Ministero dell'Istruzione
Istituto d'Istruzione Superiore **"Carlo** e **Nello Rosselli"** - Aprilia
Codice meccanografico LTIS004008 – Codice fiscale 80007670591

Generazioni Connesse
SAFER INTERNET CENTRE

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

Co-financed by the European Union
Connecting Europe Facility

Documento E-Safety Policy

A.S. 2020/21

INDICE

1. INTRODUZIONE AL DOCUMENTO DI E-POLICY

1.1 Scopo della E-policy

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.

L'utilizzo sempre più diffuso delle TIC (Tecnologie dell'Informazione e della Comunicazione) all'interno degli ambienti scolastici da parte di tutti i componenti della comunità educativa pone l'accento sulla necessità di educare ad un loro uso corretto e responsabile. Motivo per cui la scuola ha elaborato questo documento seguendo le indicazioni della Legge 71/2017 e delle LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo e cyberbullismo (ottobre 2017) elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con "Generazioni Connesse" e il Safer Internet Center per l'Italia, programma comunitario istituito dal DF C Europeo e dal Consiglio

dell'Unione. In particolare l'intento dell'istituto è quello di promuovere l'uso consapevole e critico da parte dei discenti delle tecnologie digitali e di internet, di far acquisire loro procedure e competenze "tecniche" ma anche corrette norme comportamentali, di prevenire ovvero rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile delle tecnologie digitali. Esso è redatto per accrescere le conoscenze e competenze di tutti coloro che operano nella scuola e delle famiglie per accertare situazioni a rischio e individuare modalità che permettano di prevenire, affrontare e contrastare i fenomeni del bullismo e cyberbullismo. Con il presente documento si definiscono le misure che l'Istituto intende adottare:

- per la promozione dell'utilizzo delle ICT nella didattica;
- per la prevenzione, ovvero le azioni finalizzate alla prevenzione di fenomeni legati ai rischi delle tecnologie digitali;
- per la segnalazione dei casi, ovvero le disposizioni semplici su come segnalare i casi nella scuola. per la gestione dei casi, ovvero le misure che la scuola intende attivare a supporto delle famiglie e degli studenti che sono stati vittime o spettatori attivi e/o passivi di quanto avvenuto.

Occorre, inoltre, premettere che:

- ✓ il progetto "Generazioni connesse" verrà inserito nel nostro Piano Triennale dell'Offerta Formativa e le azioni preventivate nel Piano d'Azione di questa scuola, visto il loro elevato numero e la complessità che alcune di esse presentano, verranno portate avanti progressivamente negli anni;
- ✓ b) le attività di promozione all'utilizzo delle tecnologie digitali nella didattica costituiscono un tema centrale per l'attuazione del Piano Nazionale Scuola Digitale e sono già previste nel Piano Triennale dell'Offerta Formativa, in particolare nel progetto predisposto dall'animatore digitale, come previsto dal Miur, e quindi non saranno trattate in questa policy. L'indirizzo che qui viene dato è che la prevenzione e la gestione dei casi di scorretto utilizzo delle tecnologie sono efficaci se sono strettamente legate al loro uso quotidiano e consapevole.

Per l'elaborazione del presente documento ci si è avvalsi del materiale bibliografico, reperibile in rete e messo a disposizione dai siti Generazioni Connesse e Piattaforma Elisa.

1.2 Ruoli e responsabilità

L'istituto in oggetto ha costituito un gruppo di lavoro, formato da: Referente per il Bullismo

e il Cyberbullismo, il primo collaboratore del DS, dall'Animatore digitale e da altri docenti appositamente formati per la gestione delle emergenze.

Il seguente documento definisce in modo chiaro i ruoli e le responsabilità di ogni membro della comunità educante.

I ruoli sono declinati secondo le azioni proprie di ciascuno.

Dirigente Scolastico

- Promuovere l'uso consentito delle tecnologie e di internet
- Promuovere il rispetto della E-policy d'Istituto.
- Garantire la sicurezza dei dati.
- Convocare gli interessati di atti di bullismo e cyberbullismo e i loro genitori per adottare misure di assistenza alla vittima e sanzioni, in base alla gravità del fatto, e percorsi rieducativi per l'autore.
- Garantire la sicurezza (tra cui la sicurezza on line) dei membri della comunità scolastica.
- Garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line. Essere a conoscenza delle procedure per la prevenzione, rilevazione e gestione di strategie utili per individuare casi di rischio nell'utilizzo delle TIC a scuola.
- Comprendere e seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.
- Garantire che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC).
- Ricevere relazioni periodiche di monitoraggio dal Referente del bullismo e del cyber bullismo, dall'Animatore digitale e /o dal Team digitale.

Amministratori di sistema

- Essere responsabili per i problemi di sicurezza online dell'istituto.
- Promuovere la consapevolezza e l'impegno per la salvaguardia online di tutta la comunità scolastica, attraverso informative e indicazioni.
- Garantire che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente per la sicurezza on line.

- Facilitare la formazione e la consulenza per tutto il personale.
- Formare gli utenti alla corretta condivisione dei dati personali.
- Fornire le indicazioni per evitare l'accesso ai materiali illegali.
- Monitorare e prevenire azioni di cyberbullismo (o presunte tali).

Referente bullismo e cyberbullismo

- Promuovere l'uso consentito delle tecnologie e di internet.
- Coordinare la Commissione preposta.
- Ascoltare e aiutare gli alunni per ridurre e prevenire fenomeni di illegalità e inciviltà o chi si trova in difficoltà perché oggetto di prevaricazioni online.
- Intervenire nei confronti di chi fa un uso inadeguato della rete e dei cellulari, ascoltando eventuali problemi e fornendo consigli.
- Sensibilizzare, dare informazioni agli alunni e alle famiglie su quelli che sono i rischi della rete, comunicandogli le azioni che la scuola mette in atto in caso di fenomeni di bullismo e cyberbullismo.
- Informare gli insegnanti della eventuale presenza di casi di bullismo e cyberbullismo.
- Promuovere e pubblicizzare le iniziative di formazione rivolte agli alunni, ai genitori, ai docenti e al personale ATA dell'Istituto.
- Coordinare le iniziative di prevenzione e di contrasto del bullismo e del cyberbullismo, anche in collaborazione con Forze di Polizia, associazioni e centri di aggregazione giovanili presenti nel territorio. Coordinare e curare il monitoraggio delle azioni intraprese per combattere i fenomeni di bullismo e cyberbullismo.
- Mettere a disposizione la normativa vigente e i materiali di approfondimento.

L'animatore digitale e il suo team

- Pubblicare l'E-Safety Policy sul sito della scuola.
- Garantire che i dati personali degli alunni pubblicati sul sito siano tutelati.
- Coordinare e mantenere contatti con il Team digitale, con il Referente del bullismo e del cyberbullismo, con le autorità e gli enti esperti.
- Relazionare periodicamente il lavoro del gruppo con il Dirigente Scolastico.
- Stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;

- Monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- Assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti.
- Coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".

Direttore dei Servizi Generali e Amministrativi:

- Assicurare, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione richiesti da cattivo funzionamento e/o danneggiamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate;
- Facilitare la trasmissione di comunicazioni relative alle tecnologie digitali tra le varie componenti della scuola (Dirigente scolastico, Animatore digitale, docenti e famiglie degli alunni);
- Curare la registrazione dei disservizi e delle problematiche relative alla rete e all'uso del digitale segnalate dai docenti, provvedendo all'intervento del personale tecnico di assistenza.

I CdC

- Prevedere unità didattica sulla sicurezza on line, sul rispetto alla diversità, sull'educazione emotiva e sull'uso delle TIC anche nel percorso di educazione civica.
- Informarsi e aggiornarsi sulle problematiche connesse alla sicurezza nell'utilizzo delle TIC.
- Assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e della rete.
- Promuovere un utilizzo corretto e sicuro delle TIC e di internet da parte degli alunni.
- Supervisionare gli alunni quando svolgono attività on line.
- Assicurare la riservatezza dei dati personali trattati secondo le indicazioni del Responsabile Protezione Dati.

- Segnalare al Dirigente scolastico, qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle TIC o internet, per l'adozione delle procedure previste dalle norme.
- Segnalare al Dirigente (o suoi delegati) episodi di bullismo e cyber bullismo.
- Promuovere la consapevolezza degli alunni per i problemi legali relativi ai contenuti elettronici.

Il personale scolastico

- Comprendere e contribuire a promuovere politiche di e-sicurezza.
- Essere consapevoli dei problemi di sicurezza on-line connessi all'uso dei telefonini, fotocamera e dispositivi portatili.

Gli alunni

- Leggere, comprendere e aderire l'E-Safety Policy.
- Accedere all'ambiente di lavoro con il corretto account.
- Non divulgare le credenziali di accesso (username, password), e archiviare i propri documenti in maniera ordinata e facilmente rintracciabile;
- In caso di riscontro di malfunzionamenti della strumentazione e/o di contatto accidentale con informazioni, immagini e/o applicazioni inappropriate comunicarlo immediatamente all'insegnante;
- Non eseguire tentativi di modifica della configurazione di sistema delle macchine;
- Non utilizzare la strumentazione della scuola a scopi personali, ludici e/o ricreativi (a meno che l'attività didattica non lo preveda esplicitamente);
- Non utilizzare propri dispositivi esterni personali senza aver acquisito il permesso da parte dell'insegnante (BYOD).
- Chiudere correttamente la propria sessione di lavoro.
- Capire l'importanza di segnalare abusi o uso improprio delle TIC.
- Avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali.
- Adottare condotte rispettose degli altri anche quando si comunica in rete.
- Esprimere domande o aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti, al referente bullismo e cyber bullismo e al Dirigente.
- Conoscere la politica della scuola sull'uso di immagini e sul cyber bullismo.
- Assumersi la responsabilità di conoscere i rischi legati ad internet e alle tecnologie digitali.

I genitori

- Sostenere la scuola nel promuovere la sicurezza in rete e approvare l'accordo e-safety.
- Leggere, comprendere e firmare il suddetto accordo.
- Assicurarsi che la scuola abbia preso tutte le precauzioni necessarie circa un uso corretto della tecnologia da parte degli alunni.
- Seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dalla scuola, in particolare controllare l'utilizzo del PC e di internet.
- Partecipare alle iniziative di formazione proposte dall'istituto in materia di sicurezza in rete, di bullismo e cyber bullismo.

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).

1.4 Condivisione della policy con l'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.

Allo scopo di condividere regole comuni per l'utilizzo sicuro di Internet sia a casa che a scuola, si invitano tutti i genitori a prestare la massima attenzione ai principi e alle regole contenute nel presente documento. Si richiede che ogni genitore e/o tutore si impegni a farle rispettare ai propri figli anche in ambito domestico, primariamente assistendo i minori nel momento dell'utilizzo della rete e poi ponendo in atto tutti i sistemi di sicurezza che aiutino a diminuire il rischio di imbattersi in materiale indesiderato. La scuola promuove eventi e/o dibattiti informativi e formativi, in momenti diversi dell'anno, rivolti a tutto il personale, agli alunni e ai loro genitori, con il coinvolgimento di esperti, sui temi oggetto di codesto Documento. Tra le misure di prevenzione che la scuola mette in atto ci sono, inoltre, azioni finalizzate a promuovere una cultura dell'inclusione, del rispetto dell'altro e delle differenze così che l'utilizzo di Internet e dei cellulari oltre che collocarci all'interno di un sistema di relazioni, ci renda consapevoli di gestire con un certo grado di trasparenza i rapporti che si sviluppano in tale ambiente, giungendo a riconoscere e gestire le proprie emozioni. A tal proposito si sono attivati più "Sportello di ascolto" rivolti a tutta la comunità scolastica articolati in colloqui individuali e/o collettivi, al fine di migliorare il benessere personale e scolastico mediante un'attività di supporto della sfera emotiva, relazionale e comportamentale.

1.5 Gestione delle infrazioni alla policy

Il Dirigente scolastico ha la facoltà di revocare l'accessibilità temporanea o permanente ai

laboratori informatici e/o all'utilizzo di strumenti tecnologici (pc, tablet, notebook, ecc) a chi non si attiene alle regole stabilite. In relazione a quanto specificato in questa policy e nelle responsabilità dei soggetti coinvolti si analizzano e disciplinano le seguenti infrazioni:

Infrazioni degli alunni.

È bene che i docenti introducano, preventivamente, attività laboratoriali miranti a sviluppare nei loro alunni una sempre maggiore consapevolezza dei rischi legati a un uso imprudente e improprio del web e che forniscano loro, ogniqualvolta avvenga un'infrazione alle regole stabilite, gli strumenti per affrontare le conseguenze dei loro errori. I provvedimenti disciplinari da adottare da parte del Consiglio di Classe nei confronti dell'alunno che ha commesso un'infrazione alla policy in proporzione alla gravità dell'infrazione commessa saranno i seguenti:

- richiamo verbale;
- sanzioni previste dal regolamento di disciplina in relazione alla gravità dell'azione commessa
- assegnazione di attività aggiuntive da svolgere a casa su temi di Cittadinanza e Costituzione;
- divieto temporaneo di prendere parte alla ricreazione e simili;
- convocazione dei genitori per un colloquio con l'insegnante;
- convocazione dei genitori per un colloquio con il Dirigente scolastico.

Infrazioni del personale scolastico

Le infrazioni alla policy da parte del personale scolastico possono riguardare sia la mancata osservanza delle regole qui descritte sulla gestione della strumentazione, sia la mancata sorveglianza e pronto intervento nel caso di infrazione da parte degli alunni. Nel primo caso la gravità si valuta sull'esposizione al rischio procurata agli alunni, nel secondo caso sul danno per la non tempestiva attivazione delle azioni qui indicate. La gestione delle infrazioni in quest'ambito ricade nella disciplina contrattuale.

Mancato rispetto del presente regolamento da parte dei genitori

Compito dei genitori è supportare gli insegnanti e il personale scolastico nel riconoscimento e nella costruzione di azioni di contrasto efficaci ai principali rischi rappresentati dalla navigazione in internet di utenti molto giovani e spesso poco accorti. Nel caso di mancato rispetto del documento, si prevedono interventi, rapportati alla gravità, che vanno dalla

semplice comunicazione del problema alla convocazione da parte del coordinatore di classe o del Dirigente Scolastico.

1.6 Integrazione della e-policy con regolamenti esistenti

Il Regolamento d'Istituto e il regolamento bullismo e cyberbullismo vengono aggiornati 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.

1.7 Monitoraggio dell'implementazione dell'e-policy e 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.

CAPITOLO 2

FORMAZIONE E CURRICOLO

2.1 Curricolo per le competenze digitali degli studenti

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.

In quest'ambito si seguono le indicazioni contenute nel PNSD (azione 14), in cui si individuano alcuni framework di riferimento per la definizione e lo sviluppo delle competenze digitali, tra cui il Frame work DIGCOMP, che prevede 21 competenze, di cui alcune specifiche nell'area della sicurezza.

DIMENSIONE TECNOLOGICA

- Riconoscere le criticità tecnologiche e le interfacce.
- Selezionare la tecnologia adeguata per ciascun compito.
- Operare logicamente.
- Rappresentare processi simbolici
- Distinguere tra reale e virtuale.

DIMENSIONE COGNITIVA

- ✓ Saper sintetizzare, schematizzare e analizzare i testi, i dati, le tabelle e i grafici.
- ✓ Saper valutare la pertinenza dell'informazione e la sua attendibilità.

DIMENSIONE ETICA

- Conoscere i concetti di tutela della privacy.
- Rispettare i diritti intellettuali dei materiali reperiti in Internet e l'immagine degli altri.
- Comprendere il dislivello sociale e tecnologico che può esistere tra paesi, persone, generazioni, e il problema dell'accessibilità.

OBIETTIVO COMUNE ALLE TRE DIMENSIONI

Saper comprendere l'importanza delle nuove tecnologie e delle TIC per costruire una conoscenza collaborativa.

2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle tic nella didattica

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

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

Le attività di formazione si svolgeranno su due livelli:

- formazione istituzionale, organizzata dal Miur secondo il PNSD, attraverso gli snodi formativi;
- formazione specifica di Istituto, legata alle esigenze formative rilevate ad inizio anno a cura della Funzione Strumentale, sulla base del frame work DIGCOMP, come da progetto incluso nel PTOF.

2.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di internet e delle tecnologie

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.

Anche il percorso della formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet, può prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi.

Sarà predisposta una bacheca online per la messa a disposizione e la condivisione di materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di internet, collegata alla homepage del sito scolastico.

2.4 Sensibilizzazione delle famiglie e integrazione del patto di corresponsabilità

L' Istituto ha attivato ed attiverà iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine sono previsti incontri fra tutti gli attori coinvolti per la diffusione del materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati e dalle forze dell'ordine. Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo. Sul sito scolastico e sulla relativa bacheca virtuale relativa a "Generazioni connesse" saranno messi in condivisione materiali dedicati ad alunni e alle famiglie come guide in formato .pdf e video che possono fornire spunti di approfondimento e confronto. Inoltre verranno appositamente integrati il regolamento d'istituto e il patto di corresponsabilità.

CAPITOLO 3
GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA

3.1 Protezione dei dati personali

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

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

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

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

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

3.2 Accesso a Internet

- L’accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.
- 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.
- Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.
- L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.
- Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.

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

  Il diritto di accesso a Internet è dunque presente nell’ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di “fornire a tutte le scuole le condizioni per l’accesso alla società dell’informazione e fare in modo che il “diritto a Internet” diventi una realtà, a partire dalla scuola”.

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

L'infrastruttura e la strumentazione TIC dell'istituto sono un patrimonio di tutti, esse vanno utilizzate nel rispetto delle norme contenute nel "Regolamento per l'utilizzo dei laboratori multimediali". I danni causati alle attrezzature saranno a carico di chiunque disattenda il suddetto regolamento. L'accesso ad infrastrutture e strumentazione TIC utilizzabili per la didattica è riservato ai docenti e agli alunni ed è limitato al perseguimento di scopi formativi. I docenti devono formare i propri alunni al rispetto del suddetto Regolamento, per gli aspetti di loro pertinenza. L'aggiornamento delle infrastrutture permette l'accesso a INTERNET a tutte le classi attraverso una rete WI-FI adeguata al numero di studenti.
Occorre quindi considerare tutti gli aspetti riguardanti la gestione degli account degli utenti, il filtraggio dei contenuti e gli aspetti legali che riguardano prevalentemente la privacy. Per quanto riguarda l'hardware, la scuola provvede a pianificare interventi periodici di manutenzione grazie ad una figura con incarico specifico relativo alla gestione/manutenzione delle apparecchiature.

ACCESSO AD INTERNET: FILTRI, ANTIVIRUS E SULLA NAVIGAZIONE

L'istituto è dotato di una rete a banda ultralarga; l'accesso a INTERNET è libero solo per gli ambienti di segreteria e di presidenza che, peraltro risultano protetti da software antivirus. L'accesso attraverso WI-FI è protetto: tutti gli utenti sono dotati di password personale. Gli ultimi adeguamenti tecnologici hanno previsto il potenziamento della rete LAN/WLAN attraverso access point, apparati di rete switch e firewall.

GESTIONE ACCESSI (PASSWORD, BACKUP, ECC.)

La scuola adotta tutte le necessarie precauzioni per evitare l'accesso a siti non adatti all'interno della scuola. L'accesso ai portali istituzionali come SIDI, Istanze on-line,alla Segreteria Digitale, PON ecc. prevede l'uso di credenziali personali, mentre l'accesso a portali tematici si effettua per mezzo di password uniche condivise tra i referenti di progetti e/o azioni e la dirigenza. I docenti possono accedere alla propria sezione del registro elettronico con credenziali personali. Anche a genitori sono state fornite credenziali personali di accesso al registro elettronico. I dati personali vengono trattati nel rispetto della normativa sulla privacy.
.

MAIL

L'accesso alla posta elettronica istituzionale MI può essere effettuato solo dal personale di segreteria e dalla presidenza utilizzando credenziali uniche. L'uso di e-mail personali viene

favorito come mezzo di diffusione di comunicati e notifiche di circolari d'istituto pubblicate sul sito istituzionale.

SITO WEB DELLA SCUOLA La scuola è dotata di un sito istituzionale sul quale diversi siti tematici rimandano al contenuto di interesse (pubblicità legale, circolari, bacheca sindacale ecc). Per mezzo di credenziali personali si accede all'area riservata per la presa visione di circolari e comunicazioni ufficiali.
Sul sito è possibile trovare regolamenti, materiali didattici, pubblicizzazione di eventi, documentazione di attività curricolari ed extracurricolari svolte.

3.3 Strumenti di comunicazione on line

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.

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. Inoltre l’istituto organizzerà incontri volti a formare tutta la comunità educante sul tema delle tecnologie digitali e della protezione dei dati personali.

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.*

L'istituto organizzerà uno o più incontri, anche a distanza, di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti a tutta la comunità educante.

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.

Il Referente Bullismo e Cyberbullismo:

- 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;
- svolge un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Inoltre la legge 71/2017 e relative linee di orientamento prevedono a tutela della vittima l'oscuramento del web, infatti colui che abbia compiuto almeno 14 anni, e i genitori o esercenti la responsabilità sul minore, 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 di qualsiasi altro dato personale del minore, diffuso nella rete internet. Se non si provvede entro 48 ore, l'interessato può rivolgersi al Garante della Privacy che interviene direttamente entro le successive 48 ore.

Inoltre la normativa prevede che al dirigente spetterà informare subito le famiglie dei minori coinvolti in atti di bullismo e, se necessario, convocare tutti gli interessati per adottare misure di assistenza alla vittima e sanzioni e percorsi rieducativi per l'autore. Alle iniziative in ambito scolastico collaboreranno anche polizia postale e associazioni del territorio. Il dirigente scolastico che venga a conoscenza di atti di cyberbullismo (salvo che il fatto costituisca reato) deve informare tempestivamente i soggetti che esercitano la responsabilità genitoriale o i tutori dei minori coinvolti e attivare adeguate azioni di carattere educativo. Ammonimento da parte del questore: è stata
estesa al cyberbullismo la procedura di ammonimento prevista in materia di stalking (art. 612-bis c.p.). In caso di condotte di ingiuria (art. 594 c.p.), diffamazione (art. 595 c.p.), minaccia (art. 612 c.p.) e trattamento illecito di dati personali (art. 167 del codice della privacy) commessi mediante internet da minori ultraquattordicenni nei confronti di altro minorenne, fino a quando non è proposta querela o non è presentata denuncia è applicabile la procedura di ammonimento da parte del questore. A tal fine il questore convoca il minore, insieme ad almeno un genitore o ad altra persona esercente la responsabilità genitoriale; gli effetti dell'ammonimento cessano al compimento della maggiore età.

Le responsabilità negli atti di bullismo/cyberbullismo vanno distinte le diverse responsabilità ed a tal riguardo si identificano: a) Culpa del Bullo Minore; b) Culpa in educando e vigilando dei genitori; c) Culpa in vigilando (ma anche in educando ed in organizzando) della Scuola.

a) Culpa del bullo minore

Va distinto il MINORE DI 14 ANNI da quello tra i 14 ANNI ed i 18 ANNI. Il minore di 14 anni non è mai imputabile penalmente. Se viene però riconosciuto come “socialmente pericoloso” possono essere previste misure di scurezza.

Il minore tra i 14 e i 18 anni di età è imputabile se viene dimostrata la sua capacità di intendere e volere. La competenza a determinare la capacità del minore è del giudice che si avvale di consulenti professionali.

b) Culpa in vigilando ed educando dei genitori Si applica l'articolo 2048 del codice civile. Il non esercitare una vigilanza adeguata all'età e indirizzata a correggere comportamenti inadeguati (culpa in educando e vigilando) è alla base della responsabilità civile dei genitori per gli atti illeciti commessi dal figlio minorenne che sia capace di intendere e di volere. Di tali atti non può, infatti, per legge rispondere il minorenne, in quanto non ha autonomia patrimoniale. A meno che i genitori del minore non dimostrino di non aver potuto impedire il fatto, sono oggettivamente responsabili.

c) Culpa in vigilando e in organizzando della scuola

L' Art.28 della Costituzione Italiana recita che "I funzionari ed i dipendenti dello Stato e degli Enti pubblici sono direttamente responsabili, secondo le leggi penali, civili ed amministrative, degli atti compiuti in violazioni di diritti. In tali casi la responsabilità si estende allo Stato ed agli altri enti pubblici."

Dal punto di vista civilistico trova, altresì, applicazione quanto previsto all'Art. 2048 del codice civile, secondo comma a

che stabilisce che "i precettori e coloro che insegnano un mestiere o un'arte sono responsabili del danno cagionato dal fatto illecito dei loro allievi e apprendistato nel tempo in cui sono sotto la loro vigilanza". La presunzione di colpa può essere superata solamente laddove si dimostri di aver adeguatamente vigilato ovvero si dia la prova del caso fortuito. Per superare la presunzione, la scuola deve dimostrare di adottare "misure preventive

.

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.

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?

In relazione a ciò l'istituto ha elaborato un progetto sulle dipendenze in generale e ha

aderito nel corso dell'anno la progetto "Vite in gioco" il cui obiettivo è il contrasto al gioco patologico.

Per i prossimi anni sono previsti un ampliamento del progetto di cui sopra e il proseguimento degli sportelli d'ascolto già esistenti nell'istituto.

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.

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).

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 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.

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 devono 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;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

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

Le procedure di segnalazione e valutazione approfondita sono definite nel regolamento bullismo e cyber bullismo.

5.3 Gli attori del 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.

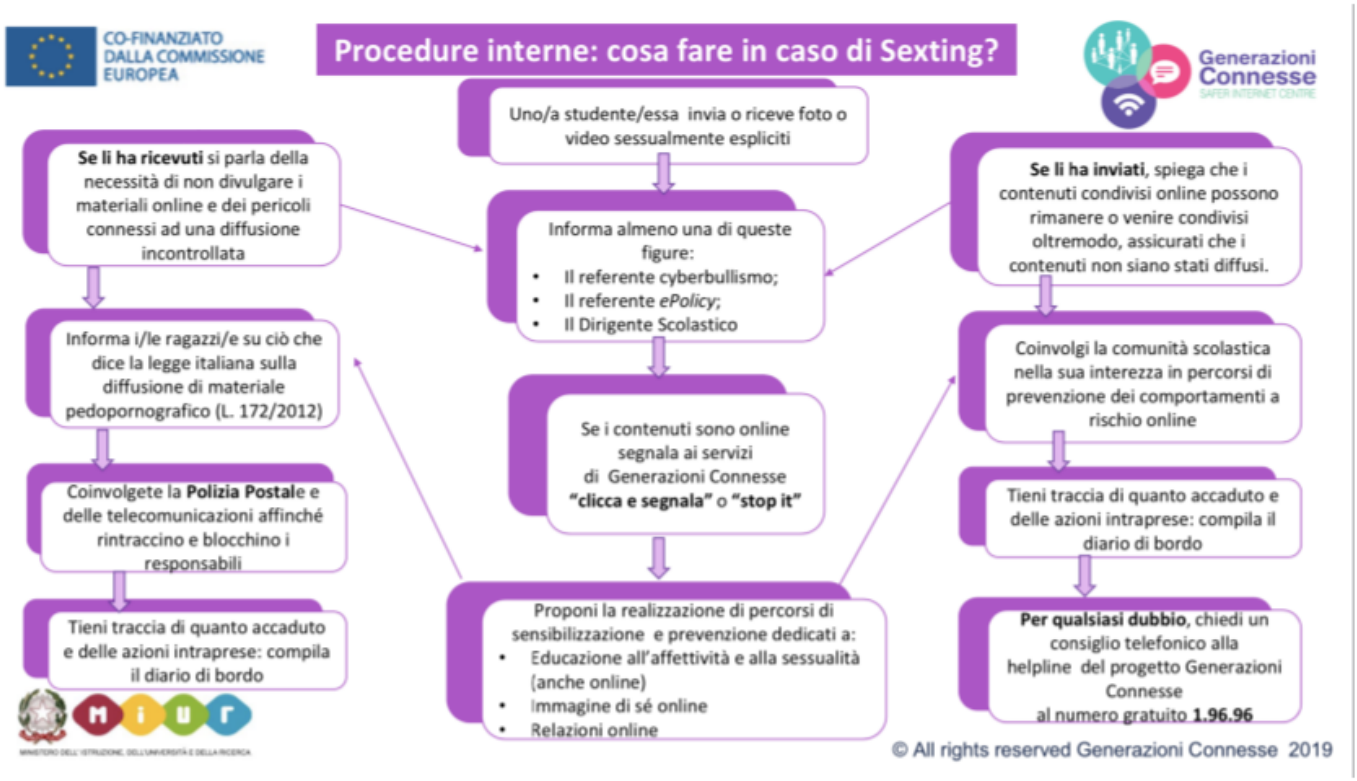
Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza 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.



Procedure interne: cosa fare in caso di adescamento online?