Documento di E-Policy

FOPS040002

LICEO SCIENTIFICO STATALE "*FULCIERI PAULUCCI DI CALBOLI*"

VIA ALDO MORO 13, 47121 FORLI' - FORLI'-CESENA (FC)

Dirigente Scolastico Dott.ssa SUSI OLIVETTI

Capitolo 1 - Introduzione al documento di E-Policy

1.1 - Scopo dell'E-Policy

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.

Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Argomenti del Documento

1. **Presentazione dell'E-Policy**
    1. Scopo dell'E-Policy
    2. Ruoli e responsabilità
    3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
    4. Condivisione e comunicazione dell'E-Policy all'intera comunità scolastica

5. Gestione delle infrazioni alla E-Policy
6. Integrazione dell'E-Policy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'E-Policy 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

1.1 Scopo dell'E-Policy. 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.

Le "Linee di Orientamento per azioni di prevenzione e contrasto al bullismo e al cyber-bullismo, nota 2519, 15/4/2015, ed infine l'istituzione della Legge 29 maggio 2017 n. 71 recante "Disposizioni a

tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", hanno determinato la necessità sempre crescente di un'azione mirata ed efficace da parte della scuola per prevenire il fenomeno nella consapevolezza della imprescindibile collaborazione della famiglia e degli enti territoriali.

Il presente documento, elaborato in collaborazione con il Safer Internet Centre, nell'ambito del progetto Generazioni Connesse, vuole coinvolgere tutte le componenti della Comunità scolastica: il personale della scuola, gli alunni e le famiglie per definire l'insieme di regolamenti, linee di azione e attività da porre in essere per facilitare e promuovere l'utilizzo delle TIC nella didattica e, attraverso lo sviluppo di competenze digitali, determinare anche una prevenzione rispetto ai rischi delle tecnologie digitali nonché le misure di gestione di situazioni problematiche.

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.

La pervasività delle nuove tecnologie nella vita personale, i rischi ad esse connesse, le sue potenzialità e l'esponenziale crescita dei contatti e delle relazioni, pone spesso il singolo di fronte ad una duplice situazione da vivere: la realtà "concreta" e quella virtuale, tra loro oramai fortemente connesse, influenzate e spesso determinate. La nascita poi di gruppi in rete richiede capacità comunicative e socio-relazionali adeguate.

È fondamentale quindi conoscere come comportarsi in questi gruppi, quali regole vanno rispettate e quali ruoli e responsabilità hanno i soggetti che vi partecipano.

È opportuno quindi che anche nell'ambito scolastico ci sia chiarezza sui ruoli e sulle responsabilità di ciascun attore del percorso formativo.

Il **Dirigente scolastico** è il soggetto su cui incombe la responsabilità di garantire la sicurezza dei membri della comunità scolastica e, conseguentemente, anche della sicurezza in rete. In quest'ottica egli si preoccupa di:

- garantire a tutti i docenti ed alunni, soprattutto quelli in entrata, la formazione per l'uso responsabile e corretto delle Tecnologie dell'Informazione e della comunicazione (alcune ore di lezione all'anno sulla websecurity nelle TIC), oltre che nell'uso personale, anche nella didattica;
- dotare la scuola di un sistema in grado di consentire il controllo della sicurezza in rete;
- seguire le procedure relative agli eventi dannosi eventualmente occorsi agli alunni nell'utilizzo delle TIC a scuola.

L'**Animatore digitale** si preoccupa di:

- promuovere la formazione interna in ambito tecnologico-digitale oltre che a fungere da referente per ogni informazione riguardo i rischi della rete, le relative misure di prevenzione nonché la gestione operativa delle eventuali minute problematiche;
- rilevare le criticità proponendo soluzioni adeguate e sostenibili;
- interessarsi sia dell'aggiornamento delle politiche di istituto sulla rete della scuola, sia della proposta di novità ed aggiornamento metodologico e tecnologico implementabile nella rete di istituto ad uso di tutto il personale scolastico;
- gestire e controllare l'accesso alla rete ed ai servizi di istituto (posta elettronica, G- suite, ecc.) da parte degli utenti mediante credenziali personalizzate, firewall, antivirus, ecc.
- individuare progetti ed attività aventi ad oggetto la sicurezza in rete in cui coinvolgere la comunità scolastica (alunni, genitori, docenti).

Il **Direttore dei Servizi Generali e Amministrativi** deve:

- assicurare, nei limiti delle risorse finanziarie, la manutenzione delle strutture informatiche ai fini del suo funzionamento, della sua sicurezza e tutela da un uso improprio, e da attacchi esterni;
- garantire la comunicazione all'interno dell'istituto, tra la rete di scuole e fra la scuola e le famiglie degli alunni (sportello, circolari, sito web ecc.), per la diffusione di informazioni nell'ambito dell'utilizzo delle tecnologie digitali e della rete.

I **docenti** si impegnano a:

- informarsi e ad aggiornarsi su tema della sicurezza in rete uniformandosi alle politiche di sicurezza adottate dalla scuola di cui rispettano il regolamento;
- supportare gli alunni nel corretto utilizzo delle tecnologie digitali per finalità didattico- educative (controllo nel rispetto delle leggi, del regolamento interno, del plagio, del diritto d'autore, ecc.);
- guidare gli studenti nella scelta della fonte di informazioni;
- garantire che le comunicazioni con i mezzi informatici avvengano nel rispetto dei ruoli e dei rispettivi codici comportamentali, mediante canali ufficiali e verificabili (posta elettronica col dominio dell'istituto, G-suite, ecc.);
- rispettare l'obbligo di riservatezza dei dati personali trattati e non, in conformità alla normativa vigente;
- interagire con i genitori, coordinando con gli stessi l'intervento educativo, nei casi di disagio, manifestato dall'alunno, collegato all'utilizzo delle tecnologie digitali;
- segnalare all'Animatore digitale eventuali criticità nei sistemi informativi soprattutto in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- seguire le procedure interne di segnalazione di eventuali abusi subiti dagli alunni e connessi all'uso delle tecnologie digitali.

Agli **alunni** è richiesto di:

- utilizzare responsabilmente le tecnologie digitali uniformandosi alle indicazioni dei docenti nonché rispettando le norme codificate nei regolamenti di istituto;
- rispettare le buone pratiche di sicurezza in rete;

- saper distinguere, con l'aiuto dei docenti, le fonti di informazione attendibili in rete per utilizzarle in modo appropriato senza violazione dei diritti d'autore altrui;
- comunicare in rete in modo appropriato rispettando le posizioni altrui;
- segnalare ai genitori e/o ai docenti situazioni di difficoltà o di bisogno di aiuto nell'utilizzo delle tecnologie digitali.

Anche i **genitori** sono coinvolti a pieno titolo. Ad essi è richiesto di:

- sostenere i docenti nell'azione educativa diretta al corretto utilizzo delle tecnologie digitali;
- educare (vigilando sui propri figli) al corretto utilizzo delle tecnologie digitali in ambiente domestico fissando regole comportamentali e di utilizzo;
- collaborare con i docenti nell'adozione di linee di intervento coerenti per contrastare l'uso non responsabile, scorretto o pericoloso delle tecnologie digitali.

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).

I soggetti esterni devono essere informati sulle regole definite all'interno dell'istituto che permettono di lavorare in modo sereno e consentono di usare le tecnologie in modo efficiente e positivo. Questo documento, che costituisce parte integrante del Regolamento di Istituto, sarà portato a conoscenza oltre che dei genitori, degli studenti e di tutto il personale della scuola, anche di tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse. Le norme di

questo documento valgono per tutti gli spazi e laboratori dell'Istituto. Il personale esterno (genitori, tirocinanti, esperti che collaborano con la scuola, ecc.), come quello interno all'Istituto (docenti, ATA e studenti) sono tenuti a prendere visione del presente documento, che sarà revisionato annualmente. Il presente regolamento, da un punto di vista legislativo e amministrativo, è ispirato e promosso da direttive del Ministero dell'Istruzione a livello nazionale e regionale e fa costante riferimento alle norme legislative specifiche del settore.

1.4 – Condivisione e comunicazione dell'E-Policy 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 studenti) 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.

Il presente documento sarà pubblicizzato in seno al Consiglio di Istituto, Collegio Docenti, Consigli di Classe e messo all'albo istituzionale, nonché sul sito web della scuola al link "Bullismo e cyberbullismo" gestito nell'ambito della prevenzione dei fenomeni dal Referente al Bullismo di Istituto e dal Web Master.
Sono previsti inoltre:

- Incontri-riflessioni con figure professionali di riferimento
- Incontri formativi con genitori
- Incontro con POLIZIA POSTALE

- Incontro con arma dei CARABINIERI
- Safer Internet Day
- Attività collegate a “GENERAZIONI CONNESSE”
- Attività e adesione a progetti relativi a tutto ciò che concerne EDUCAZIONE ALLA LEGALITÀ

1.5 - Gestione delle infrazioni alla E-Policy

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.

La gestione dei casi rilevati va differenziata a seconda della loro gravità; è opportuno condividere ogni situazione con il team docenti. Alcuni episodi possono essere affrontati e risolti con la discussione collettiva in classe. In altri è opportuno convocare genitori e alunni per cercare di rimediare all’accaduto. Nei casi più gravi occorre sottoporre all’attenzione del Dirigente Scolastico l’accaduto perché predisponga le azioni da intraprendere.

È opportuno:

- Promuovere campagne di sensibilizzazione e informazione anche con l’ausilio di progetti e realtà esterni.
- Portare a conoscenza degli alunni che per la legge italiana il cyber-bullismo, la diffusione e il possesso di materiale pornografico è reato e che una foto o un video diffuso in rete potrebbero non essere tolti mai più.
- Sensibilizzare la popolazione studentesca sull’esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione.
- Coinvolgere i genitori per attivare forme di controllo della navigazione e monitorare l’esperienza online dei propri figli.
- Tutelare la privacy e informare sull’esistenza di leggi in materia di tutela dei dati personali e di organismi per farli rispettare. I docenti, in classe, parlano di bullismo, adescamento, uso sicuro di internet e dei social network, sexting, cyberbullismo e delle conseguenze. Propongono riflessioni sulle menzogne dette per stringere relazioni online.
- Promuovere la consapevolezza e le conoscenze sul cyberbullismo, attraverso corsi di formazione, seminari, dibattiti. È infatti importante che docenti, personale ATA, genitori e studenti abbiano una chiara e condivisa definizione di cyberbullismo. Inoltre è opportuno informare i docenti, il personale ATA ed i genitori sui comportamenti non verbali correlati al cyberbullismo. Gli adulti dovrebbero allertarsi se uno studente, dopo l’uso di internet o del proprio telefonino, mostra stati depressivi, ansiosi o paura.
- Segnalare agli alunni l’esistenza di una linea di ascolto 19696 attiva tutto l’anno 24 ore su 24 di Telefono Azzurro che raccoglie richieste di ascolto e di aiuto. Al servizio HOTLINE si possono segnalare, in forma anonima, contenuti pedopornografici e altri contenuti dannosi diffusi dalla rete. Sono a disposizione dei servizi quali: Telefono Azzurro, Save

the Children, Polizia Postale.

- Per tutti i casi che costituiscono reato occorre informare il Dirigente Scolastico per confrontarsi sulle azioni da intraprendere ed eventualmente attivare l'intervento delle forze dell'ordine.

Non esistono ad oggi protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi, tuttavia si praticano forme di collaborazione nella prevenzione e contrasto del bullismo e del cyberbullismo con gli Enti Locali e il Comando dei Carabinieri.

1.6 - INTEGRAZIONE dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

La Policy va ad integrarsi con gli obiettivi del PTOF, con il Regolamento di Istituto, con il Regolamento sull'uso dei dispositivi elettronici e con la normativa vigente.

Risulta infatti necessario aggiornare il Regolamento di Istituto prevedendo apposite norme in tema di cyberbullismo e navigazione on line sicura, specificando ulteriormente quando e come si possono utilizzare all'interno della scuola i computer, gli smartphone e/o qualsiasi dispositivo in grado di collegarsi ad internet.

1.7 – Monitoraggio dell'implementazione della E-Policy 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 periodicamente dal Dirigente Scolastico con la collaborazione dell'Animatore Digitale e dal Referente Bullismo a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

Il nostro piano di azioni

Azioni svolte entro l'annualità scolastica 19/20:

- Formazione dei docenti del gruppo di lavoro sul portale GENERAZIONI CONNESSE e prima stesura del documento di E-Policy.

Azioni da svolgere nei prossimi 3 anni:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'E-Policy.
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'E-Policy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i
- Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto agli studenti, docenti e genitori
- Organizzare un evento di presentazione e conoscenza dell'E-Policy rivolto agli studenti, docenti e 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.

Il nostro Istituto da diversi anni si avvale di interventi di Esperti (Polizia di Stato, Carabinieri, Associazione di divulgazione scientifica Minerva, Caritas, Ordine degli Avvocati della provincia Forlì-Cesena, ecc..) che operano attraverso incontri specifici rivolti agli alunni e aventi come tematica il rispetto della Legalità e l’uso corretto delle nuove tecnologie. Gli alunni del primo biennio sono coinvolti sistematicamente in attività di sensibilizzazione tra le quali si segnala la partecipazione al progetto CUORI CONNESSI. Inoltre, ogni anno in occasione del SID vengono proposte attività di istituto.

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.

Ogni anno si procede con l'aggiornamento per la formazione sul digitale gestita dall'Animatore Digitale nell'ambito del PNSD.

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.

Con la partecipazione dell'Istituto al progetto "Generazioni Connesse" del Safer Internet Center, si prevede anche una fase di autoaggiornamento degli insegnanti tramite materiali informativi sulla sicurezza in internet reperibili sul web, in particolare sul sito di Generazioni Connesse (www.generazioniconnesse.it).

Nell'istituto è presente il Referente per il bullismo e cyberbullismo.

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 i ragazzi 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'E-Policy 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.

Nell'ambito del progetto "Generazioni Connesse" attraverso la pagina del sito di istituto sono pubblicizzati i materiali a disposizione delle famiglie per sensibilizzarle sui problemi legati ad un uso non corretto di internet e delle tecnologie digitali, anche al di fuori della scuola.

Il nostro piano D'AZIONI

AZIONI sviluppate nell'arco dell'a.s.19/20

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

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

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

3.1 - PROTEZIONE dei dati personali

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

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

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

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

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

In questo paragrafo dell'E-Policy 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.

Il trattamento dei dati personali riguarda unicamente le finalità istituzionali della scuola per le quali vengono raccolti solo i dati strettamente necessari. Essi saranno trattati con o senza l'ausilio di strumenti elettronici e comunque automatizzati secondo le modalità e le cautele previste dall'art. 13

del D.Lgs 196/2003 e conservati per il tempo necessario all'espletamento delle attività amministrative e istituzionali.

Il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato riceve poi istruzioni particolareggiate, applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi. All'inizio dell'anno scolastico, viene inoltre fornita ai genitori un'informativa contenente:

- richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori

- liberatorie per l'utilizzo delle immagini e dei video nel sito internet della scuola e/o nel materiale divulgativo relativo ad attività, progetti, concorsi cui partecipano gli studenti.

- il responsabile del trattamento dei dati personali

3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva

2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

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

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

L'accesso a internet è possibile e consentito per la didattica in tutte le classi attraverso reti LAN e WiFi; al momento l'accesso per gli studenti non risulta filtrato quindi le credenziali delle WiFi non devono essere loro fornite, e il lavoro sulle postazioni fisse è vigilato e mediato dai docenti. Tutti gli studenti sono dotati di credenziali personali di accesso ai dispositivi in uso nei laboratori e nei carrelli multimediali.

I docenti, attraverso le credenziali personali in loro possesso, possono accedere alla rete LAN di istituto da qualsiasi postazione interna alla scuola; possono altresì accedere, previa registrazione, alla rete Wifi utilizzando i propri dispositivi (notebook, smartphone, tablet).

Le regole di base relative all'accesso ad Internet faranno parte integrante del Regolamento d'Istituto, e saranno esposte all'albo dell'Istituto, all'interno dei laboratori di informatica.

I genitori saranno informati sulle E-policy d'istituto tramite la pubblicazione del regolamento sul sito web della scuola.

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.

Ogni aula ha a disposizione un PC, laptop o fisso, connesso alla rete dell'istituto, utilizzato dagli insegnanti per la didattica. Non sono utilizzati dagli studenti senza autorizzazione del docente.

3.4 - STRUMENTAZIONE personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli studenti 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 E-Policy 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").

Per gli **studenti**

Per quanto concerne l'utilizzo dei tablet o PC portatili (Attività BYOD – Bring your own device), potranno essere utilizzati solo se permessi dal docente, alla presenza del docente e per ragioni prettamente scolastiche.

La gestione degli strumenti personali - cellulari, tablet ecc. è normata dal REGOLAMENTO di ISTITUTO.

Per i **docenti**

Durante le ore di lezione è consentito ai docenti l'uso di cellulari, PC portatili e tablet di loro proprietà unicamente a scopo didattico e ad integrazione dei dispositivi scolastici disponibili (Attività BYOD – Bring your own device).

Il nostro piano D'AZIONI

AZIONI sviluppate nell'arco dell'anno scolastico 2019/2020.

- Durante il periodo di Didattica a distanza è stata effettuata un'analisi sulla disponibilità e sull'utilizzo dei dispositivi personali da parte degli studenti.

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

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti.
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare gli studenti 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 dei ragazzi.*

Rischi

Gli insegnanti, per la natura stessa del loro lavoro, devono in molti casi fungere da "torre di avvistamento", avamposto privilegiato delle problematiche e dei rischi che bambini e adolescenti possono trovarsi ad affrontare ogni giorno.
Responsabilità degli insegnanti è, dunque, imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente. Tra questi, un'attenzione specifica deve essere prestata ai fenomeni di:

- bullismo/cyberbullismo – una forma di prepotenza virtuale e non, attuata attraverso l'uso di internet e delle tecnologie digitali;

- sexting - pratica di inviare o postare messaggi di testo e immagini a sfondo sessuale, via cellulare o tramite Internet;

- adescamento o grooming – una tecnica di manipolazione psicologica, che gli adulti potenziali abusanti utilizzano online, per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata;

I rischi che gli alunni possono correre a scuola derivano da un uso non corretto dei dispositivi elettronici, in particolare di quelli personali.

Azioni

Scuola e famiglia possono essere determinanti nella diffusione di un atteggiamento mentale e culturale che consideri la diversità come una ricchezza e che educhi all'accettazione, alla consapevolezza dell'altro, al senso della comunità e della responsabilità collettiva. Occorre pertanto rafforzare e valorizzare il Patto di Corresponsabilità educativa previsto dallo Statuto delle studentesse e degli studenti della Scuola Secondaria. La scuola è chiamata ad adottare misure atte a prevenire e contrastare ogni forma di violenza e di prevaricazione; la famiglia è chiamata a collaborare, non solo educando i propri figli, ma anche vigilando sui loro comportamenti.

Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli studenti vi sono le seguenti:

- Diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web.

- Organizzare incontri con esperti (psicologo, Polizia Postale, ecc.) nelle singole classi e aventi per oggetto le tematiche del cyberbullismo, del sexting e dell'adescamento.

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

- Attento monitoraggio da parte del personale docente affinché il presente regolamento venga rispettato.

- Tempestivo intervento tramite opportuna sanzione qualora il regolamento venga disatteso.

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 adottare 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).

Casi di **cyberbullismo**

Si definiscono bullismo tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o a volte un piccolo gruppo). Si tratta, pertanto, di una serie di comportamenti portati avanti ripetutamente nel tempo. Si parla di cyberbullismo quando queste forme di prevaricazione reiterate nel tempo si estendono anche alla vita online. Tale specifica forma di bullismo ha caratteristiche peculiari:

- È pervasivo: il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo;
- È un fenomeno persistente: il materiale messo online vi può rimanere per molto tempo;

- Spettatori e cyberbulli sono potenzialmente infiniti: le persone che possono assistere agli atti di cyberbullismo sono potenzialmente illimitate;
- Occorre tenere presente che il cyberbullo non è mai del tutto consapevole della gravità dei suoi comportamenti, se non viene aiutato ad esserne consapevole.

Qualora ci si trovi di fronte ad un caso di cyberbullismo (denunciato dalla vittima stessa, da persone vicino alla vittima o scoperto da un docente) si procederà nel modo seguente.

Il **docente** venuto a conoscenza del fatto dovrà:

- Informare tempestivamente la referente tramite modulo (Allegato 1);
- Informare tempestivamente il Consiglio di Classe dell'alunno oggetto di cyberbullismo;
- Informare i genitori dell'alunno oggetto di cyberbullismo, offrendo loro la possibilità di avere il supporto della psicologa della scuola per affrontare al meglio la situazione.

La **referente**, in collaborazione con il CdC raccoglierà tutte le informazioni possibili;

Il **CdC**:

- valuterà, a seconda della gravità del caso, come sanzionare il/i responsabile/i (qualora sia stato possibile individuarlo/i);
- Con la collaborazione della psicologa della scuola, proporrà agli studenti attività durante le quali questi possano confrontarsi sull'accaduto;

Il **Dirigente Scolastico** valuterà se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali.

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

Con l'espressione incitamento all'odio (o "discorso di incitamento all'odio", che traduce il concetto di hate speech usato dalle organizzazioni internazionali) o discorso d'odio si intende un particolare tipo di comunicazione che si serve di parole, espressioni o elementi non verbali aventi come fine ultimo quello di esprimere e diffondere odio ed intolleranza, nonché di incitare al pregiudizio e alla paura verso un soggetto o un gruppo di persone accomunate da etnia, orientamento sessuale o religioso, disabilità, appartenenza politica, culturale o sociale e via dicendo. Il fenomeno ha acquisito particolare visibilità ed estensione con la diffusione dei social network.

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.

Azioni

Qualora ci si trovi di fronte ad un caso di hate speech (denunciato dalla vittima stessa, da persone vicino alla vittima o scoperto da un docente) si procederà in maniera analoga ai casi di cyberbullismo.

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.

Il liceo già nell'anno scolastico 2019/2020 ha organizzato, su progetto dell'Animatore Digitale, una serie di cinque incontri (per un totale di 10 ore) propedeutici alla realizzazione di un convegno (n. 2 ore) sulla **Ludopatia** secondo il seguente programma:

1. Esempi di gioco d'azzardo

2. Giochi equi e non equi

3. I numeri e la nostra percezione

4. Prova della conferenza

5. Prove generali

6. Conferenza

Azioni
Qualora ci si trovi di fronte ad un caso di ludopatia e/o dipendenza da internet (denunciato dalla vittima stessa, da persone vicino alla vittima o scoperto da un docente) si procederà in maniera analoga ai casi di cyberbullismo.

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.

Casi di **sexting**

Con il termine sexting si intende l'invio e/o la ricezione e/o la condivisione di testi, video o immagini sessualmente esplicite tramite cellulare o tramite internet.

Azioni
Qualora ci si trovi di fronte ad un caso di sexting (denunciato dalla vittima stessa, da persone vicino alla vittima o scoperto da un docente) si procederà in maniera analoga ai casi di cyberbullismo.

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).

Azioni

È bene che anche gli insegnanti aiutino i propri alunni a tutelarsi, scegliendo con cura chi frequentare online, per evitare che una condotta imprudente possa comportare ripercussioni non banali nella loro vita reale.

Una volta riconosciuti alcuni segni che possono rinviare a una situazione di adescamento online, quali un improvviso calo nel rendimento scolastico; un aumento del tempo trascorso dall'alunno online associato ad una particolare riservatezza al riguardo, allusioni da parte dell'alunno alla frequentazione di una persona più grande, o a regali ricevuti ecc., si procederà nel modo seguente.

Il docente venuto a conoscenza del fatto dovrà:

- Informare tempestivamente la referente tramite modulo (Allegato 1);
- Informare tempestivamente il Consiglio di Classe dell'alunno oggetto di grooming;
- Informare i genitori dell'alunno oggetto di grooming, offrendo loro la possibilità di avere il supporto della psicologa della scuola per affrontare al meglio la situazione;
- La referente, in collaborazione con il CdC raccoglierà tutte le informazioni possibili;
- Il CdC con la collaborazione della psicologa della scuola proporrà agli studenti attività durante le quali gli alunni possano confrontarsi con la tematica in oggetto;
- Il Dirigente valuterà se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali.

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.

La legge n. 38 del 6 febbraio 2006 affida al "Centro Nazionale per il Contrasto della Pedopornografia sulla rete Internet" la lotta a questo odioso crimine.
Il Centro è la risposta della Polizia di Stato ai criminali che usano la rete per delinquere senza frontiere nei confronti dei minori.

È istituito presso il Servizio Polizia postale e delle Comunicazioni del Dipartimento della Pubblica Sicurezza, e si occupa di prevenzione e repressione di questi reati.

L'obiettivo primario è la difesa dei ragazzi in Internet, attraverso servizi di monitoraggio per la ricerca di spazi virtuali clandestini dove si offrono immagini e filmati di minori abusati per un turpe commercio online. Più in generale il monitoraggio continuo focalizza l'attenzione sulla scoperta di siti e dinamiche che possano rappresentare fonte di pericolo nella navigazione dei più giovani.

Per ciò che concerne i siti pedopornografici, la legge istitutiva individua nel Centro il punto di raccordo per la trattazione delle segnalazioni, provenienti sia da altre Forze di Polizia anche straniere, sia da cittadini, da Associazioni di volontariato e da Provider.

Da tutta questa attività il Centro provvede a ricavare l'elenco dei siti pedopornografici della Rete, la c.d. "black list", che viene fornito agli "Internet Service Provider" perché ne venga inibita la navigazione, attraverso sistemi tecnici di filtraggio.
Se navigando ci si imbatte, anche involontariamente, in uno di questi siti interdetti appare un'apposita "stop page", pagina di blocco, contenente l'avviso di interdizione.

Il nostro piano d'azioni

AZIONI sviluppate nell'arco dell'anno scolastico 2019/2020.

- Individuazione dei siti "non sicuri" ed elaborazione di una "black list" con l'inserimento di filtri, di blocchi e limitazioni di accesso.

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

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti anche 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, anche con il coinvolgimento di esperti.
- Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti.

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'E-Policy 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'E-Policy).

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 studenti coinvolti (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 all'adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. È importante ricordare 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.

Si suggeriscono, 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.

Qualora si riscontri la pubblicazione di:

- dati sensibili o riservati (foto, immagini, video personali, informazioni private proprie o di amici; l'indirizzo di casa o il telefono, ecc.);

- contenuti che possano considerarsi in qualche modo lesivi dell'immagine altrui (commenti offensivi, minacce, osservazioni diffamatorie o discriminatorie, foto o video denigratori, videogiochi che contengano un'istigazione alla violenza, ecc.);

- contenuti riconducibili alla sfera sessuale: messaggi, immagini o video a sfondo sessuale, ecc.

andranno opportunamente segnalati per gli interventi opportuni.

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 degli studenti

Per aiutare gli studenti a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;

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

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

Il personale della scuola, anche con l'ausilio tecnico dell'Animatore Digitale, provvederà a conservare le eventuali tracce di una navigazione non consentita su internet o del passaggio di materiali inidonei sui pc della scuola nonché la data e l'ora. Nel caso di messaggi, si cercherà risalire al mittente attraverso i dati del suo profilo. Si cercherà di raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico, alla famiglia ed, eventualmente, alla Polizia Postale. Qualora siano coinvolti più alunni, in qualità di vittime o di responsabili della condotta scorretta, le famiglie degli alunni in questione saranno convocate e informate tempestivamente per un confronto. In base alla gravità dei fatti si provvederà:

- a una nota disciplinare sul registro on-line;
- a una convocazione formale dei genitori degli alunni, tramite segreteria;
- a una convocazione delle famiglie da parte del Dirigente scolastico; per i reati più gravi la scuola si rivolgerà direttamente agli organi di polizia competenti.

Per il telefono cellulare ci si può assicurare che l'alunno vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine, conservando così il numero del mittente. Per le segnalazioni di fatti rilevanti si agirà conformemente a quanto stabilito nel Regolamento d'Istituto. In caso di abusi sessuali, la denuncia all'autorità giudiziaria o agli organi di Polizia, da parte degli insegnanti o del Dirigente scolastico costituisce il passo necessario per avviare un intervento di tutela a favore della vittima e attivare un procedimento penale nei confronti del presunto colpevole. La presa in carico di situazioni di abuso sessuale, così delicate e complesse, richiede un approccio multidisciplinare, da parte di diverse figure professionali. L'intervento dovrebbe riguardare gli ambiti medico, socio-psicologico e giudiziario. Il compito della scuola è quello di prevenire l'abuso e, nel caso questo avvenga, di aiutare l'eventuale vittima, in quanto ha al suo interno aspetti relazionali ed educativi che possono contribuire alla crescita serena del minore. Per riuscire in questi intenti la scuola collabora con altre figure professionali e le famiglie, scambiando informazioni e condividendo progetti e prassi operative, favorendo occasioni di confronto e di dialogo.

La scuola non può intervenire su ciò che gli alunni svolgono fuori da essa con strumenti digitali ma qualora il docente venisse a conoscenza di eventuali atti scorretti come la condivisione di foto non autorizzate o l'insulto da parte di un alunno ad un compagno sul gruppo classe di WhatsApp (la creazione dei gruppi classe su WhatsApp è oggi una pratica molto diffusa) dovrà tempestivamente invitare le famiglie degli alunni coinvolti ad un attento monitoraggio delle attività svolte dai propri figli in rete.

5.3. - Gli attori sul territorio

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

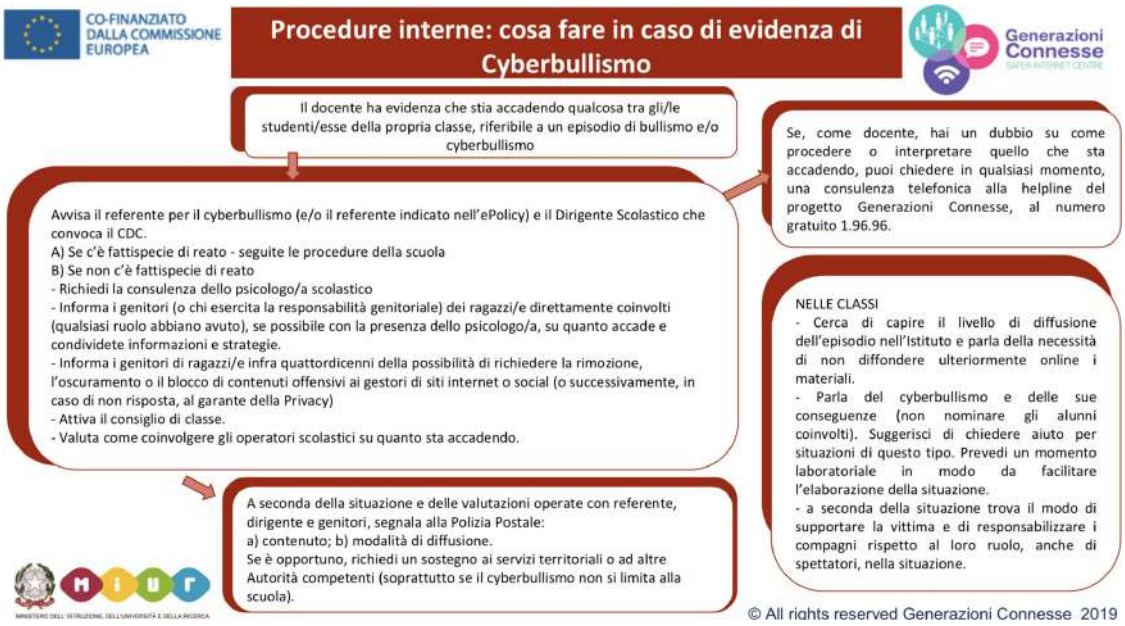
Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza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

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

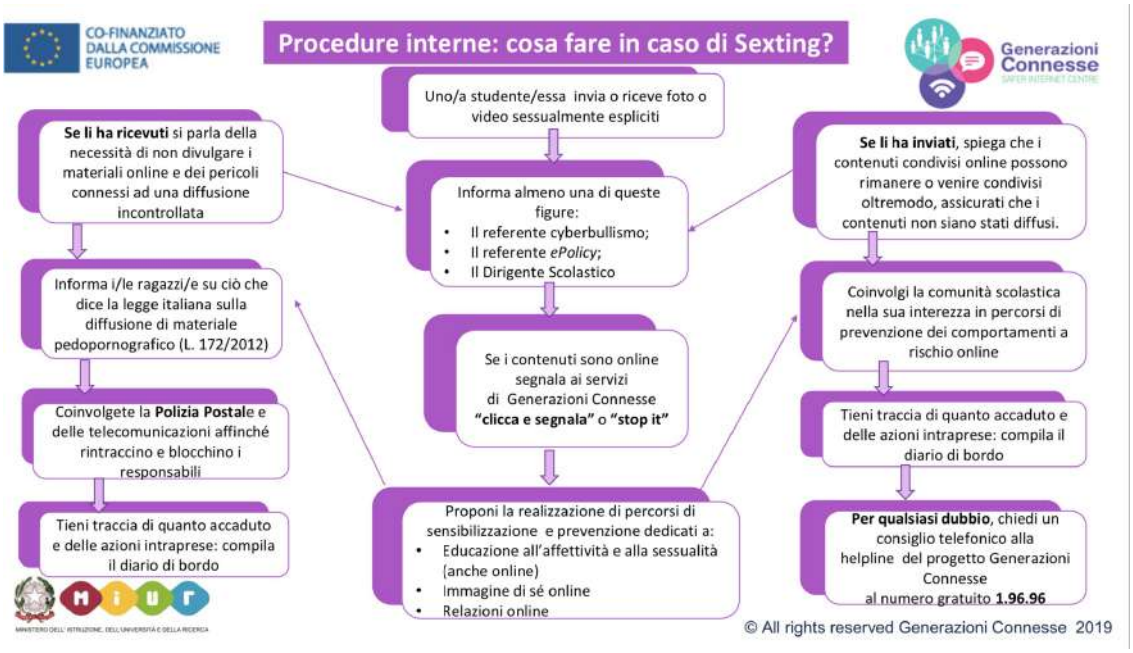
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

5.4. - Allegati con le procedure

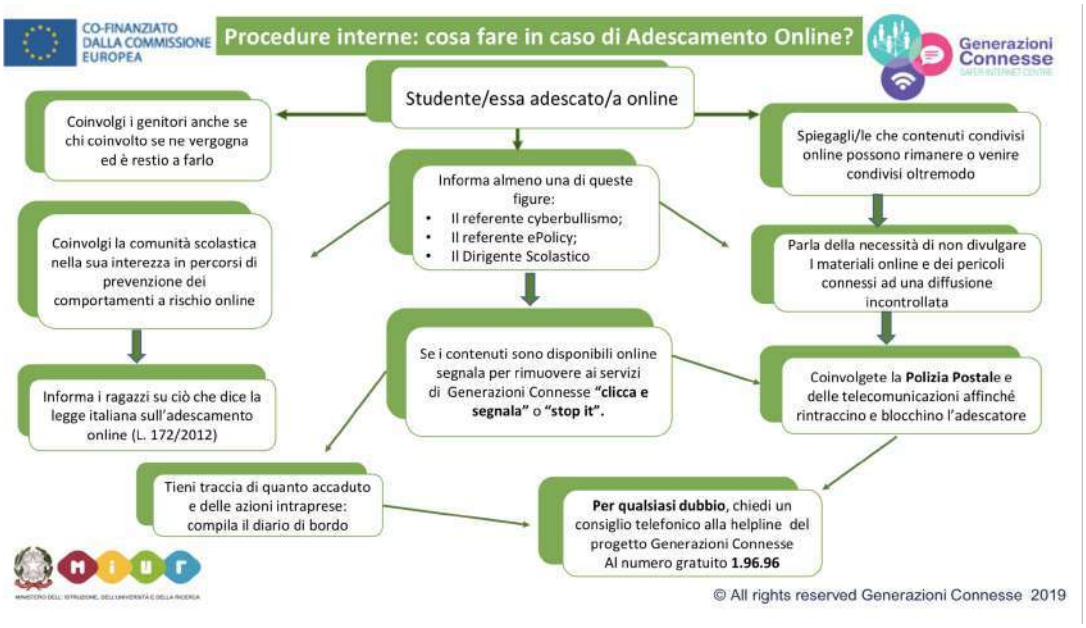
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



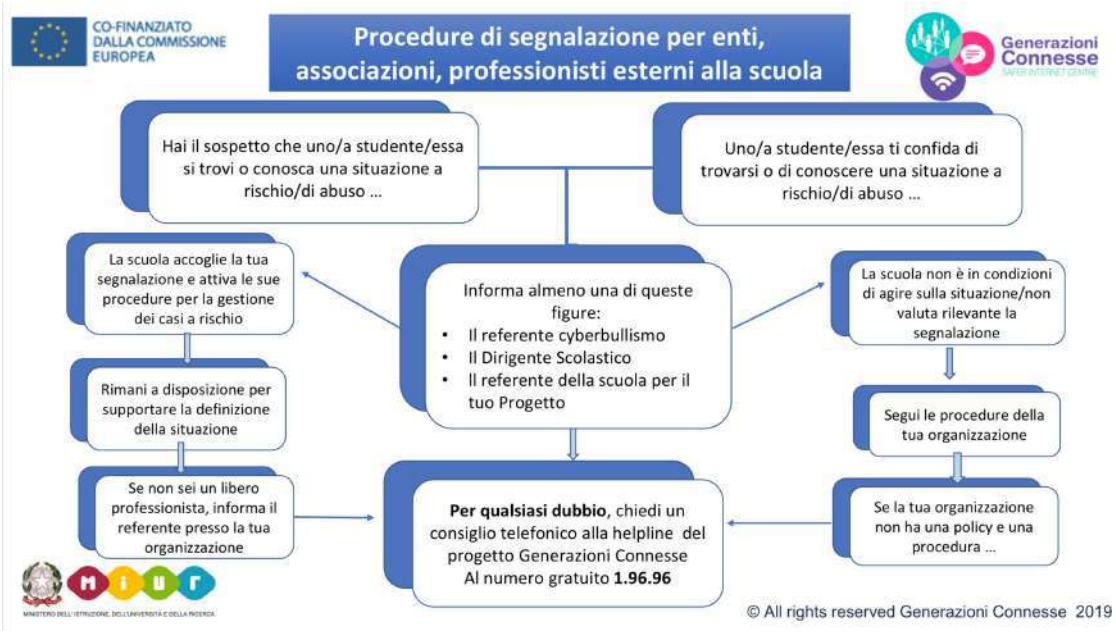
Procedure interne: cosa fare in caso disexting?



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

Per quanto riguarda la gestione dei casi il nostro Istituto ha individuato una figura referente. La segnalazione del caso dovrà quindi essere fatta dal singolo docente, tramite modulo allegato al presente documento (Allegato 1), alla referente, la quale si occuperà di raccogliere tutte le informazioni possibili e di segnalare l'accaduto al Dirigente. Sarà poi il Dirigente a valutare se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali o se il caso vada gestito all'interno della scuola con il coinvolgimento del Consiglio di Classe e delle famiglie degli alunni coinvolti.

Il nostro piano D'AZIONI

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

- diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web, condividendo materiali messi a disposizione sul sito del progetto "Generazioni connesse";
- richiedere all'inizio di ogni anno scolastico autorizzazione esplicita da parte dei genitori all'utilizzo dei dati personali degli alunni (es. liberatoria per la pubblicazione di foto, immagini, video relativi al proprio/a figlio/a per la partecipazione a progetti didattici e altro);
- far rispettare il divieto di utilizzo di dispositivi digitali propri, quali lo smartphone, agli studenti in orario scolastico. Le dovute eccezioni (uso del cellulare per comunicazioni alunno-famiglia in occasione di uscite didattiche) andranno espressamente regolamentate e dovranno comunque avvenire sotto la supervisione diretta di un docente responsabile;

Azioni utili a impedire un utilizzo incauto, scorretto o criminoso degli strumenti digitali sono:

- bloccare l'accesso a un sito o a un insieme di pagine impedendone la consultazione;
- controllare periodicamente i siti visitati dagli alunni;
- affidare a un gruppo di docenti scelto le regole di filtraggio.