ISTITUTO STATALE DI ISTRUZIONE SUPERIORE
"Leopoldo II di Lorena"
Via de Barberi - 58100 Grosseto Tel.
0564/484821 Via Meda – Giolitti 58100 Grosseto Tel.
0564/484881
E - mail: gris00600c@istruzione.it - PEC: gris00600c@pec.istruzione.it

Documento di ePolicy

GRIS00600C

ISIS LEOPOLDO II DI LORENA

VIA DE' BARBERI S.N.C. - 58100 - GROSSETO

Approvato con delibera del
Consiglio di Istituto del 9 ottobre 2024

Capitolo 1
Introduzione

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'ePolicy, 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'ePolicy 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 online 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

1. **Presentazione dell'ePolicy**
    1. Scopo dell'ePolicy
    2. Ruoli e responsabilità
    3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
    4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
    5. Gestione delle infrazioni alla ePolicy
    6. Integrazione dell'ePolicy con regolamenti esistenti
    7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
2. **Formazione e curricolo**
    1. Curricolo sulle competenze digitali per gli studenti
    2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
    3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
    4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
    1. Protezione dei dati personali
    2. Accesso ad Internet
    3. Strumenti di comunicazione online
    4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
    1. Sensibilizzazione e prevenzione
    2. Cyberbullismo: che cos'è e come prevenirlo
    3. Hate speech: che cos'è e come prevenirlo
    4. Dipendenza da Internet e gioco online
    5. Sexting
    6. Adescamento online
    7. Pedopornografia
5. **Segnalazione e gestione dei casi**
    1. Cosa segnalare
    2. Come segnalare: quali strumenti e a chi
    3. Gli attori sul territorio per intervenire
    4. Allegati con le procedure

Perché è importante dotarsi di una ePolicy?

Attraverso l'ePolicy 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' ePolicy 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.

La diffusione dei Social fra gli adolescenti ha influenzato le modalità di accesso all'informazione e ha ridefinito le dinamiche comunicativo - relazionali. Tuttavia, anche se la Rete rappresenta per i più giovani una indubbia fonte di opportunità e stimoli di natura cognitiva, comunicativa e relazionale, un utilizzo scorretto può esporre a situazioni di vulnerabilità e pericolosità.
In una simile situazione la Scuola, luogo di formazione, inclusione e accoglienza, ha il dovere di mediare il rapporto tra gli adolescenti e le nuove tecnologie digitali, promuovendone un uso sicuro, consapevole ed efficace.
Il MIM è impegnato da anni sul fronte della prevenzione del **fenomeno del bullismo e del cyberbullismo** e più in generale, di ogni forma di sopruso e violenza online. Diverse sono le strategie di intervento utili ad arginare i comportamenti a rischio, attraverso il **Decreto prot. n. 1176 del 18/05/2022** - Assegnazione fondi per **contrastare il fenomeno del cyberbullismo (Legge n.234/2021)**, il Decreto assegnazione fondi per contrastare il fenomeno del cyberbullismo da destinare agli Uffici Scolastici Regionali, la Legge 107 del 2015 che ha introdotto, tra gli obiettivi formativi prioritari, lo sviluppo di competenze digitali negli studenti per un uso critico e consapevole dei social network e dei media. Tali iniziative hanno trovato il loro coronamento nel progetto Generazioni Connesse, iniziativa sostenuta dalla Commissione Europea e coordinata dal MIM, realizzata in partenariato con le principali Agenzie nazionali sensibili al tema della sicurezza in Rete.

La nostra scuola, convinta dell'opportunità di integrare le TIC nella didattica e sensibile al benessere psico-fisico dei propri studenti, si impegna quotidianamente nella promozione di valori e competenze finalizzate all**'acquisizione di una cittadinanza digitale consapevole** e vuole, adesso, **con questo Documento, fissare i cardini e le procedure ePolicy e rendere edotta tutta la comunità scolastica.**

1.2 - Ruoli e responsabilità

Affinché l'ePolicy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, s'impegni nell'attuazione e promozione di essa.

Il Dirigente Scolastico

il Dirigente Scolastico deve garantire la sicurezza, anche *online*, di tutti i membri della comunità scolastica. È importante, quindi, che sia adeguatamente formato sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIM; promuove inoltre la cultura della sicurezza online e, ove possibile, dare il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC.

L'Animatore digitale

L'Animatore digitale può supportare il personale scolastico da un punto di vista non solo

tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica); potrebbe, inoltre, monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e avere il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

Il Referente bullismo e cyberbullismo

"Ogni Istituto scolastico, nell'ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo" **(Art. 4 Legge n.71/2017**, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo"). Tale figura ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Fondamentale, dunque, il suo ruolo non solo in ambito scolastico ma anche in quello extrascolastico, in quanto (ove possibile) potrebbe coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

I Docenti

i Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Possono, innanzitutto, integrare parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica. I docenti dovrebbero accompagnare e supportare gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM/Digital Board o di altri dispositivi tecnologici che si connettono alla Rete; hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

Il personale Amministrativo, Tecnico e Ausiliario (ATA)

Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il dirigente scolastico e con il personale docente tutto. Diverse figure che, in sinergia, si occupano ciascuno per la propria funzione, del funzionamento dell'Istituto scolastico che passa anche attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola. Esiste, cioè, un concreto coinvolgimento del personale ATA nell'applicazione della legge 107/15, che concerne non solo il tempo scuola e il potenziamento dell'offerta formativa, ma anche le attività di formazione e autoformazione in tema di bullismo e cyberbullismo. Il personale ATA dovrebbe, all'interno dei singoli regolamenti d'Istituto, essere coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi.

Le Studentesse e gli Studenti

Gli Studenti, in relazione al proprio grado di maturità e consapevolezza raggiunta, dovrebbero utilizzare al meglio le tecnologie digitali e in coerenza con quanto richiesto dai docenti; con il supporto della scuola dovrebbero imparare a tutelarsi online, tutelare i propri compagni e

rispettarli.
Dovrebbero partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

I Genitori

i Genitori, in continuità con l'Istituto scolastico, dovrebbero essere partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali. Dovrebbero relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i propri figli non usano responsabilmente le tecnologie digitali o Internet. È estremamente importante che accettino e condividano quanto scritto nell'ePolicy dell'Istituto.

Gli Enti educativi esterni e le associazioni

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

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

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto

dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

Al fine di rendere l'ePolicy uno strumento efficace per la tutela degli studenti e delle studentesse, intesa in senso ampio, è utile individuare un insieme di regole o norme di comportamento da condividere con le organizzazioni/associazioni extrascolastiche e gli

esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve e/o lungo periodo.

Dotarsi di un'informativa sintetica sull'ePolicy comprensiva delle procedure di segnalazione da condividere con tutte le figure che operano con studenti e studentesse, significa non solo tutelare questi ultimi e la scuola stessa, ma anche porre in essere nuove modalità per rilevare, limitare e contrastare possibili pericoli legati a condotte educative non professionali. Tale documento chiarisce il sistema di azioni e le procedure di segnalazione da seguire valide anche per i professionisti e le organizzazioni esterne, finalizzate a rilevare e gestire le problematiche connesse ad un uso non consapevole delle tecnologie digitali.

In questo modo, si facilita la presa in carico da parte della scuola, qualora si verificassero problematiche derivanti da un utilizzo non corretto delle tecnologie digitali o quando, nei casi più estremi, si sospettassero forme di maltrattamento/abuso sia nel reale che nel virtuale, sia di tipo fisico che psicologico a danno di minori. Tale documento, inoltre, permette di tutelare ragazzi e ragazze da comportamenti potenzialmente rischiosi messi in atto da soggetti esterni alla scuola e che si trovano ad operare all'interno dell'Istituto.

In coerenza con il percorso intrapreso e con le azioni che l'Istituto già pone in essere, la predisposizione di un'informativa sintetica sull'ePolicy comprensiva delle procedure di segnalazione garantisce un migliore rapporto fiduciario fra scuola e famiglia, consente di distinguere i ruoli e le azioni da compiere e di attivare direttamente, a seconda della tipologia dei casi da segnalare, le autorità competenti collaborando con i servizi del territorio per la prevenzione e la gestione di quanto rilevato, in un'ottica di gestione condivisa degli interventi.

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

"Tutti gli attori che entrano in relazione educativa con i nostri studenti 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 il Regolamento del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali e di 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 e comunicazione dell'ePolicy all'intera comunità scolastica

Il documento di ePolicy 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'ePolicy 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'ISIS Leopoldo II di Lorena 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. Al fine di comunicare al meglio il documento di ePolicy a tutta la comunità scolastica, sono previste le seguenti azioni: presentazione mirata del documento ai docenti, al personale A.T.A., ai rappresentanti dei genitori e ai rappresentanti degli studenti durante specifici incontri, appositamente organizzati ad inizio anno scolastico o attraverso circolari.

1.5 - Gestione delle infrazioni alla ePolicy

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

In relazione all'uso improprio delle TIC a scuola da parte degli studenti e delle studentesse, LE SANZIONI sono quelle previste dal Regolamento di Istituto e decise dal Consiglio di Classe interessato.

Sono punite le seguenti CONDOTTE (lista esemplificativa che <u>non esclude</u> ulteriori comportamenti similari o riferiti)

- **episodi di cyberbullismo;**
- **realizzazione e condivisione online, o anche solo condivisione, di immagini o video di compagni/e senza il loro consenso o che li ritraggono in pose offensive e denigratorie o comunque volti all'esclusione di compagni;**

- **realizzazione e condivisione, o anche solo condivisione, di scatti intimi e a sfondo sessuale;**
- **condivisione di dati personali di terzi (compagni, docenti, personale A.T.A.) senza il loro consenso;**
- **uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;**
- **condivisione in rete di comunicazione ufficiali interne all'Istituto: compiti in classe, circolari, comunicazioni, valutazioni e similari;**
- **registrazioni audio delle lezioni senza una preventiva autorizzazione da parte del docente;**
- **connessioni a siti proibiti o comunque non autorizzati;**
- **pirateria informatica;**
- **scaricamento di file (video, film, musica, immagini, test, ecc.) per finalità personali non autorizzate.**

Tutte le infrazioni alla presente ePolicy devono essere segnalate con tempestività al Dirigente Scolastico, che provvederà a convocare le parti interessate allo scopo di valutare le possibili azioni da intraprendere. Riguardo ai **provvedimenti disciplinari** da adottare da parte del Consiglio di classe nei confronti dello studente/essa che ha commesso un'infrazione alla ePolicy (in proporzione sia all'età dello studente sia alla gravità dell'infrazione commessa), **saranno privilegiati interventi di tipo educativo e non punitivo, sanzioni disciplinari di tipo riparativo, convertibili quando possibile in attività a favore della comunità.**

Nello specifico:

a. **colloquio con lo/a studente/essa coinvolto/a;**

b. **eventuale confronto con i genitori;**

c. **ripristino delle regole di convivenza all'interno della classe;**

d. **interventi di educazione tra pari (peer education);**

e. **incontri con esperti esterni;**

f. **provvedimenti disciplinari educativi (eventuale sospensione con obbligo di frequenza presso strutture convenzionate dove svolgere mansioni di pubblica utilità sociale);**

g. **eventuale segnalazione alle autorità (Polizia postale, Garante per la protezione dei dati personali, Garante dell'Infanzia e dell'Adolescenza, servizi minorili dell'amministrazione della Giustizia, richiesta di ammonimento da parte del Questore).**

Le infrazioni 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) e **dal Codice disciplinare pubblicato tramite il sito istituzionale e dalla normativa in vigore inerente alla privacy**.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico sarà aggiornato con specifici riferimenti all'ePolicy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida MIM e le indicazioni normative generali sui temi in oggetto. Il presente documento di ePolicy si integrerà pienamente con gli obiettivi enunciati nel PTOF e con il Regolamento di Istituto.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L 'ePolicy 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.

L 'ePolicy sarà riesaminata periodicamente e allorquando si verifichino cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. L'ISIS Leopoldo II di Lorena si impegnerà 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, ma anche qualora si rendessero necessari adeguamenti alla normativa sul tema. Ne verrà testata l'efficacia con particolare riferimento agli obiettivi in esso esplicitati e cioè 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.

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.
In ottemperanza alla L. 71/2017 -Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo-, il nostro Istituto realizza progetti volti all'educazione alla legalità e alla prevenzione delle nuove e pericolose forme di prevaricazione che hanno per teatro la Rete. In particolare, per tutte le classi prime e seconde viene annualmente programmato un incontro con Polizia Postale e/o Guardia di Finanza, finalizzato a sensibilizzare gli studenti rispetto all'uso consapevole di Internet e dei Social Network, educare al rispetto delle leggi che regolano il mondo virtuale, informare e responsabilizzare sul fenomeno del Cyberbullismo. Aderisce inoltre alle iniziative del Safer Internet Day, giornata mondiale per la sicurezza in Rete, istituita e promossa dalla Commissione europea.

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 PNSD promuove e valorizza il buon uso delle TIC nella didattica, estendendo il concetto di scuola da luogo fisico a spazio di apprendimento virtuale. In risposta alle sollecitazioni di un contesto socio - culturale in costante evoluzione, la Scuola ormai da tempo ha avviato una fase di ripensamento delle proprie strutture e dei propri assetti didattici in un'ottica digitale. L'introduzione delle Digital board nelle classi rappresenta l'acme di questo processo. Considerevoli i vantaggi: l'impiego strutturato ed integrato delle TIC nella didattica, promuovendo un uso sincretico di più canali comunicativi, rende gli apprendimenti motivanti, coinvolgenti ed inclusivi, diversifica la prassi educativa, la rende innovativa e capace di offrire efficaci risposte ai diversi stili di apprendimento. Non ultimo, stimola negli studenti la maturazione di senso critico rispetto all'eventuale fruizione di contenuti online. Ma affinché le potenzialità insite nell'uso delle TIC si trasformino in soluzioni concrete ed efficaci, è necessario che vengano utilizzate in modo opportuno e significativo, con un adeguamento costante delle competenze degli insegnanti. Sono stati attivati dei corsi di formazione per il personale docente sull'utilizzo di nuova strumentazione digitale e corsi per aumentare le competenze in questo campo.

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 ed usufruendo delle molteplici proposte di formazione presenti sulla Piattaforma Generazioni Connesse, per studenti, docenti e genitori.

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

Per tali ragioni, l'ISIS Leopoldo II di Lorena crea e creerà specifici momenti di formazione permanente per gli insegnanti che mettano al centro i temi in oggetto, considerando anche percorsi di autoaggiornamento personali o collettivi, iniziative seminariali con professionisti-esperti interni (si pensi al supporto dell'Animatore digitale) ed esterni alla scuola, giornate-settimane di approfondimento in accordo con la rete scolastica del territorio (USR, Osservatori

regionali sul bullismo, amministrazioni comunali, i servizi socio-educativi e le associazioni/enti presenti sul territorio). Previsto l'inserimento di tali azioni programmatiche nel Piano triennale dell'offerta formativa.

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.

Solo mediante una attività divulgativa periodica sarà possibile rendere partecipi le famiglie dell'indirizzo che il nostro Istituto persegue in merito, delle strategie adottate per prevenire eventuali devianze, delle misure previste per contrastarle e degli eventuali provvedimenti sanzionatori da irrogare, commisurati all'entità del danno arrecato e sempre in un'ottica educativa e mai punitiva. Il Regolamento d'Istituto, cui è garantita massima diffusione mediante pubblicazione sul sito web della Scuola, viene integrato con l'ePolicy e lo stesso vale per il Patto di Corresponsabilità.

ll Patto di Corresponsabilità è un documento centrale per ogni istituzione scolastica e per la comunità educante tutta. Per questo, recentemente è stato avviato dal Miur un percorso di revisione finalizzato a definire in modo più dettagliato modalità, tempi e ambiti della partecipazione da parte di genitori e studenti alla vita scolastica. E ciò, anche al fine di creare una maggiore collaborazione e condivisione degli interventi di formazione e di contrasto al bullismo e al cyberbullismo all'interno della comunità educante. Aggiornare il "Patto di corresponsabilità" con specifici riferimenti all'uso delle tecnologie digitali e all'ePolicy è dunque fondamentale per informare e rendere partecipi le famiglie sul percorso che volete intraprendere con il documento e il piano d'azione. A tale proposito è importante informare i genitori sulle condotte che si dovranno adottare a scuola e, in generale, offrire loro consigli da mettere in pratica con i propri figli. Questo Istituto propone di:

- **elaborare regole sull'uso delle tecnologie digitali** da parte dei genitori nelle comunicazioni con la scuola e con i docenti (es. mail, sito della scuola, gruppo Facebook, Instagram, etc.) e informarli adeguatamente anche riguardo alle regole per gli studenti e le studentesse;
- **fornire ai genitori consigli o linee guida sull'uso delle tecnologie digitali nella comunicazione** con i figli e in generale in famiglia (ad es. a tal fine si potrà fare

riferimento alla sezione dedicata ai genitori del sito www.generazioniconnesse.it e fare un richiamo ad essa anche sul sito web della scuola);

- **organizzare percorsi di sensibilizzazione e formazione dei genitori** su un uso responsabile e costruttivo della Rete in famiglia e a scuola.
- **prevedere azioni e strategie per il coinvolgimento delle famiglie** in tali percorsi di sensibilizzazione, ad esempio, mediante l'organizzazione di iniziative in cui anche gli studenti e le studentesse siano protagonisti.

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 predispone modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali.

L'ISIS Leopoldo II di Lorena:

- garantisce la tutela in generale della privacy degli studenti;
- definisce un regolamento per la gestione della privacy legata all'uso dei dispositivi;
- adotta sistemi di sicurezza per la navigazione online sottolineando che dell' uso accidentale e improprio ai siti illeciti non può ritenersi responsabile adotta sistemi di sicurezza per la navigazione online sottolineando che dell' uso accidentale e improprio ai siti illeciti non può ritenersi responsabile;
- individua e definisce le misure di tutela, le modalità per garantirne nel tempo la continuità e l'adeguatezza e le responsabilità per la gestione dei dati: titolare, responsabile, persone autorizzate al trattamento;
- rispetta la privacy dei propri utenti e si impegna a proteggere i dati personali che gli stessi conferiscono all'istituzione, a trattarli in conformità alla normativa vigente;
- in caso di raccolta di dati personali, l'istituzione informerà l'utente sulle finalità della raccolta al momento della stessa, ove necessario, richiederà il consenso dell'utente.

L'Istituto non comunicherà i dati personali dell'utente a terzi senza il consenso dello stesso. Se l'utente decide di fornire alla scuola i propri dati personali, la scuola potrà comunicarli all'interno dell'Istituto od a terzi che prestano servizi alla scuola, solo rispetto a coloro che hanno bisogno di conoscerli in ragione delle proprie mansioni, e, ove necessario, con il permesso dell'utente.

La scuola tratta i dati personali dell'utente:

- per soddisfare le richieste a specifici prodotti o servizi, per personalizzare la visita dell'utente al sito;
- per aggiornare l'utente sulle ultime novità in relazione ai servizi offerti;
- per comprendere meglio i bisogni dell'utente ed offrire allo stesso servizi migliori.

Infine, si fa riferimento a tutto quanto previsto dal Decreto legislativo 30 giugno 2003, n. 196 (c. d. Codice della Privacy}. Si individuano al riguardo alcune linee guida di e-safety:

I video e le fotografie raccolte dai genitori durante le pubbliche attività scolastiche non violano la privacy. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione. Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime su Internet, e sui social network in particolare.

In caso di diffusione diventa necessario, di regola, ottenere il consenso informato delle persone presenti nelle fotografie e nei video.
Si deve quindi prestare attenzione prima di caricare immagini e video sui social network, oppure di diffonderle attraverso sistemi di messaggistica istantanea.
Tale pratica può dar luogo a gravi violazioni del diritto alla riservatezza delle persone riprese, e fare incorrere in sanzioni disciplinari, pecuniarie e in eventuali reati. L'utilizzo di telefoni cellulari, di apparecchi per la registrazione di suoni e immagini, quando autorizzato dai docenti, è consentito, ma esclusivamente per fini didattico-educativi e sempre nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte (siano essi studenti o professori), in

particolare della loro immagine e dignità.

La scuola ha, comunque, la possibilità di regolare o di inibire l'utilizzo di dispositivi elettronici all'interno delle aule o laboratori. Gli studenti e gli altri membri della comunità scolastica, in ogni caso, non possono diffondere o comunicare sistematicamente i dati di altre persone (ad esempio pubblicandoli su Internet) senza averle prima informate adeguatamente e averne ottenuto l'esplicito consenso.

3.2 - Accesso a 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 nostro Istituto si è attivato per garantire la *security* per l'accesso a internet configurando dei

filtri controllati dai gestori telefonici e dei firewall, per monitorare il traffico web e bloccare l'accesso a siti inappropriati; ha valutato tutti i rischi connessi alla sicurezza permettendo al personale scolastico l'accesso alla rete tramite i dispositivi della scuola o tramite i dispositivi personali nel caso del BYOD.

Ha aggiornato l'infrastruttura di rete, permettendo l'accesso a internet a tutte le classi.

Si impegna a gestire gli account di tutti gli utenti (studenti, insegnanti e personale ATA) e gli aspetti legali in relazione alla privacy.

Attraverso azioni del PNSD, la scuola è stata raggiunta da banda larga, sufficientemente veloce, per favorire l'uso di cloud per la didattica e l'uso di contenuti di apprendimento multimediali, attraverso cablaggio LAN e wireless in ogni spazio della scuola. Per l'accesso a internet gli studenti si impegnano a:

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

I docenti si impegnano a:

- utilizzare la rete nel modo corretto
- non utilizzare device personali se non per uso didattico
- formare gli studenti all'uso della rete
- dare consegne chiare e definire gli obiettivi delle attività

La scuola chiederà il consenso genitoriale a tutti i minorenni per l'uso di internet e per la pubblicazione di lavori e delle loro fotografie. Gli studenti con età superiore ai 16 anni (o maggiorenni) non hanno bisogno del consenso scritto dei genitori.

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.

Registro elettronico

Le famiglie ricevono le credenziali per l'accesso riservato al registro elettronico Nuvola, in cui il corpo docente è tenuto a registrare:

- assenze, valutazioni, note e osservazioni;
- risultati scolastici (voti, documenti di valutazione);
- prenotazioni colloqui individuali;
- eventi;
- comunicazione varie.

La pubblicazione delle informazioni attraverso tale strumento assolve l'obbligo di comunicare prontamente ed efficacemente ogni evento riguardante gli alunni.

Piattaforma didattica Google Workspace

I docenti, gli studenti e il personale amministrativo disporranno a partire dal mese di dicembre 2024 di un account Google Workspace

L'account è strettamente personale, per cui ogni utente dovrà avere cura di disconnettere il proprio accesso al termine del suo utilizzo in ogni dispositivo utilizzato che non sia il dispositivo personale. Lo spazio del proprio account è destinato alla ricezione di comunicazioni, all'invio di documentazione e alla condivisione di materiali, progetti didattici o progetti con altri docenti. Sono attive piattaforme di lavoro condiviso con Google Classroom per attività di e_learning.

La scadenza degli accessi sarà programmata al 31 agosto dell'anno di fine percorso scolastico. Lo stesso sarà per gli account dei docenti e del personale della scuola con contratto a tempo determinato.

Le comunicazioni tra personale scolastico, famiglie e studenti via e-mail avvengono tramite un indirizzo e-mail della scuola o tramite il registro elettronico Nuvola.

Sito della scuola

Il DS e il personale incaricato (in possesso di credenziali) hanno il compito di gestire il sito della scuola (www.isisleopoldo2dilorena.edu.it) e la responsabilità di garantire che i contenuti pubblicati e i servizi siano accurati e appropriati.

Social network

I social network utilizzati per pubblicare commenti su persone e/o istituzioni e per diffondere foto/filmati senza il consenso degli utenti della comunità, possono causare reati penali.

Si invitano pertanto tutti gli studenti a non prelevare o diffondere immagini, video o registrazioni - anche solo audio - non autorizzate, ed eliminare da internet eventuali riferimenti offensivi o comunque illeciti (ed inopportuni) nei confronti dell'Istituto e dei suoi docenti e studenti.

Allo stesso tempo, si invitano gli alunni e i genitori a fare un uso prudente dei social e delle piattaforme di messaggistica istantanea, limitandone l'uso alle sole comunicazioni funzionali.

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 MIM 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.

L'uso dei dispositivi personali in classe è normato dai seguenti regolamenti DPR n. 249/1998; DM n 30 del 15/03/2007; Regolamento d'Istituto.

In questi ultimi sono indicate le sanzioni disciplinari in caso di uso scorretto dei cellulari da parte dei ragazzi e delle ragazze in classe.

Gli studenti

Per alunni diversamente abili oppure con BES, previa consultazione con il Consiglio di Classe, si concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili.

Se dovessero verificarsi eventi riconducibili all'uso non corretto o non legittimo di uno qualsiasi dei dispositivi, le responsabilità sono tutte ascrivibili alle famiglie degli studenti eventualmente coinvolti e condivise dal personale scolastico solo quando, avendo personalmente constatato che qualche ragazzo/a fa uso di un device (smartphone o tablet) durante l'orario scolastico e lo utilizza in modo scorretto e contro il regolamento di istituto non dovesse immediatamente intervenire nelle forme già indicate e comunque in modo tale da prevenire o reprimere sul nascere situazioni incompatibili con le più elementari regole della civile convivenza.

Il personale scolastico Docenti/ATA

Ai docenti è consentito utilizzare i dispositivi della scuola per realizzare tutte le attività connesse alla loro funzione.

È consentito per i docenti l'uso dei propri dispositivi in classe per quanto attiene l'attività didattica qualora siano necessari, ma non possono essere utilizzati durante le lezioni per questioni personali.

Utilizzeranno la strumentazione fornita dalla scuola rispetto a quella personale, l'utilizzo improprio verrà contestato al titolare delle credenziali con cui è avvenuta la connessione.

Durante l'attività didattica il docente spiega ai propri alunni la netiquette e ne chiarisce le regole; si assume la responsabilità di segnalare prontamente eventuali malfunzionamenti o danneggiamenti al tecnico informatico.

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'ISIS Leopoldo II di Lorena propone corsi di formazione (attraverso collaborazione con le Forze dell'ordine, ASL, enti locali) per studenti, docenti e/o famiglie, al fine di promuovere un uso consapevole e proficuo della Rete e degli strumenti digitali, per sviluppare competenze nella prospettiva di una prevenzione dei rischi online.

La scuola offre opportunità formative a studenti, docenti e genitori, anche attraverso la Piattaforma di Generazioni Connesse, che è stato lo strumento di supporto per l'elaborazione del Documento di ePolicy di Istituto.

Da qualche anno viene affrontata anche la tematica della cybersecurity, a tutela della privacy negli ambienti digitali.

Inoltre, l'Istituto fa parte di una Rete cui aderiscono tutti gli Istituti della Provincia di Grosseto,

che organizza azioni tese a:

- informare e sensibilizzare gli studenti rispetto alle tematiche e ai pericoli connessi con l'uso delle tecnologie digitali

- creare una rete di riferimento per contrastare l'insorgenza di situazioni problematiche legate al fenomeno del bullismo e cyberbullismo;

- formare gli studenti ed i docenti sull'uso consapevole delle tecnologie digitali;

- informare e sensibilizzare le famiglie sull'uso consapevole delle tecnologie digitali:

- promuovere la conoscenza dell'ePolicy nella comunità scolastica attraverso i diversi canali digitali.

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).

All'interno della scuola" il docente referente Bullismo e Cyberbullismo si impegna per una adeguata e necessaria formazione attraverso la Piattaforma Elisa del MIM sulle tematiche connesse al contrasto al bullismo e al cyberbullismo.

4.3 - Hate speech: che cos'è e come prevenirlo

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

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

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete.

L'ISIS Leopoldo II di Lorena prevede per questo la strutturazione di percorsi e la realizzazione di attività di analisi e/o produzione multimediale, finalizzate soprattutto a:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di *hate speech*, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e *i*

social network;

- favorire una presa di parola consapevole e costruttiva da parte dei giovani.
- sviluppare una riflessione sul concetto di libertà di espressione e sul labile confine tra scherzo e offesa
- utilizzare il linguaggio mediatico come veicolo di inclusione e non di vessazione.
- promuovere la conoscenza del Manifesto della comunicazione non ostile.

In particolare, riguardo a quest'ultimo punto, durante il mese di Ottobre 2023, le classi terze del nostro Istituto, hanno incontrato Rosy Russo, ideatrice del *Manifesto della comunicazione non ostile.* Si tratta di una carta che elenca dieci princìpi di stile utili a migliorare lo stile e il comportamento di chi sta in Rete. Si tratta di un impegno di responsabilità condivisa, che mira a promuovere e sviluppare un lessico rispettoso e comportamenti civili, sia nella pratica quotidiana, didattica e non, sia negli ambienti digitali, in modo che la Rete costituisca un luogo accogliente e sicuro per tutti.

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.

Secondo uno studio inglese, più del 23% dei giovani intervistati ha una relazione disfunzionale con lo smartphone. Vengono riportati stati d'ansia provocati dall'uso compulsivo del cellulare che, nei casi più gravi, possono sfociare in vera e propria depressione. In Italia una ricerca condotta su 6.671 giovani tra gli 11 e i 25 anni ha fatto registrare tali risultati: il 45% degli studenti dichiara di passare sul web almeno 5-6 ore ogni giorno e il tempo trascorso online raggiunge picchi più alti nel fine settimana. Un intervistato su cinque dice di sentirsi a disagio o comunque va in ansia quando manca la connessione alla Rete e cresce in contemporanea la percentuale di coloro che manifestano attacchi di panico quando finiscono i giga e le promozioni tariffarie a cui sono abbonati (circa 1 su 3).

La dipendenza da Internet si può manifestare anche attraverso il gioco online: la comunità scolastica ha il compito di vigilare sul fenomeno e promuovere negli studenti lo sviluppo di una consapevolezza dei rischi che comporta una connessione prolungata, quali ad esempio il progressivo assorbimento del soggetto alla Rete e la la conseguente sottrazione del tempo alle altre attività quotidiane del minore.

La dipendenza da Internet domina infatti i pensieri ed il comportamento del soggetto, assumendo un ruolo primario rispetto ad altri interessi, provoca cambiamenti nel tono dell'umore e fa scaturire conflitti interpersonali tra il soggetto e coloro che gli sono vicini. I segnali patologici sono gli stessi di altre dipendenze: da una parte la tolleranza, che si manifesta quando vi è un crescente bisogno di aumentare il tempo su internet e dall'altra l'astinenza

quando l'interruzione o la riduzione dell'uso della Rete comporta ansia, agitazione psicomotoria, fantasie, pensieri ossessivi, malessere psichico-fisico. Tutto ciò si ripercuote sulla sfera delle relazioni interpersonali che si riducono , in quanto ad esse si preferisce il mondo virtuale.

L'ISIS Leopoldo II di Lorena mira a promuovere azioni di prevenzione anche su questo ambito, attraverso la strutturazione di percorsi rivolti al benessere digitale, vale a dire la capacità di creare e mantenere una relazione sana con la tecnologia. Si tratta di un argomento trasversale, in materia di cittadinanza digitale, di cyberbullismo, di uso integrativo dei dispositivi e della Rete. Può essere utile riflettere con gli studenti per fare in modo che la tecnologia sia strumento per raggiungere i propri obiettivi e non sia solo distrazione o addirittura ostacolo.

La scuola può insegnare molto da questo punto di vista se integra la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online.

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. In pochi istanti e attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e potenzialmente infinito di persone.

I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di "*revenge porn*", letteralmente "vendetta porno", che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte. La Legge 19 luglio 2019 n. 69, all'art.10 ha introdotto in Italia il reato di *revenge porn*, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti.

L'ISIS "Leopoldo II di Lorena" mira a promuovere azioni di prevenzione anche in relazione a questo fenomeno, attraverso la strutturazione di percorsi rivolti al benessere digitale, vale a dire la capacità di creare e mantenere una relazione sana con la tecnologia.

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).

La scuola ha il compito di favorire negli studenti e nelle studentesse la presa di coscienza dei rischi in cui si può incorrere in Rete. Risultano utili eventi ed incontri con esperti della Polizia postale, per la prevenzione e la sensibilizzazione sui reati legati all'utilizzo di internet e delle piattaforme online Attivare uno sportello d'ascolto

Fondamentale quindi è progettare e realizzare percorsi di educazione all'utilizzo delle tecnologie digitali e della Rete, anche per sviluppare negli studenti e nelle studentesse una maggiore consapevolezza riguardo alla protezione della propria *privacy,* alla gestione dell'immagine e dell'identità *online*, fino alla capacità di gestire adeguatamente le relazioni negli ambienti digitali (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è). Per consigli e per un supporto è possibile rivolgersi alla Helpline di Generazioni Connesse (19696): operatori esperti sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che degli adolescenti, 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 esperienze negative e/o problematiche inerenti l'utilizzo dei nuovi media.

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.

L'ISIS Leopoldo II di Lorena intende sviluppare e promuovere tra gli studenti e le studentesse una consapevolezza anche riguardo al reato di pedopornografia e, a tale scopo, si avvale della collaborazione e di relazione sinergiche con le forze dell'Ordine, attraverso la realizzazione di incontri con le classi.

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.

Nell'ottica di un progetto educativo di prevenzione e sensibilizzazione sulle tematiche sopra riportate, oltre ad una necessaria adeguata formazione per il maggior numero di docenti dell'Istituto, è fondamentale anche la creazione di un rapporto di fiducia tra docenti e studenti, in modo da rendere possibile la segnalazione di situazioni di difficoltà o disagio da parte di una possibile vittima di un qualsiasi fenomeno di bullismo o cyberbullismo.

Il docente che viene a conoscenza di una situazione riconducibile a tali fenomeni,

attiva la procedura corretta in base alla gravità della situazione, riferendosi al Team antibullismo e cyberbullismo, coordinato dal Referente Bullismo di Istituto. In base alle Linee guida della Legge del 2017, è previsto il coinvolgimento progressivo di vari soggetti, docenti

del Consiglio di Classe, personale ATA, Referente bullismo con il Team Antibullismo, Dirigente Scolastico, genitori e per i casi più gravi autorità esterne di competenza.

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.

In caso di necessità e per gestire eventuali casi che si dovessero verificare, l'Istituto utilizzerà le procedure e gli strumenti messi a disposizione da Generazioni Connesse, presenti in allegato. L'ISIS Leopoldo II di Lorena ha un protocollo per gestire eventuali casi riconducibili ai fenomeni di bullismo e cyberbullismo, descritto di seguito.

Il docente che assiste oppure viene a conoscenza di una situazione che potenzialmente può essere ricondotta ai fenomeni di bullismo o cyberbullismo, ha il compito di:

1. Descrivere in modo dettagliato sul registro elettronico lo svolgimento dei fatti, nel caso essi siano avvenuti in sua presenza oppure, in caso contrario, accertarsi dell'accaduto cercando di comprendere la dinamica degli eventi, ascoltando testimonianze e dichiarazioni, nel rispetto e nella tutela della privacy dei soggetti coinvolti

2. Se il docente ha il sospetto o l'evidenza certa che si tratti di un caso di bullismo o cyberbullismo, dovrà contattare il coordinatore di classe che provvederà ad informare tempestivamente il Referente Bullismo. A seguito di tale confronto, si procederà secondo questi step:

- Confronto tra alunni coinvolti alla presenza del Referente Bullismo, del coordinatore di classe e di almeno un altro docente della classe.

- Richiesta colloquio con le famiglie degli alunni coinvolti al fine di chiarire la dinamica dei fatti ed individuare in modo condiviso soluzioni di intervento sia all'interno della scuola che all'esterno dell'Istituzione scolastica.

- Richiesta al DS di convocazione di un consiglio di classe straordinario per individuare strategie di primo intervento individuali e per il gruppo classe alla presenza del Referente Bullismo che dovrà relazionare al Dirigente Scolastico.

Il tutto è strutturato per raggiungere, quando possibile, una conciliazione delle controversie che si sono verificate qualora vi sia volontà unanime in tal senso delle famiglie e degli alunni coinvolti. Nei casi più complessi i docenti del team per la prevenzione si avvalgono anche del parere dello psicologo di Istituto. Se tali tentativi non producono risultati positivi o l'azione commessa è grave la scuola segnalerà la situazione alle Autorità competenti.

Per tutti i dettagli si faccia riferimento agli allegati con le procedure (Sezione 5.4)

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'ISIS Leopoldo II di Lorena tende a prevenire i rischi legati ai fenomeni di bullismo, cyberbullismo o connessi ad un utilizzo non consapevole della Rete, attraverso incontri con le Forze dell'Ordine, ASL, enti locali, ma anche con la partecipazione a progetti annuali promossi dal Referente per il bullismo ed il cyberbullismo attraverso la partecipazione agli incontri di Rete BULLOUT.

Sul sito di Istituto è inoltre presente un'area nella quale è consultabile la normativa di riferimento è possibile reperire i contatti da poter utilizzare per eventuali segnalazioni. Gli studenti sono invitati a segnalare situazioni che possono potenzialmente rientrare nell'ambito dei fenomeni di bullismo, cyberbullismo, uso inappropriato della Rete, come navigazione in siti che incitano all'odio e/o con contenuti inappropriati per l'età degli studenti. Il referente bullismo, informato dallo studente o dai colleghi, provvede ad informare il Dirigente Scolastico.

5.3. - Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di

Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

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

- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico**: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

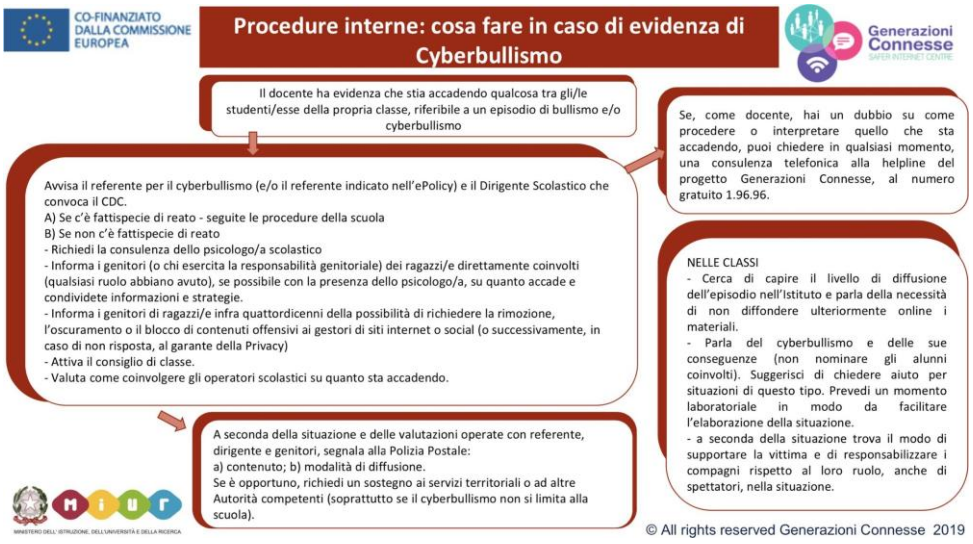
L'Istituto collabora ogni anno scolastico con le Forze dell'Ordine (Polizia Postale, Polizia di Stato, Arma dei Carabinieri), con ASL ed altri enti locali o agenzie territoriali allo scopo di organizzare incontri con gli studenti e le studentesse per sensibilizzarli rispetto alle tematiche relative a bullismo, cyberbullismo ed utilizzo consapevole delle tecnologie digitali e della Rete.

Vengono proposti, inoltre, corsi di formazione per i docenti, promossi dalla Asl Toscana Sud Est. Sono disponibili anche corsi di formazione sulla Piattaforma Generazioni Connesse, per Studenti, Docenti e Genitori.

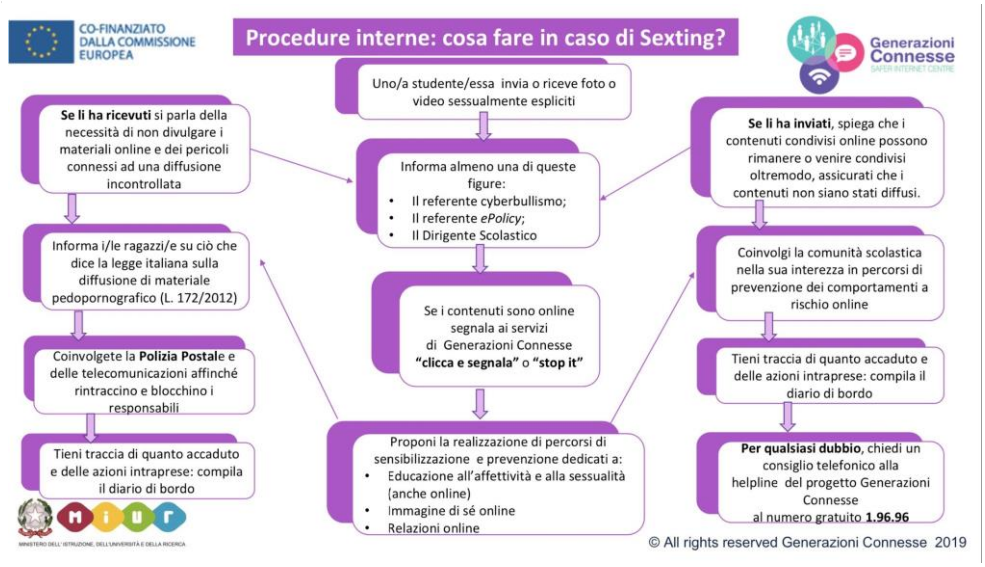
L'Istituto fa parte di una Rete di scuole della Provincia di Grosseto, istituita nel 2022, che collabora con l'Ufficio Scolastico Provinciale e che persegue finalità di prevenzione di bullismo e cyberbullismo.

5.4. - Allegati con le procedure

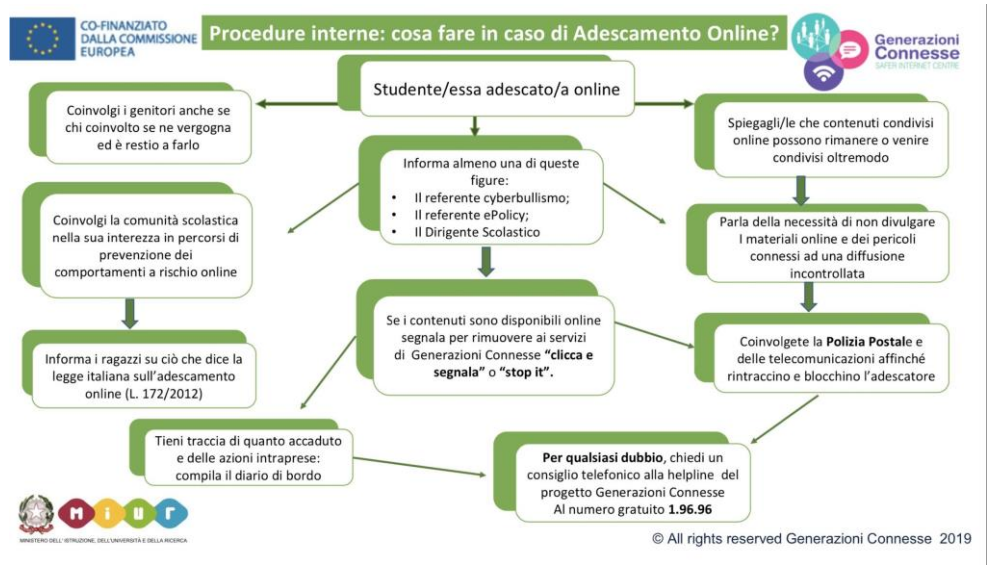
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



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

