire di conseguenza, con azioni di contrasto efficaci e mirate, rispetto ai rischi. Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli studenti in orario scolastico, vi sono le seguenti:

- diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web, condividendo materiali messi a disposizione sul sito del progetto "Generazioni connesse" e attraverso incontri di formazione;

- richiedere l'autorizzazione esplicita da parte dei genitori all'utilizzo dei dati personali degli alunni (es. liberatoria per la pubblicazione di foto, immagini, video relativi al proprio/a figlio/a per la partecipazione a progetti didattici e altro);

- far rispettare il divieto di utilizzo di dispositivi digitali propri, quali smartphone e tablet, agli studenti in orario scolastico se non necessari allo svolgimento di un'attività didattica.

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.

Tali situazioni di presunto o comprovato pericolo vanno comunicate con urgenza al Dirigente Scolastico.
Eventuale convocazione, da parte del Dirigente, di un Consiglio straordinario per decidere la sanzione. Fatti particolarmente gravi verranno segnalati alle autorità competenti dal Dirigente scolastico.

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

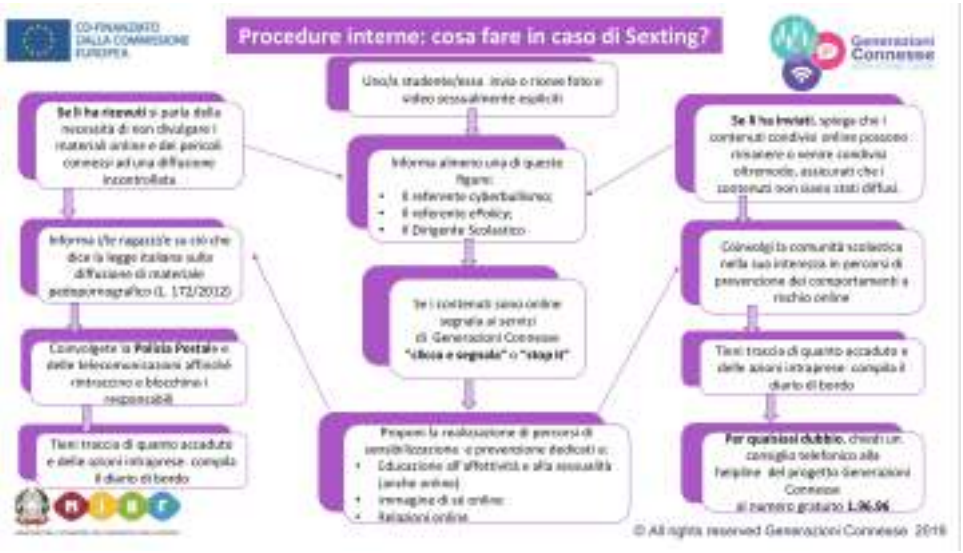
carenti o inadeguate.

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

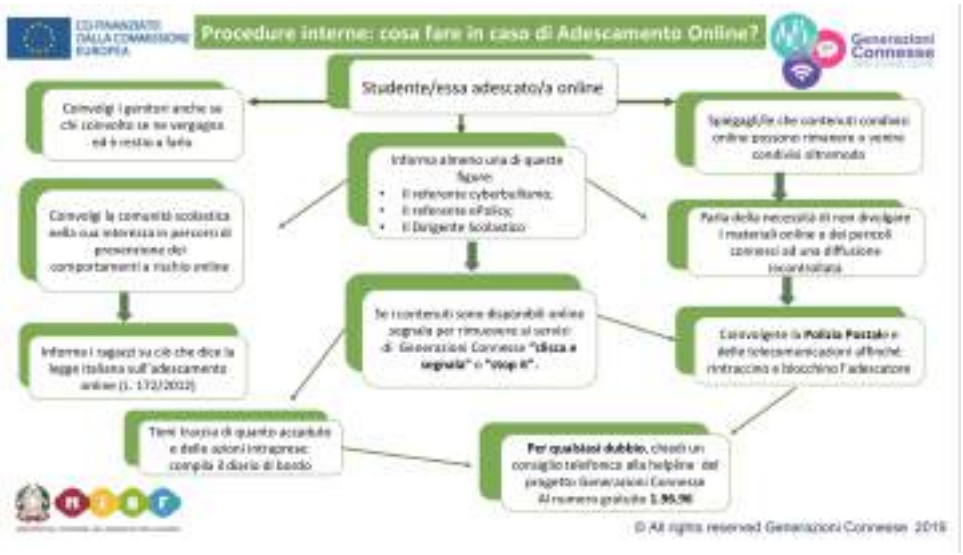
5.4. - Allegati con le procedure

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

Il nostro piano d'azioni:

- monitoraggio delle procedure di segnalazione;

- condivisione delle procedure con la comunità scolastica tramite il sito istituzionale;

- condivisione del documento e-policy con tutta la comunità scolastica tramite il sito d'istituto.