Documento di ePolicy

PZIS001007

I.I.S."DE SARLO-DE LORENZO" LAGONEGRO

VIA S. ANTUONO 192 - 85042 - LAGONEGRO - POTENZA (PZ)

Dott. ROBERTO SANTARSIERE

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.

L'IIS "De Sarlo- De Lorenzo", considerando l'importanza di favorire sempre più e implementare l'utilizzo dell'ICT nella pratica didattica quotidiana, è consapevole della necessità e dell'opportunità di elaborare una E-policy che rappresenti una guida per un uso consapevole, critico e responsabile dell'ICT (TIC).

Nell'elaborazione del presente documento l'Istituto ha tenuto conto delle "Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e cyberbullismo" emanate dal MIUR nel 2018, diretta emanazione della L. 71/2017 in collaborazione con il Safer Internet Center (SIC) per l'Italia, progetto co-finanziato dalla Commissione Europea nell'ambito del programma "Connecting Europe Facility" (CEF) – Telecom. E' opportuno citare le principali Agenzie nazionali sensibili al tema della sicurezza in Rete:

- Polizia Postale e delle Comunicazioni
- Autorità Garante per l'Infanzia e l'Adolescenza
- Save the Children Italia Onlus
- SOS Il Telefono Azzurro
- Università degli Studi di Firenze
- Università degli Studi di Roma "La Sapienza"
- Skuola.Net
- Cooperativa EDI (Educazione ai Diritti dell'Infanzia)
- Movimento Difesa del Cittadino
- Agenzia Dire

L'IIS "De Sarlo- De Lorenzo" ha da anni lavorato per proporre ai/alle propri/e studenti/studentesse un'offerta formativa che integri le nuove tecnologie nella didattica, facendo però sempre attenzione al benessere psico-fisico dei/delle suoi/sue discenti e si è impegnato nella promozione di valori e competenze finalizzate all'acquisizione di una cittadinanza digitale consapevole. Ecco perché è convinto che l'E-policy potrà costituire anche un valido supporto per l'organizzazione dell'insegnamento dell'Educazione Civica. Il presente documento è parte integrante del PTOF.

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.

L'IIS "De Sarlo-De Lorenzo", per rispondere efficacemente a tale esigenza, individua le seguenti figure, declinando per ciascuna gli specifici ambiti di intervento:

Il Dirigente Scolastico

- garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica;
- garantisce la formazione del personale docente e non docente sulla sicurezza e sulla prevenzione online;
- controlla e vigila su fenomeni di hacking ai danni delle reti e dei computer dell'Istituto, nonché delle piattaforme utilizzate per la didattica e per la gestione dei dati amministrativi;
- promuove la cultura della sicurezza online favorendo iniziative di formazione e prevenzione del fenomeno del cyberbullismo;
- promuove azioni di periodico monitoraggio sul tema;
- interviene nei casi più gravi di bullismo, cyberbullismo e uso improprio delle tecnologie digitali.

L'Animatore Digitale

- supporta la comunità scolastica per quanto concerne gli aspetti tecnico-informatici;
- cura la formazione interna alla Scuola negli ambiti del PNSD mediante l'organizzazione di laboratori formativi;
- controlla che gli utenti autorizzati accedano alla Rete della Scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione);
- supporta le attività del personale tecnico e amministrativo in relazione all'utilizzo delle tecnologie informatiche;
- favorisce la dematerializzazione delle attività relative alla didattica e l'informatizzazione di parte delle comunicazioni scuola-famiglia;
- monitora e rileva eventuali problematiche connesse all'utilizzo sicuro delle TIC.

Il Referente bullismo e cyberbullismo

- coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo, avvalendosi della cooperazione del Team Bullismo e Cyberbullismo, delle forze di Polizia, delle associazioni e dei centri di aggregazione giovanile presenti sul territorio;
- coinvolge, con progetti e percorsi formativi dedicati, tutte le componenti della comunità scolastica (personale docente e non docente, studenti, genitori).

I Docenti

- integrano il curriculum della propria disciplina con approfondimenti inerenti la sicurezza online e la politica adottata a riguardo dall'Istituto promuovendo così l'uso consapevole e responsabile delle TIC;
- nel rispetto della libertà d'insegnamento accompagnano e supportano gli studenti nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM e di altri dispositivi;
- segnalano, in quanto Pubblici Ufficiali, al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che veda coinvolti studenti e studentesse nel momento in cui ne vengano a conoscenza;
- gestiscono le comunicazioni digitali a carattere ufficiale nel rispetto del codice di comportamento professionale.

Il Personale Amministrativo, Tecnico e Ausiliario (ATA)

- garantisce supporto tecnico a studenti, studentesse e docenti nei laboratori che prevedono l'uso della LIM e di altri dispositivi;
- segnala, in qualità di Incaricato di Pubblico Servizio, comportamenti non adeguati nell'uso delle TIC ed episodi di bullismo e di cyberbullismo, nel momento in cui ne venga a conoscenza;
- è coinvolto nelle attività di formazione e di autoformazione in tema di bullismo e cyberbullismo e uso responsabile della rete.

Gli Studenti e le Studentesse

- utilizzano efficacemente e responsabilmente le tecnologie digitali in coerenza con quanto richiesto dai docenti;
- imparano a tutelare se stessi e i propri compagni dai rischi online;
- partecipano con senso di responsabilità alle iniziative e ai progetti di formazione proposti dalla scuola circa l'uso delle TIC e della Rete e si fanno promotori di quanto appreso;
- denunciano liberamente difficoltà o richieste di aiuto dinanzi ad eventuali disagi emersi.

I Genitori

- si impegnano a relazionarsi in maniera costruttiva con i docenti e ad agire in coerenza e continuità con l'Istituto scolastico nella promozione e nell'educazione all'uso consapevole, responsabile e rispettoso delle TIC e della rete, nonché all'uso responsabile dei device personali;
- controllano e vigilano, in ambito domestico, sulle attività svolte dai propri figli sui social network e sull’uso dei devices personali;
- leggono, accettano e condividono, all'atto dell'iscrizione, la E-policy dell'Istituto;
- concordano con i docenti le linee di intervento di carattere educativo in relazione ad eventuali problemi connessi ad un approccio inadeguato o pericoloso alle tecnologie digitali o a Internet.

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).

Le organizzazioni/associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve o/e lungo periodo, dovranno prendere atto di quanto stilato nell' E-policy dell’IIS “De Sarlo- De Lorenzo” e sottoscrivere un'informativa sintetica del documento in questione.

Essi sono tenuti a:

- prendere visione della politica dell'Istituto riguardo all'uso consapevole e responsabile della rete e delle TIC;
- promuovere la sicurezza online durante le attività di cui sono titolari;
- segnalare ai docenti preposti e al Dirigente Scolastico eventuali comportamenti problema o casi di abuso nell'utilizzo 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.

Attraverso una serie di iniziative dedicate, l'IIS "De Sarlo- De Lorenzo" si impegna ad assicurare la concreta promozione degli intenti dichiarati nel documento, valorizzando studenti e studentesse ed esplicitando ruoli e prerogative di tutte le figure operanti a vario titolo nella comunità scolastica.

In particolare:

- ai Coordinatori di Classe si fornirà copia del documento per la condivisione con gli studenti e le studentesse delle loro classi;
- agli studenti e alle studentesse verrà illustrato il presente documento insieme ai regolamenti correlati, al fine di fornire loro spunti di riflessioni, regole condivise di sicurezza e chiavi di lettura per interpretare e gestire consapevolmente il complesso mondo del Web;
- nel corso dell'anno ciascun docente dedicherà alcune lezioni alle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al Cyberbullismo;
- i rischi della rete e la lotta al Cyberbullismo saranno affrontati in UDA per classi parallele legate all'insegnamento dell'Educazione Civica;
- le famiglie saranno informate in merito alla linea di condotta adottata dalla Scuola per un uso sicuro e responsabile delle tecnologie digitali e di Internet attraverso la condivisione del presente documento e di materiali informativi specifici sul sito web della Scuola;

- espliciti riferimenti all'E-policy verranno inseriti nel Patto di corresponsabilità, per darne comunicazione alle famiglie;
- con cadenza periodica, la Scuola organizzerà incontri finalizzati a sensibilizzare/informare le famiglie sul tema della sicurezza informatica e sui comportamenti da monitorare o da evitare. La condivisione con le famiglie avverrà anche in seno ai singoli Consigli di Classe;
- sintetica informativa sull' e-Policy, con relativa procedura di segnalazione, verrà fornita ai soggetti esterni che erogano attività educative nell'Istituto.

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.

Eventuali infrazioni alla presente E-policy andranno tempestivamente segnalate al Dirigente Scolastico, che avrà cura di convocare le parti interessate onde valutare le possibili azioni da intraprendere.

Oltre a quanto espressamente indicato nel Regolamento di Istituto e di Disciplina e alle loro integrazioni, si segnalano le seguenti condotte inappropriate correlate all'uso delle TIC:

- uso di social network e blog per pubblicare, condividere o, in genere, postare commenti o giudizi lesivi della dignità altrui (condivisione online di immagini o video di compagni/e e/o di docenti senza il loro consenso; condivisione di scatti intimi e a sfondo sessuale; condivisione di dati personali altrui; invio di immagini o video volti all'esclusione di compagni/e; utilizzo di linguaggio denigratorio in una chat con lo scopo di escludere un compagno dal gruppo; diffamazione di docenti o collaboratori/collaboratrici scolastici/che attraverso social o app di messaggistica istantanea);
- condivisione di dati personali che possano permettere l'identificazione dei soggetti;
- connessioni a siti proibiti o comunque non autorizzati;
- collegamenti a siti web inadeguati durante la permanenza a scuola;
- incitamento all'odio nei confronti di un compagno o di un piccolo gruppo.

Gli interventi correttivi previsti saranno rapportati alla gravità dell'infrazione commessa, coerentemente con quanto definito nel Regolamento d'Istituto, allegato 1, regolamento di disciplina, e sue integrazioni.

Qualora l'infrazione dovesse configurarsi come reato, la Scuola, nella persona del

Dirigente Scolastico, attiverà le procedure di segnalazione formale alle competenti autorità previste dalla L. 71/2017. Si rimanda inoltre agli allegati al cap.5 del presente documento.

Le potenziali infrazioni alla E-policy da parte del personale scolastico sono identificabili in:

- utilizzo delle tecnologie e della strumentazione della Scuola non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- diffusione delle password assegnate e custodia non adeguata degli strumenti e degli accessi di cui possano approfittare terzi;
- mancata sorveglianza che possa favorire un utilizzo non autorizzato delle TIC da parte degli alunni; mancato pronto intervento dinanzi a palesi o sospetti episodi di infrazione.

Eventuali infrazioni nell'uso del device o della Rete compiute dal personale scolastico saranno gestite dal Dirigente Scolastico, secondo quanto previsto dal Codice di comportamento dei dipendenti pubblici (GU n.129 del 4-6-2013), dal CCNL (29 novembre 2007), dal DPCM (28 novembre 2000), dal Codice disciplinare e dalla normativa in vigore inerente alla privacy.

Tra le iniziative familiari meno favorevoli va annoverata:

- una piena autonomia concessa al proprio figlio nella navigazione sul Web e nell'utilizzo dei devices personali, e/o il mancato dialogo rispetto alle problematiche oggetto di questo documento.

I genitori degli/lle studenti/esse possono essere convocati a Scuola da parte del Coordinatore di classe o del Dirigente scolastico per concordare misure educative sanzionatorie.

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 documento di E-policy dialoga e si armonizza con gli altri regolamenti vigenti

nell'Istituto, integrandosi pienamente con gli obiettivi enunciati nel PTOF, con il Regolamento di Istituto, con il Patto educativo di corresponsabilità controfirmato da Scuola, genitori e studenti all'atto dell'iscrizione, con il Piano scolastico per la didattica digitale integrata nel quale vengono individuati criteri e modalità di rimodulazione dell'attività didattica in regime di DDI.

Tra le integrazioni si segnalano:

- qualsiasi azione di hacking ai danni del registro elettronico e/o del sito della scuola (violazione e/o diffusione delle credenziali,alterazione, danneggiamento, cancellazione di dati o software…), anche ai fini della falsificazione;
- qualsiasi azione di hacking ai danni delle reti d'Istituto (violazione e/o diffusione delle credenziali, alterazione, danneggiamento, uso delle reti per scopi o attività sanzionate dalla legge o comunque non previste dai Regolamenti specifici);
- qualsiasi azione di hacking ai danni di oggetti, di hardware, periferiche e software delle apparecchiature informatiche dell'Istituto;
- qualsiasi azione di hacking ai danni dell'identità e degli orientamenti sessuali;
- atti ascrivibili a sexting e pedopornografia.

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 monitoraggio e l'eventuale aggiornamento del documento è a cura del Dirigente Scolastico, coadiuvato dall'Animatore Digitale, dal Referente per il bullismo e il cyberbullismo, dal Team per il contrasto al bullismo e al cyberbullismo, previa raccolta di feedback provenienti dalla comunità educante tutta.

L'IIS "De Sarlo- De Lorenzo" si impegna a valutarne l'incidenza e l'efficacia con cadenza annuale e ogni qual volta si dovessero verificare rilevanti variazioni in merito alla dotazione digitale della Scuola oppure si rendessero necessari adeguamenti alla

normativa ministeriale sul tema.

L'efficacia del documento sarà testata con particolare riferimento agli obiettivi in esso esplicitati:

- promozione delle competenze digitali e dell'uso delle TIC nei percorsi educativi e didattici;
- prevenzione e gestione dei rischi connessi alla Rete;
- tutela del benessere socio- relazionale delle studentesse e degli studenti.

Il nostro piano d'azioni

Azioni da svolgere nei prossimi tre anni:

- Organizzare 1 evento di presentazione e conoscenza dell'E-policy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'E-policy rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'E-policy rivolto ai genitori

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali".

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

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale.

L'Istituto ha sviluppato, da qualche anno, un curricolo digitale per gli studenti/studentesse; supporta altresì con corsi di formazione e risorse di varia natura i docenti.

Una particolare attenzione verrà dedicata, a partire dal prossimo anno scolastico, allo sviluppo di abilità socio-comunicative e partecipative: lo scopo è quello di acquisire la necessaria consapevolezza dei propri doveri nei confronti di coloro con cui comunichiamo online.

In altri termini, vanno evidenziati con chiarezza i danni provocati, agli altri ma anche a sè stessi, attraverso un uso inadeguato, se non scorretto, della Rete.

Il curricolo sulle competenze digitali per gli studenti è trasversale alle discipline previste dal piano di studi ed incentrato su cinque aree operative individuate dal "Quadro comune di riferimentoeuropeo per le competenze digitali" (DIGCOMP), come

di seguito riportato:

- Alfabetizzazione su informazioni e dati
- Comunicazione e collaborazione
- Creazione di contenuti digitali
- Sicurezza
- Risolvere problemi

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

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

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

Il corpo docente del nostro Istituto utilizza con frequenza e sistematicamente le TIC nella didattica. L'uso delle stesse è previsto e pianificato nei programmi annuali.

All'interno delle singole discipline vengono individuati moduli didattici integrati con le TIC. Si utilizzano anche specifici software didattici, oltre che video e presentazioni multimediali.

Negli ultimi due anni sono stati sostenuti corsi di aggiornamento ad hoc. L'Istituto beneficia degli effetti positivi di tali corsi e ne valuta costantemente l'impatto sull'attività di studio.

L'esperienza suddetta deve rappresentare uno stimolo per dare carattere permanente a tale processo di aggiornamento, in modo da rendere le conoscenze diffuse e condivise all'interno del corpo docente.

Le modalità possono comprendere fasi di formazione collettiva ma anche fasi di autoformazione: a tal fine, sarà importante incentivare la partecipazione dei docenti a tutte le inziative di formazione, promosse a livello ministeriale, di ''scuole-polo'' ed anche di singola istituzione scolastica.

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.

Il corpo docente ha seguito, in questi anni, corsi di aggiornamento sull'utilizzo sicuro e positivo di Internet e delle tecnologie digitali, che hanno portato allo sviluppo di una programmazione specifica e consequenziali attività didattiche.

Tale esperienza non deve ritenersi conclusa, anzi va intensificata , dando un ruolo rilevante alla sfera emotiva e affettiva degli studenti e delle studentesse che usano le nuove tecnologie.

In tal modo si forniscono, ai docenti, strumenti decisivi per poter formare ragazzi e ragazze in merito alla modulazione e gestione dei propri ed altrui comportamenti, favorendo e promuovendo così forme di convivenza civile.

Il successo di tali iniziative dipende poi, in larga misura, dalla capacità di coinvolgere le famiglie insieme agli studenti ed alle studentesse. Laboratori, progetti specifici, giornate a tema appaiono modalità idonee allo scopo.

Una buona base di partenza può essere rappresentata dall'analisi del fabbisogno formativo del corpo docente, riguardo, per esempio, ad argomenti specifici avvertiti

come particolarmente importanti; in un secondo momento tale analisi va estesa alle richieste in merito provenienti dagli studenti e dalle studentesse.

Un possibile schema di lavoro potrebbe essere il seguente :

- analizzare il fabbisogno formativo degli insegnanti sull'uso sicuro della Rete;
- analizzare le richieste degli studenti e studentesse;
- promuovere la partecipazione dei docenti a corsi di formazione;
- monitorare le azioni svolte per mezzo di specifici momenti di valutazione;
- organizzare incontri con professionisti della scuola o con esperti esterni, enti/associazioni, etc.

Opportuna appare la predisposizione di un'area specifica sul sito dell'Istituto con materiali formativi per gli insegnanti.

2.4. - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

Il nostro Istituto, nell'intento di favorire un'azione congiunta fra scuola e famiglia, si impegna a garantire la più ampia informazione possibile su tutte le attività ed iniziative intraprese in relazione al tema delle tecnologie digitali, previste dall'E-policy e dal suo piano di azioni.
Di conseguenza, il presente documento è messo a disposizione di tutta la comunità scolastica e delle famiglie sul sito web dell'Istituto, insieme al Patto educativo di

corresponsabilità.
Con tale documento scuola e famiglia assumono l'impegno a collaborare nel processo di formazione di studenti e studentesse in riferimento ai temi legati alla E-policy.
L'Istituto intende valorizzare le opportunità di incontro e formazione per le famiglie su tali temi, individuando iniziative significative promosse da Enti e/o Associazioni presenti sul territorio.

Il nostro piano d'azioni

AZIONI da svolgere nei prossimi tre anni:

- Effettuare un’analisi del fabbisogno formativo del corpo docente sull’utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare e promuovere per il corpo docente incontri formativi sull’utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i genitori sull’educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

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

(cfr. http://www.garanteprivacy.it/scuola).

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

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

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

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare

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

In merito alla protezione dei dati personali, si fa riferimento a quanto previsto dal Decreto Legislativo del 30 giugno 2003, n.196 (cosiddetto Codice della Privacy), integrato dal D.Lgs. 10 agosto 2018, n. 101, e dal GDPR (General Data Protection Regulation) n. 679 del 2016. All'atto dell'iscrizione viene fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli studentii e delle studentesse eccedenti i trattamenti istituzionali obbligatori, come ad esempio l'utilizzo di fotografie, video o altri materiali audiovisivi contenenti l'immagine e/o il nome del proprio figlio/a all'interno di attività educative e didattiche per scopi documentativi, formativi e informativi, durante gli anni di frequenza della scuola. A tale proposito si evidenzia che le immagini e le riprese audiovideo realizzate dalla scuola, nonché gli elaborati prodotti dagli studenti durante le attività scolastiche, potranno essere utilizzati esclusivamente per documentare e divulgare le attività della scuola tramite il sito Internet di Istituto. L'autorizzazione non consente l'uso dell'immagine in contesti che pregiudichino la propria dignità personale ed il decoro e comunque per uso e/o fini diversi da quelli sopra indicati.Inoltre, in caso di partecipazioni a concorsi o manifestazioni l'Istituto richiede apposita autorizzazione, chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato all'interno di modulistica o sul proprio sito web istituzionale. La formula utilizzata per chiedere il consenso è, in ogni caso, comprensibile, semplice e chiara. Pertanto, in ottemperanza al GDPR (General Data Protection Regulation) e al D. Lgs. 10 agosto 2018, n. 101, la scuola non si impegna solo a tutelare la privacy degli/lle studenti/esse e delle loro famiglie, ma anche ad informare e soprattutto rendere consapevoli gli/le studenti/esse di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri.

Inoltre si richiede:

- la predisposizione e condivisione con l'intera comunità scolastica di un'informativa che illustri il ruolo del DPO (Data Protection Officer),in italiano RPD (responsabile della protezione dei dati), la tipologia di dati raccolti, il loro utilizzo e il fine per cui vengono utilizzati;
- la messa a disposizione dei genitori sul sito istituzionale del modello di reclamo al Garante per la protezione dei dati personali in caso di violazioni in materia di cyberbullismo;
- la regolamentazione sull'uso di dispositivi in grado di registrare e di strumenti compensativi previsti nei PDP/PEI.
- la definizione, sul sito istituzionale della scuola, di una specifica sezione dedicata al Documento di E-policy;
- di allegare all'E-policy i modelli di liberatoria che l'Istituto utilizza o intende utilizzare, modelli che devono essere conformi alla normativa vigente, in

materia di protezione dei dati personali;
- Pubblicazione, nella sezione Privacy, dei dati del DPO (nominativo, PEO, PEC, riferimento telefonico).

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.

Il Piano Nazionale per la Scuola Digitale (PNSD), adottato con Decreto Ministeriale n. 851 del 27 ottobre 2015, è un documento pensato per guidare le scuole in un percorso di innovazione e digitalizzazione. Il PNSD prevede interventi specifici, promossi e coordinati dall'Animatore Digitale, in merito alla formazione degli insegnanti, al miglioramento delle dotazioni hardware, fino alle attività didattiche. Per quanto riguarda la formazione, l'Animatore promuoverà la partecipazione a seminari, convegni, corsi on-line organizzati dagli Enti del territorio, dalle scuole in rete che partecipano al PNSD, da esperti interni e esterni alla Scuola. Tali interventi saranno rivolti tutti/e i/le docenti e a quelli/e che avranno un profilo di accesso personale al sito, con il quale contribuiranno ad alimentare i contenuti didattici dello stesso; al personale amministrativo, dotato di un profilo di accesso personale al sito, che gestirà la comunicazione delle circolari e il registro elettronico; ai collaboratori scolastici, in primo piano nella comunicazione con gli utenti della scuola; alle famiglie, destinatarie di servizi on line.. Il processo avverrà in modo graduale.. E' importante creare un ambiente sicuro anche online. Esistono due termini per parlare di sicurezza: il primo termine è safety e riguarda la prevenzione dei rischi, l'altro termine è security che, in relazione ad Internet e ai media, si riferisce a tutte quelle risorse tecnologiche che rendono sicuro l'ambiente digitale. Al fine di garantire la safety nell'accesso ad Internet gli studenti saranno guidati allo sviluppo di competenze digitali per un uso consapevole delle TIC e della RETE e al rispetto della "netiquette" (insieme di regole, comunemente accettate e seguite da quanti utilizzano Internet e i servizi di rete, che disciplinano il comportamento di un utente nel rapportarsi agli altri utenti attraverso risorse come wiki, newsgroup, mailing list, forum, blog o email). L'Istituto si propone di dotarsi di una PUA (Politica d'uso accettabile e sicura della rete): norme di buon utilizzo che la scuola si impegna a redigere e a divulgare prima che sia concesso l'accesso a Internet alla componente studentesca. La security sarà invece implementata attraverso l'adozione delle seguenti misure cautelative:

- mantenere separate le reti didattica e segreteria: importante per garantire maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le due reti grazie al firewall;
- aggiornare periodicamente software e Sistema operativo: garantire che il sistema sia aggiornato lo protegge dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo;
- definire la programmazione di backup periodici: cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi (possibilmente anche una copia offline);
- garantire formazione adeguata allo staff, incluso il corpo docenti: la formazione deve riguardare la gestione dei dispositivi, la conoscenza delle regole basilari sulla sicurezza;
- testare regolarmente le possibili vulnerabilità;
- preparare piani di azione in risposta ai problemi più seri: è importante non dover improvvisare nel momento in cui si verifica un problema serio, ma avere un protocollo di azione;
- predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo

di inutilizzo: se non è previsto uno stand-by, il dispositivo resta accessibile nel caso in cui qualcuno dimentichi di spegnerlo, con il rischio potenziale di accesso da parte di persone non autorizzate;

- impostare il browser per l'eliminazione dei cookies alla chiusura: in questo modo si evita che qualcuno possa avere accesso ad account altrui senza autorizzazione;
- definire una policy sulle password: le password devono essere forti: richiedere password complesse con almeno 8 caratteri con numeri, maiuscole e minuscole e caratteri speciali; sensibilizzare rispetto al non uso di password facilmente identificabili (nomi dei figli, compleanni, etc.); non memorizzare le password nei dispositivi scolastici; non condividere le password con nessuno;
- minimizzare i privilegi amministrativi: solo poche persone autorizzate dovrebbero avere privilegi amministrativi. Studenti e la maggior parte dei docenti possono accedere con account con permessi limitati;
- sviluppare il regolamento sull'uso delle tecnologie a scuola (policy di uso accettabile): deve riguardare chiunque abbia accesso alla Rete, studenti/esse, docenti, amministrazione e segreteria, includere i dispositivi della scuola e quelli personali, anche in caso di BYOD (Bring Your Own Device).

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.

Il Nostro Istituto si avvale di diversi strumenti di comunicazione, per trasmettere l'identità, i valori, le azioni, i progetti e l'idea di educazione che porta avanti.

E' stato individuato un docente responsabile del Sito Web che risponde a specifici regolamenti approvati dal Consiglio di Istituto.

Un altro mezzo di comunicazione online in dotazione alla scuola è il registro elettronico con tutte le sue funzionalità.. Esso consente una comunicazione chiara e immediata con le famiglie relativamente a:

- andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);
- risultati scolastici (voti, documenti di valutazione);
- udienze (prenotazioni colloqui individuali);
- eventi (agenda eventi);
- comunicazioni varie (comunicazioni di classe, comunicazioni personali). Tutte le comunicazioni scuola-famiglia contenenti dati sensibili sono visibili da parte della famiglia dell'alunno interessato e non dal resto della classe. Solo il DS e i docenti del CdC possono avere accesso a tali informazioni. Il riepilogo delle medie con relative valutazioni ed eventuali assenze è accessibile sul registro elettronico Spaggiari dal profilo dei Coordinatori di classe.

Inoltre, attraverso l'account a dominio è possibile l'accesso in cloud a tutta una serie di applicazioni incluse in Microsoft 365, che, nel loro insieme, costituiscono il sottosistema informatico per la comunicazione e la collaborazione.. Agli studenti e a tutto il personale della scuola è stato assegnato un account per il dominio dell'Istituto: nome.cognome@iisdesarlo.education Alle famiglie sarà inviata l'informativa riguardo l'uso e le caratteristiche del Documento di E-policy, Per la messaggistica istantanea testuale o in videocall (docenti-docenti e docenti-genitori) si utilizzeranno Chat della piattaforma in uso (Teams). Sia per la DDI che per le riunioni in modalità telematica sono stati predisposti specifici regolamenti approvati dagli organi collegiali competenti.

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 da Regolamento d'Istituto agli studenti e alle studentesse è fatto assoluto divieto di usare all'interno dell'Istituto scolastico, se non per scopi esclusivamente didattici autorizzati dal/la docente, smartphone e/o ogni altro apparato multimediale (walkman, mp3, ipod, ipad, notebook, fotocamera, videocamera, ecc…). Il divieto non si applica soltanto all'orario delle lezioni, ma all'intera permanenza dello studente all'interno della struttura scolastica (intervalli, pausa …). I predetti dispositivi devono essere tenuti spenti e opportunamente custoditi e depositati in borsoni, zaini, giacconi. Al personale docente è' consentito l'uso di dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili. Le medesime disposizioni valgono anche per il personale ATA della scuola.

Il nostro piano d'azioni

AZIONI da svolgere nei prossimi tre anni:

- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

Capitolo 4 - Rischi on line: conoscere, prevenire e rilevare

4.1 - Sensibilizzazione e Prevenzione

Il rischio online si configura come la possibilità per il minore di:

- commettere azioni online che possano danneggiare se stessi o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e contenerli, ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. Ciò è possibile lavorando su aspetti di ampio raggio che possano permettere una riduzione dei fattori di rischio e di conseguenza una minore probabilità che i ragazzi si trovino in situazioni non piacevoli. È importante che abbiano gli strumenti idonei per riconoscere possibili situazioni di rischio e segnalarle ad un adulto di riferimento.

Gli strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio si configurano come interventi di **sensibilizzazione e prevenzione.**

- Nel caso della **sensibilizzazione** *si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.*
- Nel caso della **prevenzione** *si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.*

A partire dall'anno scolastico 2022/23, oltre i corsi di aggiornamento già effettuati dal corpo docente, il nostro Istituto si prefigge di promuovere altre attività riguardanti la sensibilizzazione e la prevenzione, a proposito della quale si possono individuare tre livelli:

- "La prevenzione universale", con programmi ad ampio raggio, poichè parte dal presupposto che tutti gli studenti e le studentesse sono potenzialmente a rischio.
- "La prevenzione selettiva", dedicata ad un gruppo di studenti/esse in cui il rischio online è presente.
- "La prevenzione indicata" che prevede un programma di intervento sul caso specifico.

Attività relative alla sensibilizzazione:

- Incontri periodici, anche con esperti esterni, con gli studenti e le studentesse riguardanti i rischi online finalizzati ad accrescere la consapevolezza circa il problema e la motivazione al cambiamento.
- Attività laboratoriali da svolgere nelle singole classi volte ad incoraggiare il gruppo a modificare il proprio comportamento sull'uso del digitale.

Attività relative alla prevenzione:

- "Prevenzione universale": progetti atti a promuovere le competenze digitali ed informare sui rischi connessi all'uso della Rete; azioni di contrasto al cyberbullismo e agli altri rischi online (come descritto nei paragrafi successivi).
- "Prevenzione selettiva": in questo caso si adotteranno interventi mirati verso quel gruppo di studenti/esse in cui il rischio è presente, coinvolgendo il Dirigente Scolastico, il docente referente sul cyberbullismo, i docenti della classe, altre figure esterne di riferimento e le famiglie interessate. La responsabilità di alcune azioni legate ad un uso improprio della Rete può ricadere anche sul Dirigente ("culpa in organizzando"), sui docenti (" culpa in vigilando"), sui genitori ("culpa in educando").
- " Prevenzione indicata": per quest'ultimo livello di prevenzione si attuerà un programma di intervento sul caso specifico, con il supporto di professionalità diverse, in quanto affronta problemi legati alla salute mentale del minore.

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).

In relazione al bullismo e al cyberbullismo all'interno dell'Istituto è stato individuato un docente Referente, che collabora con il Dirigente Scolastico e con altri insegnanti e figure di riferimento esterne, al fine di stilare e/o integrare i regolamenti specifici. Tale docente promuove attività atte a sensibilizzare gli studenti e le studentesse sul fenomeno del cyberbullismo, monitorato anche attraverso la somministrazione annuale di un questionario anonimo. Lo stesso docente collabora con agenzie, istituzioni e autorità locali. Inoltre è attivo uno sportello di ascolto. L'Istituto promuove l'utilizzo del servizio, la cui attività è nota a tutta la comunità scolastica.Tale servizio potrà essere utile anche per individuare situazioni problematiche legate al cyberbullismo e agli altri rischi online. Le figure professionali che operano presso lo sportello di ascolto lavorano in stretta collaborazione con gli altri servizi del territorio e di ascolto per bambini/e e adolescenti.

A partire dall'anno scolastico 2022/23, da parte di tutti i docenti, sarà avviata una maggiore attività di osservazione della popolazione studentesca, per valutare bisogni e

potenzialità. Si programmeranno UDA trasversali a tutte le discipline, nel contesto dell'Educazione civica, finalizzate ad una maggiore conoscenza del cyberbullismo in tutte le sue forme e conseguenze: cyberbullismo diretto e indiretto, effetti sulle vittime, responsabilità del gruppo silente (" bystander "), modalità di intervento. La visione di filmati e video interattivi sul fenomeno in esame potrà maggiormente invogliare gli studenti e le studentesse a riflettere sulle loro azioni, spesso inconsapevoli, a confrontarsi e a modificare i propri comportamenti.

La realizzazione di percorsi formativi e l'attività di sensibilizzazione sul bullismo e il cyberbullismo è prevista anche dalla Legge 71/2017 che pone al centro il ruolo dell'istituzione scolastica in merito alla prevenzione e al contrasto di tale fenomeno. La stessa legge indica pure provvedimenti a carattere amministrativo: chi compie atti di bullismo e cyberbullismo può essere responsabile di reati penali e danni civili. Pertanto, le azioni intraprese dalla scuola in merito a questa tematica si ritengono opportune e potranno risultare efficaci con il coinvolgimento di tutta la comunità scolastica, studenti, studentesse, docenti e famiglie.

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.

L'insieme delle pratiche che esprimono odio o intolleranza verso un gruppo o una persona identificata avviene nella maggior parte dei casi attraverso l'uso di Internet. Dal momento che il termine " Hate speech " indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità ecc...), tale fenomeno è correlato al tema delle diversità e in senso più ampio al rispetto dei diritti umani che nel discorso d'odio risultano violati.

L'IIS " De Sarlo- De Lorenzo " ha sempre prestato attenzione a questa tematica (nell'Istituto sono presenti studenti/esse di nazionalità straniera, di differenti culture, lingue e religioni, altri con disabilità di varia natura). Sono previsti annualmente una serie di incontri e dibattiti e specifiche attività di comunicazione per la promozione delle iniziative presso gli/le studenti/esse. Inoltre è stata individuata, tra il personale, una figura incaricata di curare e coordinare gli interventi rivolti al rispetto delle diversità a scuola, a cui tutto il personale può fare riferimento per segnalare e proporre a sua volta la partecipazione a iniziative esterne.

Sul fenomeno specifico dell'hate speech, l'Istituto si prefigge di fornire agli studenti e alle studentesse gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di incitamento all'odio, promuovendo la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network. Si ritiene opportuna una riflessione sull'uso corretto e consapevole del linguaggio tra pari, anche attraverso attività laboratoriali, dibattiti e discussioni nelle classi. L'Istituto si avvarrà, ove necessario, anche di consulenti/esperti esterni (Carabinieri, Polizia Postale, associazioni del territorio preposte allo scopo) per organizzare incontri formativi rivolti a docenti, studenti, studentesse e genitori.

4.4 - Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

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

La dipendenza da Internet, che può manifestarsi anche attraverso le ore trascorse

online a giocare, rappresenta una questione importante per la comunità scolastica, che deve rivolgere grande attenzione al fenomeno e fornire adeguati strumenti agli studenti e alle studentesse affinchè questi siano consapevoli dei rischi che comporta l'iperconnessione. E' importante non demonizzare l'uso di strumenti tecnologici o il gioco online, ma cercare di entrare nel mondo degli studenti e delle studentesse promuovendo un uso consapevole della tecnologia per favorire il " benessere digitale", ossia la capacità di creare e mantenere una relazione sana con essa.

Il nostro Istituto, pertanto, si prefigge quanto segue:

- stutturare regole condivise e stipulare con gli studenti e le studentesse una sorta di " patto d'aula", proponendo delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d'aula (adoperando, per esempio, la LIM o il dispositivo personale);
- dedicare al tema un momento specifico e riflettere con studenti e studentesse per fare in modo che la tecnologia non sia solo distrazione, ma uno strumento utile per raggiungere i propri obiettivi;
- creare una didattica per competenze trasversali, discutendo di cittadinanza digitale, di cyberbullismo, di uso integrativo e non sostitutivo dei dispositivi e della Rete;
- condividere e concordare con la famiglia un percorso educativo sull'uso corretto ed equilibrato della Rete.

4.5 - Sexting

Il “sexting” è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti mediali sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

Il sexting (abbreviazione di sex-sesso e texting-messaggiare, inviare messaggi) indica l'invio e/o la ricezione di contenuti sessualmente espliciti (immagini o video spesso realizzati con il cellulare, tramite il quale vengono diffuse nella maggior parte dei casi), che ritraggono se stessi e gli altri. Tali immagini o video, anche se inviate ad una stretta cerchia di persone, possono diffondersi in modo incontrollabile e creare seri problemi, sia personali che legali, alla persona ritratta. L'invio di foto che raffigurano minorenni in pose sessualmente esplicite configura non solo il reato di " distribuzione di materiale pedopornografico", ma può diventare motivo di ricatto, assumendo la forma di " revenge porn", letteralmente " vendetta porno ", fenomeno

quest'ultimo che consiste nella diffusione illecita di contenuti sessuamente espliciti al fine di ricattare l'altra parte (il reato di " revenge porn" è stato introdotto nella Legge 19 luglio 2019 n.69, art.10).

Il fenomeno del sexting presenta principalmente le seguenti caratteristiche:

- la fiducia tradita: chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta;
- la pervasività con cui si diffondono i contenuti in pochi istanti attraverso una condivisione che diventa virale anche su differenti piattaforme. Il contenuto, così, può essere 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.

La consapevolezza o comunque la sola idea di diffusione di contenuti personali, si replica nel tempo e può finire con il danneggiare, in termini psicologici e sociali, sia i soggetti delle foto/video sia colui/coloro che hanno contribuito alla diffusione.

Considerata l'importanza e la complessità di tale fenomeno, il nostro Istituto ritiene opportuno sensibilizzare tutta la comunità scolastica su questo tema, anche con il supporto esterno di esperti e figure professionali presenti nel nostro territorio che operano in tale settore.

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.

In merito a tale problematica, i docenti del nostro Istituto intendono approfondire la conoscenza del fenomeno, imparando a riconoscerne i segnali e individuando le modalità di intervento.

Come riconoscerlo?

Per riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli segnali che possono essere indicatori importanti, come ad esempio un improvviso cambiamento nel comportamento di uno/a studente/essa, la tendenza ad isolarsi totalmente dal gruppo ed essere coinvolto solo da una relazione online, le allusioni sessuali o le prese in giro da parte dei compagni, l'imbarazzo e la preoccupazione ad affrontare l'argomento anche in modo generico.

L'importanza di un'adeguata educazione all'affettività e alla sessualità

Il miglior modo per prevenire casi di adescamento online è accompagnare studenti e studentesse in un percorso di educazione (anche digitale) all'affettività e alla sessualità, se possibile pure attraverso progetti PCTO. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innazitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. E' molto importante, inoltre, che gli/le studenti/esse sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver commesso un errore, provano vergogna e si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinchè ciò avvenga, è necessario tenere sempre aperto un canale di comunicazione con gli/le studenti/esse sui temi dell'affettività, del digitale e, se possibile, della sessualità.

Pertanto, risulta fondamentale promuovere un percorso di educazione digitale che comprenda anche lo sviluppo di capacità, quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, allo scopo di riuscire a gestire adeguatamente le proprie relazioni online.

Come intervenire?

Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innazitutto, che l'adulto di riferimento non si sostiuisca al minore nel rispondere, ad esempio, all'adescatore. Inoltre non bisogna utilizzare il computer o altri dispositivi elettronici della vittima al fine di non compromettere eventuali prove.

Casi di adescamento online richiedono l'intervento della Polizia Postale e delle

Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video...). Inoltre, considerato che l'adescamento è una problematica molto delicata da gestire, poichè può avere ripercussioni psicologiche significative sul minore, sarà necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile...), in grado di fornire alla vittima un adeguato supporto sotto questo aspetto. Nei casi estremi in cui l'adescamento porta ad un incontro fisico e ad un abuso sessuale, un sostegno psicologico esperto per il minore è da considerarsi prioritario e urgente.

Per consigli e/o per un supporto è possibile rivolgersi alla Helpline di Generazioni Connesse (19696): operatori esperti e preparati sono sempre a disposizione del Dirigente, degli insegnanti, degli operatori scolastici, degli studenti e delle studentesse, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali problematiche inerenti l'utilizzo dei nuovi media e i rischi online.

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.

Se nel nostro Istituto si ravvisasse un rischio per il benessere psicofisico degli studenti e delle studentesse coinvolti nella visione di contenuti pedopornografici, si renderà opportuno ricorrere alle autorità competenti (Polizia di Stato, Compartimento di Polizia Postale e delle Comunicazioni, Questura, Arma dei Carabinieri, Comando Provinciale o Stazione del territorio di competenza), provvedendo contestualmente a fornire un supporto psicologico e consultando il medico di base o pediatra di riferimento.

Anche in tale contesto risulta molto utile l'attività educativa sull'affettività e le relazioni, sottolineando sempre la necessità di rivolgersi ad un adulto quando qualcosa online crea disagio. In un'ottica di interventi preventivi, il tema della pedopornografia è estremamente delicato; occorre parlarne sempre in considerazione della maturità e della fascia d'età, selezionando il tipo di informazioni che si possono condividere e considerando che serve a chiarire anche alcuni aspetti legati alle conseguenze del sexting.

Inoltre è auspicabile che possa rientrare nelle tematiche di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico, promuovendo i servizi della hotline.

Il nostro piano d'azioni

AZIONI da svolgere nei prossimi tre anni:

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

.

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.

I minori potrebbero riferire all'insegnante fatti o eventi personali o altrui, accaduti anche al di fuori della scuola, che potrebbero mettere in allarme il docente. Pertanto sono da segnalare:

- contenuti afferenti alla violazione della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);
- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, frasi che istigano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

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.

L' IIS "De Sarlo- De Lorenzo" ha individuato i/le docenti del Team Anti Bullismo e Cyberbullismo che faranno da supporto agli altri docenti nella formazione e il monitoraggio degli eventuali casi e i docenti del Team per l'Emergenza che valuteranno in maniera approfondita le segnalazioni e sceglieranno la strategia di intervento più opportuna. In relazione al CASO A (SOSPETTO), è opportuno che i docenti coinvolgano il Referente d'Istituto per il contrasto del bullismo e del cyberbullismo, al fine di valutare le possibili strategie d'intervento. Si potrebbe pensare anche alla possibilità di avvisare l'intero consiglio di classe e, se si ravvisa la necessità e l'urgenza, di coinvolgere il Dirigente Scolastico. Nel frattempo, il/la docente (e i/le docenti informati) ascolta gli studenti e le studentesse, osservando e monitorando il clima di classe, ciò che accade, le dinamiche relazionali nel contesto classe, senza fare indagini dirette. Uno strumento utile per raccogliere informazioni può essere il diario di bordo (allegato alla presente E-policy). Inoltre, il docente deve cercare di capire se gli episodi sono circoscritti al gruppo o se interessano l'intero Istituto. Operativamente è fondamentale coinvolgere tutti gli studenti e le studentesse, informandoli sui fenomeni e sulle caratteristiche degli stessi, suggerendo di chiedere aiuto se pensano di vivere situazioni, di subire atti identificabili come bullismo o cyberbullismo.

In relazione al CASO B (EVIDENZA), il docente deve condividere immediatamente quanto osservato con il Referente per il bullismo e il cyberbullismo, attraverso il MODULO DI PRIMA SEGNALAZIONE c h e deve essere compilato e consegnato all'indirizzo mail PZIS001007@istruzione.it all'attenzione del referente bullismo, per

valutare insieme le possibili strategie di intervento. Si avvisa anche il Dirigente Scolastico che convoca il Consiglio di Classe. Se non si ravvisano fattispecie di reato, è opportuno:

- informare i genitori (o chi esercita la responsabilità genitoriale) degli/delle studenti/studentesse direttamente coinvolti/e (qualsiasi ruolo abbiano avuto), se possibile con la presenza di professionisti dell'aiuto, per strategie condivise e modalità di supporto;
- creare momenti di confronto costruttivo in classe, con la presenza di figure specialistiche territoriali;
- informare i genitori degli/delle studenti/studentesse infra-quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al Garante della Privacy);
- informare gli/le studenti/studentesse ultraquattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al Garante della Privacy);
- convocare il Consiglio di Classe;
- valutare come coinvolgere gli operatori scolastici su quello che sta accadendo.

A seconda della situazione e delle valutazioni effettuate con Referente, Dirigente e genitori, si potrebbe poi segnalare alla Polizia Postale, ove necessario, ai sensi di legge:

- contenuto del materiale online offensivo;
- modalità di diffusione;
- attispecie di reato eventuale.

Se è opportuno, richiedere un sostegno ai servizi e alle associazioni territoriali o ad altre autorità competenti. E' bene sempre dialogare con la classe, attraverso interventi educativi specifici, cercando di sensibilizzare studenti e studentesse sulla necessità di non diffondere ulteriormente online i materiali dannosi, ma anzi di segnalarli e bloccarli.

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.

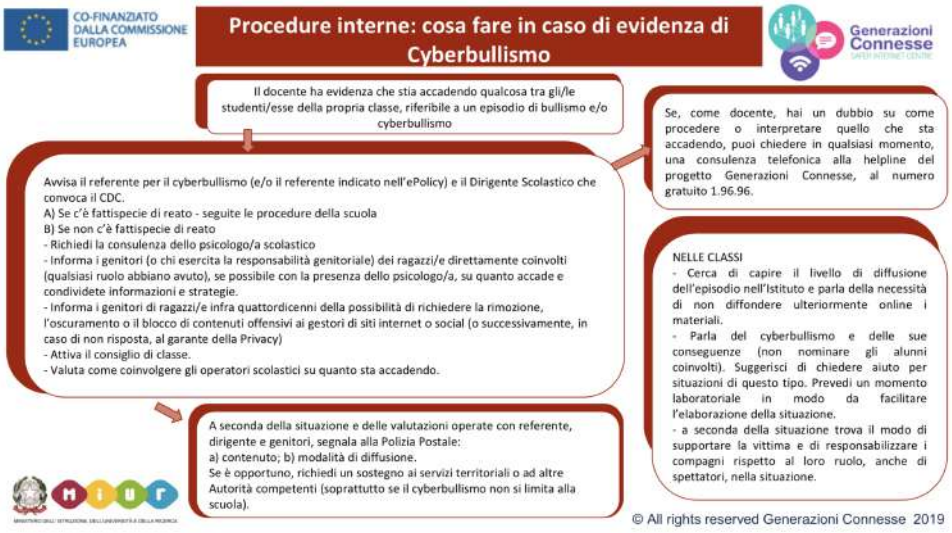
Al fine di prevenire episodi di bullismo/cyberbullismo e diffondere consapevolezza su questi temi, l'IIS "De Sarlo-De Lorenzo" organizza incontri con esperti ed eventi formali rivolti a tutti gli Studenti/Studentesse, Docenti e Genitori, come, ad esempio, iniziative legate alla Giornata contro il bullismo e cyberbullismo, o UDA di Educazione Civica e progetti PCTO.

Nei casi di maggiore gravità, si valuterà anche il coinvolgimento di attori esterni quali Forze dell'ordine e Servizi sociali. I documenti relativi alle procedure operative e i

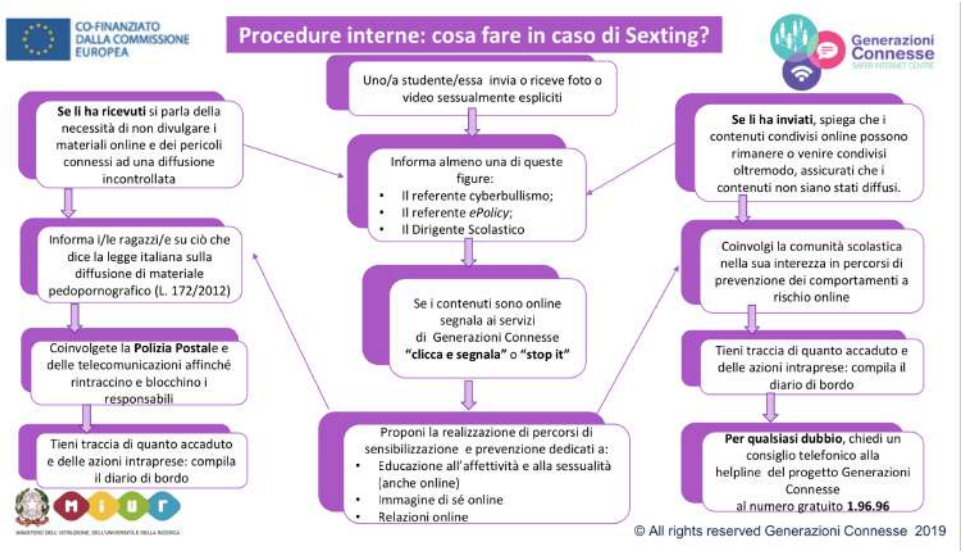
protocolli sono da elaborare in collaborazione con i suddetti attori del territorio, con cui siglarli unitamente.

5.4. - Allegati con le procedure

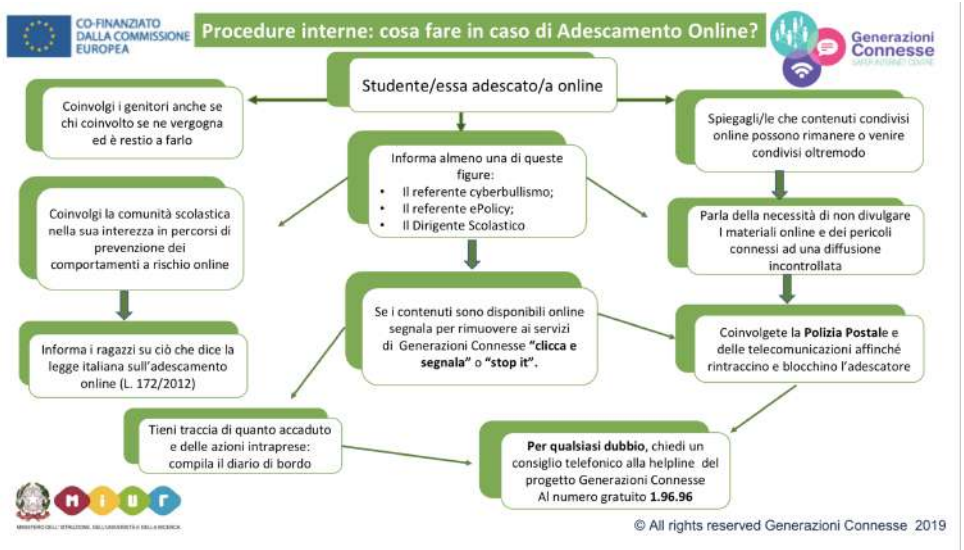
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



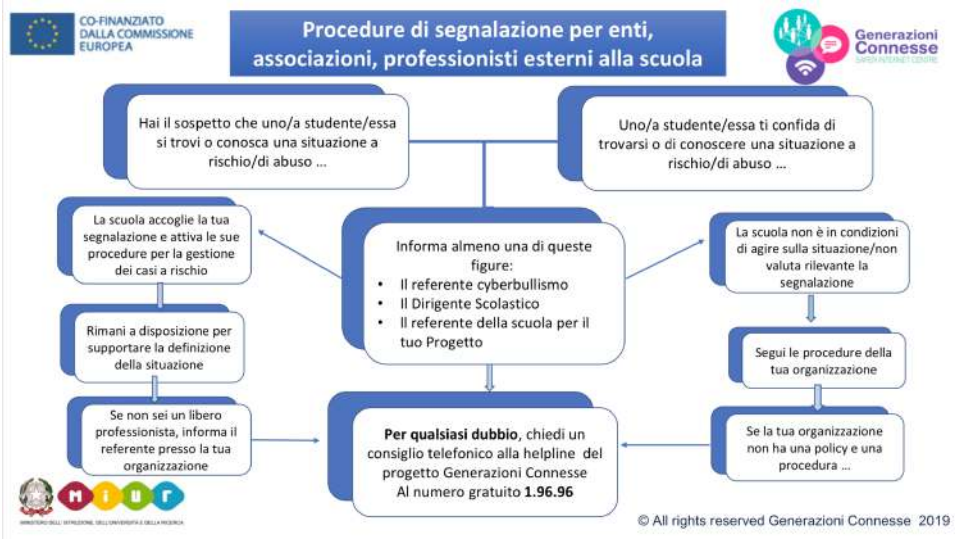
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il nostro piano d'azioni

Non è prevista alcuna azione.