Documento di ePolicy

SAIC81900C

IST.COMPR. EBOLI III S.CECILIA

PIAZZA FRATELLI CIANCO - 84025 - EBOLI - SALERNO (SA)

Gabriella Ugatti

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

Perché è importante dotarsi di una E-policy?

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi

all'uso di Internet.

L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

L'Istituto Comprensivo "Virgilio", dopo aver constatato una sempre più precoce esposizione degli utenti alle occasioni di interazione con Internet tramite una vasta gamma di dispositivi facilmente alla loro portata, con questo documento mira a promuovere un uso consapevole e critico da parte delle alunne e degli alunni delle tecnologie digitali e di internet, a far acquisire loro procedure e competenze "tecniche" ma anche corrette norme comportamentali, a prevenire ovvero rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali.

Gli utenti, soprattutto minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete, ma anche delle opportunità. E' importante sottolineare come sia necessario adottare una strategia integrata e globale, che coinvolga tutti gli attori della scuola: studenti e studentesse, docenti, genitori, e personale Ata, per l'affermazione di un modello di scuola come comunità.

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 Dirigente Scolastica, congiuntamente ai suoi collaboratori, è garante per la sicurezza on-line e off-line di tutti i membri della comunità scolastica. In linea con il quadro normativo di riferimento e le indicazioni del MIUR, promuove la cultura della sicurezza online ed ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali;

L'animatore digitale supporta il personale scolastico da un punto di vista non solo

tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale";

Il referente bullismo e cyberbullismo, come da art. 4 Legge n.71/2017, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo", coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo;

I docenti accompagnano e supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso dei dispositivi tecnologici che si connettono alla Rete, integrando l'uso delle tecnologie digitali nella didattica;

Il personale Amministrativo, Tecnico e Ausiliario (ATA) è 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 di bullismo/cyberbullismo;

Studentesse e studenti sono tenuti ad utilizzare al meglio le tecnologie digitali. Con il supporto della scuola devono imparare a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le. La partecipazione attiva a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete li rende promotori di quanto appreso anche attraverso possibili percorsi di peer education;

I Genitori, in continuità con l'Istituto scolastico con il quale condividono la responsabilità educativa e formativa (1° e 2° comma dell'art. 2048 c.c; 1° comma dell'art. 30 della Costituzione; art. 147 del c.c.), promuovono in modo partecipe e attivo i percorsi di educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali;

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

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

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).

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

1.4 - Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.

L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

Dal momento dell'approvazione, ad ogni avvio dell'anno scolastico, il documento di e-policy sarà integrato nelle attività di accoglienza, pubblicizzato e socializzato tramite il sito di istituto. Per raggiungere opportunamente tutte le fasce di età, saranno redatte diverse versioni che utilizzino un linguaggio, modalità e canali di comunicazione più adatti al target di riferimento.

1.5 - Gestione delle infrazioni alla ePolicy

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

Richiamo verbale; Sanzioni estemporanee commisurate alla gravità della violazione commessa (assegnazione di attività aggiuntive da svolgere a casa sui temi di Cittadinanza e Costituzione); Nota informativa ai genitori o tutori mediante registro elettronico; Convocazione dei genitori o tutori per un colloquio con l'insegnante; Convocazione dei genitori o tutori per un colloquio con il Dirigente Scolastico.

Denunce di bullismo On-line saranno trattate in conformità con la legge.

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.

da compilare con le indicazioni contenute nella lezione

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

da compilare con le indicazioni contenute nella lezione

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

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

Azioni da svolgere nei prossimi 3 anni:

- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy 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 genitori dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

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

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

Fonti di legittimazione:

Indicazioni Nazionali 2012 e Nuovi Scenari 2018:

La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione per il lavoro, il tempo libero e la comunicazione. Essa implica abilità di base nelle tecnologie dell'informazione e della comunicazione (TIC): l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet. (IN, 2012)

La responsabilità è l'atteggiamento che connota la competenza digitale. Solo in minima parte essa è alimentata dalle conoscenze e dalle abilità tecniche, che pure bisogna insegnare. I nostri ragazzi, anche se definiti nativi digitali, spesso non sanno usare le macchine, utilizzare i software fondamentali, fogli di calcolo, elaboratori di testo, navigare in rete per cercare informazioni in modo consapevole. Sono tutte abilità che vanno insegnate. Tuttavia, come suggeriscono anche i documenti europei sulla educazione digitale, le abilità tecniche non bastano. La maggior parte della competenza è costituita dal sapere cercare, scegliere, valutare le informazioni in rete e nella responsabilità nell'uso dei mezzi, per non nuocere a se stessi e agli altri. (Nuovi scenari, 2018)

LEGGE n° 92, art. 5 del 20 agosto 2019:

Nel rispetto dell'autonomia scolastica, l'offerta formativa erogata nell'ambito dell'insegnamento dell'educazione civica prevede almeno le seguenti abilita' e conoscenze digitali essenziali, da sviluppare con gradualita' tenendo conto dell'eta' degli alunni e degli studenti:

a) analizzare, confrontare e valutare criticamente la credibilita' e l'affidabilita' delle fonti di dati, informazioni e contenuti digitali;

b) interagire attraverso varie tecnologie digitali e individuare i mezzi e le forme di comunicazione digitali appropriati per un determinato contesto;

c) informarsi e partecipare al dibattito pubblico attraverso l'utilizzo di servizi digitali pubblici e privati; ricercare opportunita' di crescita personale e di cittadinanza partecipativa attraverso adeguate tecnologie digitali;

d) conoscere le norme comportamentali da osservare nell'ambito dell'utilizzo delle tecnologie digitali e dell'interazione in ambienti digitali, adattare le strategie di comunicazione al pubblico specifico ed essere consapevoli della diversita' culturale e generazionale negli ambienti digitali;

e) creare e gestire l'identita' digitale, essere in grado di proteggere la propria reputazione, gestire e tutelare i dati che si producono attraverso diversi strumenti digitali, ambienti e servizi, rispettare i dati e le identita' altrui; utilizzare e condividere informazioni personali identificabili proteggendo se stessi e gli altri;

f) conoscere le politiche sulla tutela della riservatezza applicate dai servizi digitali relativamente all'uso dei dati personali;

g) essere in grado di evitare, usando tecnologie digitali, rischi per la salute e minacce al proprio benessere fisico e psicologico; essere in grado di proteggere se' e gli altri da eventuali pericoli in ambienti digitali; essere consapevoli di come le tecnologie digitali possono influire sul benessere psicofisico e sull'inclusione sociale, con particolare attenzione ai comportamenti riconducibili al bullismo e al cyberbullismo.

PNSD, 4.2 azioni #14-18;

Definire una matrice comune di competenze digitali che ogni studente deve sviluppare Sostenere i docenti nel ruolo di facilitatori di percorsi didattici innovativi, definendo con loro strategie didattiche per potenziare le competenze chiave

Coinvolgere gli studenti attraverso format didattici innovativi e 'a obiettivo'

Innovare i curricoli scolastici

Raccomandazioni del Consiglio Europeo

Le competenze chiave sono quelle di cui tutti hanno bisogno per la realizzazione e lo sviluppo personale, l'occupabilità, l'inclusione sociale, uno stile di vita sostenibile, una vita fruttuosa in società pacifiche, una gestione della vita attenta alla salute e la cittadinanza attiva. Esse si sviluppano in una prospettiva di apprendimento permanente, dalla prima infanzia a tutta la vita adulta, mediante l'apprendimento formale, non formale e informale in tutti i contesti, compresi la famiglia, la scuola, il luogo di lavoro, il vicinato e altre comunità.

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. Conoscenze, abilità e atteggiamenti essenziali legati a tale competenza Le persone dovrebbero comprendere in che modo le tecnologie digitali possono essere di aiuto alla comunicazione, alla creatività e all'innovazione, pur nella consapevolezza di quanto ne consegue in termini di opportunità, limiti, effetti e rischi. Dovrebbero comprendere i principi generali, i meccanismi e la logica che sottendono alle tecnologie digitali in evoluzione, oltre a conoscere il funzionamento e l'utilizzo di base di diversi dispositivi, software e reti. Le persone dovrebbero assumere un approccio critico nei confronti della validità, dell'affidabilità e dell'impatto delle informazioni e dei dati resi disponibili con strumenti digitali ed essere consapevoli dei principi etici e legali chiamati in causa con l'utilizzo delle tecnologie digitali. 4.6.2018 IT Gazzetta ufficiale dell'Unione europea C 189/9 Le persone dovrebbero essere in grado di utilizzare le tecnologie digitali come ausilio per la cittadinanza attiva e l'inclusione sociale, la collaborazione con gli altri e la creatività nel raggiungimento di obiettivi personali, sociali o commerciali. Le abilità comprendono la capacità di utilizzare,

accedere a, filtrare, valutare, creare, programmare e condividere contenuti digitali. Le persone dovrebbero essere in grado di gestire e proteggere informazioni, contenuti, dati e identità digitali, oltre a riconoscere software, dispositivi, intelligenza artificiale o robot e interagire efficacemente con essi. Interagire con tecnologie e contenuti digitali presuppone un atteggiamento riflessivo e critico, ma anche improntato alla curiosità, aperto e interessato al futuro della loro evoluzione. Impone anche un approccio etico, sicuro e responsabile all'utilizzo di tali strumenti.

DigComp 2.1:

1: Alfabetizzazione su informazioni e dati: identificare, organizzare e conservare le informazioni digitali;

2: Comunicazione e collaborazione: comunicare, condividere e collaborare con gli altri;

3: Creazione di contenuti digitali: creare, modificare e programmare contenuti;

4: Sicurezza: protezione personale, dei dati e dell'identità digitale;

5: Risolvere problemi: utilizzare creativamente le tecnologie digitali e risolvere problemi.

OBIETTIVI GENERALI DEL CURRICOLO VERTICALE

Per la scuola dell'infanzia:

l'alunna/o riconosce e denomina correttamente alcuni degli hardware principali, quali LIM, PC, tablet, stampante, mouse; è in grado di utilizzare le frecce direzionali, i tasti spazio e invio e muovere il mouse; esegue giochi ed esercizi di tipo logico sul tablet o pc

Per la scuola primaria:

l'alunna/o è in grado di creare ed inviare le email, sa utilizzare la stampante; sa organizzare, denominare e conservare le cartelle; sa utilizzare i programmi di scrittura, di calcolo, di presentazione dati; sa eseguire giochi e conosce la programmazione a blocchi e la robotica educativa di base.

Per la scuola secondaria:

l'alunna/o sa gestire e organizzare le informazioni sul cloud, sa identificare una rete

internet, sa installare un software e gestire un sistema operativo; sa lavorare in modo collaborativo con programmi di scrittura, di calcolo e programmi creativi; conosce i pericoli relativi all'uso scorretto di internet, alle violazioni di privacy e copyright, sa generare password valide e sicure; conosce la programmazione a blocchi, ha nozioni di programmazione testuale e conosce e sa usare la robotica di base e avanzata

---

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 grado di formazione della scuola sarà fotografato annualmente dal Selfie, strumento europeo nato per migliorare l'uso delle tecnologie digitali per la didattica e l'apprendimento. Fonti di legittimazione sono le sei aree di competenza del DigCompEdu:

1: Impegno professionale: usare le tecnologie digitali per la comunicazione, la collaborazione e lo sviluppo professionale;

2: Risorse digitali: ricerca, condivisione e creazione di risorse digitali;

3: Insegnamento e apprendimento: gestire e orchestrare l'uso delle tecnologie digitali nell'insegnamento e nell'apprendimento;

4: Valutazione: utilizzo di tecnologie e strategie digitali per migliorare la valutazione;

5: Responsabilizzare le/gli studentesse/i: utilizzare le tecnologie digitali per migliorare l'inclusione, la personalizzazione e il coinvolgimento attivo delle studentesse e degli studenti;

6: Facilitare l'acquisizione delle Competenze Digitali: consentire ad alunne e alunni di utilizzare in modo creativo e responsabile le tecnologie digitali per l'informazione, la

comunicazione, la creazione di contenuti, il benessere e la risoluzione dei problemi.

Congiuntamente alle azioni del PNSD (azioni #25-27) ed agli obiettivi proposti dall'Agid, Agenzia italiana per il digitale, sarà pianificata su piano annuale e triennale, l'azione formativa in linea con i progressi e le innovazioni tecnologiche.

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.

Coerentemente con quanto previsto dal PNSD, l'Istituto si avvale dell'Animatore Digitale, che coordina la diffusione dell'innovazione digitale e collabora con tutti i soggetti che possono contribuire alla realizzazione degli obiettivi del Piano. Anche il percorso della formazione specifica dei docenti sull'utilizzo consapevole e sicuro di INTERNET prevede momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi. Sono diffuse informazioni circa opportunità formative esterne in presenza e/o a distanza. Si prevede, inoltre, la promozione di attività formative interne (seminari, workshop, caffè digitali, ecc.), avvalendosi di risorse interne e/o esterne. Il docente referente partecipa a specifiche iniziative di formazione dedicate alla prevenzione e contrasto del 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 ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023)

- 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.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie

digitali.

- Organizzare incontri con esperti per i docenti sulle competenze digitali..

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

Ogni docente è responsabile del proprio username e della propria password di accesso al registro elettronico, alle email di istituto e delle password d'accesso alla rete wifi dell'Istituto. In caso di smarrimento o dimenticanza i docenti devono rivolgersi alla segreteria o al team digitale e far presente il problema. A tutto il personale, docente e non docente, è stato raccomandato di non salvare le password nei browser se gli strumenti vengono utilizzati da più persone e di effettuare sempre il logout dai siti a cui si accede con login e dalle caselle di posta personali. In ogni caso è consigliata la navigazione in modalità incognito del browser sulle periferiche della scuola (PC, notebook, tablet, ecc.). Si invitano altresì i docenti ad una custodia responsabile di tutte le credenziali di accesso con password segrete, alfanumeriche e sicure, cambiate almeno ogni tre mesi.

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 disponibile in tutti i plessi dell'Istituto. Nei laboratori di informatica e nelle aule sono attivi filtri per la navigazione sicura. Su tutti i dispositivi sono stati installati sistemi atti a rilevare la presenza e bloccare l'esecuzione di malware e vengono aggiornati automaticamente (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico. Ogni dispositivo ha attivo un Firewall. Il traffico viene bloccato da e verso url presenti nella blacklist implementata sul Firewall. Le impostazioni sono definite e manutenute dall'amministratore di rete esterno che ha anche funzione di consulente tecnico per il parco informatico. Ciascun docente è tenuto a segnalare eventuali disservizi in forma scritta. In merito alla gestione degli accessi (password, backup, ecc.) nei computer presenti nelle aule e nei laboratori sono previsti tre profili di accesso (amministratore - docenti autorizzati) con relative password. A tutela della sicurezza e del buon funzionamento dei dispositivi, sui device della scuola è possibile effettuare installazioni e aggiornamenti di software solo tramite la password amministratore, fornita al personale di assistenza tecnica e all'Animatore Digitale. E' inoltre fatto divieto di inserire file sul server o sul computer principale ovvero di scaricare da Internet software non autorizzati.

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.

Per la gestione della comunicazione interna e per gli adempimenti amministrativi del personale docente, nell' Istituto viene utilizzato il registro elettronico "AXIOS" tramite il quale i docenti firmano giornalmente la loro presenza, registrano assenze, uscite anticipate e ritardi, presenze, riportano le attività e le valutazioni effettuate e visualizzano le comunicazioni inviate. Il medesimo strumento è utilizzato dalle famiglie: utilizzando una password personale possono accedere alla bacheca delle comunicazioni, al registro presenze, al giornale di classe (attività svolta, compiti assegnati, note disciplinari o di altra natura) e all'area dedicata al documento di valutazione da scaricare alla fine del primo e del secondo quadrimestre.

Gli scambi comunicativi interni alla scuola vengono gestiti dagli insegnanti e dagli uffici amministrativi anche attraverso l'account di posta elettronica legato al dominio della scuola @istitutovirgilioeboli.com. Gli scambi comunicativi tra docenti, seguono le stesse procedure previste in precedenza, con l'aggiunta dell'utilizzo di chat di messaggistica di gruppo, regolamentate da uno specifico documento allegato.

Per la comunicazione esterna la scuola si avvale di un sito web (https://www.istitutovirgilioeboli.edu.it) e dei canali social ufficiali, che si configurano quale strumento di comunicazione e condivisione di contenuti educativi e di attività didattico-formative. Tutti i contenuti sono pubblicati direttamente sotto la supervisione dei responsabili del sito e del team digitale, che ne valutano con il Dirigente scolastico l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc… e la rispondenza ai requisiti di sicurezza e tutela dei dati personali. Per la gestione del sito il dirigente sottoscrive regolare contratto con personale esterno e affida l'incarico scritto ad un docente interno. Per le pubblicazioni vengono rispettate le disposizioni di legge sulla proprietà intellettuale. In particolare, per la pubblicazione di immagini degli alunni legate ad attività prettamente didattiche, viene acquisita ad inizio anno scolastico la preventiva liberatoria da parte dei genitori o da chi ne esercita la funzione. Anche in presenza di liberatoria da parte dei genitori, la scuola procede con la massima attenzione, adottando il principio di massima precauzione: si danno indicazioni affinché per la pubblicazione si scelgano immagini a campo lungo, senza primi piani e che ritraggano gruppi in attività piuttosto che singoli individui.

Ulteriore strumento digitale ad uso del personale scolastico e delle allieve e degli allievi è il cloud di Google Workspace con relative APP, un ambiente in cui poter operare in maniera collaborativa nel rispetto della normativa contenuta nella GDPR. Per ragioni di sicurezza gli account degli adulti e dei bambini hanno impostazioni diversificate sia per la comunicazione all'esterno del dominio sia per la fruizione di

canali non autorizzati.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente ***ePolicy*** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

L'utilizzo di strumentazione personale è stato valutato con attenzione sia in relazione alle implicazioni dettate dagli accessi alla rete attraverso connessioni private e non controllabili sia rispetto alla responsabilità legata alla custodia del device. Considerata tuttavia la valenza didattico educativa ed inclusiva dell'utilizzo di strumenti digitali in classe è concesso l'utilizzo di BYOD (PC/Tablet) esclusivamente per scopi didattici e sotto la sorveglianza del docente nel rispetto di quanto indicato dalla normativa nazionale inerente alla tematica; non è consentito invece l'uso del cellulare da parte degli allievi come ribadito nel patto educativo di corresponsabilità e nel regolamento d'Istituto. I docenti possono utilizzare il telefono cellulare solo in caso di emergenza o per motivi legati all'adempimento del proprio lavoro. L'uso di dispositivi elettronici personali è consentito solo a scopo didattico-educativo. Durante l'orario di servizio al restante personale scolastico l'uso degli strumenti personali (cellulari, tablet, ecc.) è consentito per comunicazioni personali urgenti. L'uso di altri dispositivi elettronici personali è permesso solo per attività funzionali al servizio e preventivamente autorizzate.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).

Scegliere almeno 1 di queste azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte deglistudenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte delpersonale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto perredigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- 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

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

Scegliere almeno 1 di queste azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli
- studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte delpersonale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto perredigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione degli studenti/studentesse suindicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamentisull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori

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

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

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).

Da implementare con le indicazioni contenute nella lezione.

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 di cittadinanza è l'obiettivo primario del nostro istituto, da perseguire in sinergia con le famiglie e attraverso la quotidiana azione educativa: la scuola ha inserito tra i contenuti del curricolo di Educazione Civica percorsi didattici e progetti, che suggeriscono riflessioni utili a prevenire, riconoscere e contrastare il fenomeno dell'hate speech; al contempo sono proposte agli alunni attività finalizzate al superamento degli stereotipi e al potenziamento delle capacità espressive/argomentative e progettate all'interno di specifici percorsi di formazione per i docenti.

4.4 - Dipendenza da Internet e gioco online

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

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

benessere digitale?

La scuola nell'educare ad un uso consapevole e responsabile delle tecnologie digitali riserva particolare attenzione non solo alle modalità di accesso e utilizzo degli strumenti ma anche alla riflessione sui tempi da dedicarvi al fine di prevenire e contrastare fenomeni di dipendenza da Internet e dal gioco on line, fenomeni che a causa della situazione pandemica e della conseguente didattica a distanza sono diventati oggetto di riflessione. Gli interventi educativi sono attivati in sinergia con le famiglie attraverso il dialogo e il confronto e finalizzati alla prevenzione e alla promozione del benessere e alla tutela della salute dei minori.

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.

La scuola coglie appieno le potenzialità e rischi connessi all'utilizzo delle immagini come strumento privilegiato di narrazione di sé e della realtà nella società attuale.

Gli allievi sono esposti, specialmente via web, a stimoli audiovisivi che non sempre si configurano come modelli positivi di stili di vita e che spesso violano il rispetto delle norme sulla sicurezza e ledono la dignità e l'integrità personale, ma che costituiscono un'attrattiva e invitano all'emulazione. Pertanto attraverso l'azione didattico educativa e il dialogo con le famiglie il nostro istituto promuove azioni di formazione/informazione mirate all'adozione di comportamenti attenti e responsabili in merito all'utilizzo e alla diffusione in Rete delle immagini personali, vigila e segnala in prima istanza alle famiglie eventuali condotte scorrette o dannose e, se necessario, all'autorità giudiziaria eventi che possano configurarsi come reati.

4.6 - Adescamento online

Il ***grooming*** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di ***teen dating*** (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies – l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

Tra le azioni che il nostro istituto intraprende per informare sui rischi della Rete sono comprese anche quelle volte a fornire ai minori e alle loro famiglie gli elementi per individuare un caso di adescamento on line attraverso l'esplicitazione delle sue fasi (amicizia, solidificazione del rapporto, valutazione del rischio, esclusività del rapporto) e sostiene con fermezza la necessità che i genitori vigilino puntualmente sulle frequentazioni virtuali dei minori. Particolare attenzione viene posta nel riconoscere i segnali che possono manifestare i bambini vittime di adescamento on line (conoscenze nel campo della sessualità non adatte all'età, disagio e imbarazzo nel commentare video o immagini ricevute o realizzate, amicizie on line esclusive di altre…).

L'azione educativa a prevenzione e contrasto di questo fenomeno si avvale delle opportunità formative offerte da percorsi di educazione all'affettività e alla sessualità condotti anche da personale qualificato esterno alla scuola e dalla collaborazione con i professionisti dello sportello d'ascolto. In caso si verifichino episodi di rilevanza, in particolar modo in ambito penale, la scuola interviene con segnalazioni alle autorità competenti.

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.

Considerata l'età degli alunni, il nostro istituto tratta il tema della pedopornografia con la massima cautela, ponendosi come punto di riferimento per la comunità. Nel "Regolamento di prevenzione e contrasto al bullismo e al cyberbullismo" l'istituto fornisce indicazioni sulla normativa di riferimento e strumenti utili per segnalare casi.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).

Scegliere almeno 1 di queste azioni:

☐ Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

☐ Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.

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/studentesse.

☐ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.

☐ Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.

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

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire).

Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).

Nelle procedure:

- sono indicate le **figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso**.
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

Inoltre, la scuola **individua le figure che costituiranno un team** preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la **collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio** (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica.

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e

studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

A seguire, le problematiche a cui fanno riferimento le procedure allegate:

- **Cyberbullismo**: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online**: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting**: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per

segnalare la presenza di materiale pedopornografico online.

Azioni di informazione e prevenzione, che comprendono momenti di formazione per docenti e interventi educativi rivolti alle allieve e agli allievi per consentire a tutti di riconoscere episodi di bullismo/cyberbullismo, i relativi responsabili e le procedure da rispettare in caso si verifichino episodi accertati.

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

- CASO A (SOSPETTO) – Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
- CASO B (EVIDENZA) – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

Per tutti i dettagli fate riferimento agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

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

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;

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

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

Nel caso si verifichino episodi di bullismo/cyberbullismo i docenti li segnalano al Dirigente e al referente d'istituto che procederanno alla loro verifica e valutazione in collaborazione con docenti, alunni e famiglie. Come già segnalato, all'interno del "Regolamento di Prevenzione e contrasto al bullismo e cyberbullismo" sono indicati riferimenti (siti e numeri telefonici) per reperire informazioni e/o per segnalare un utilizzo improprio del web.

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.

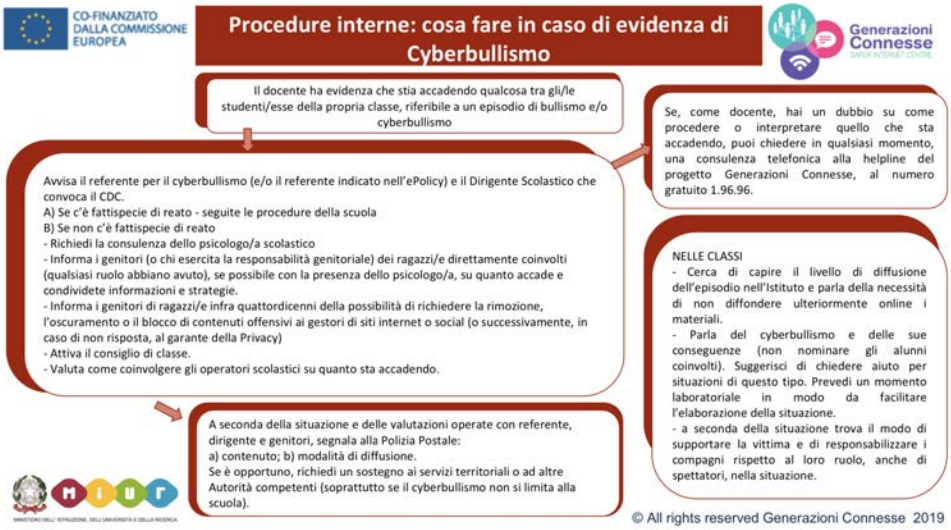
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare 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.

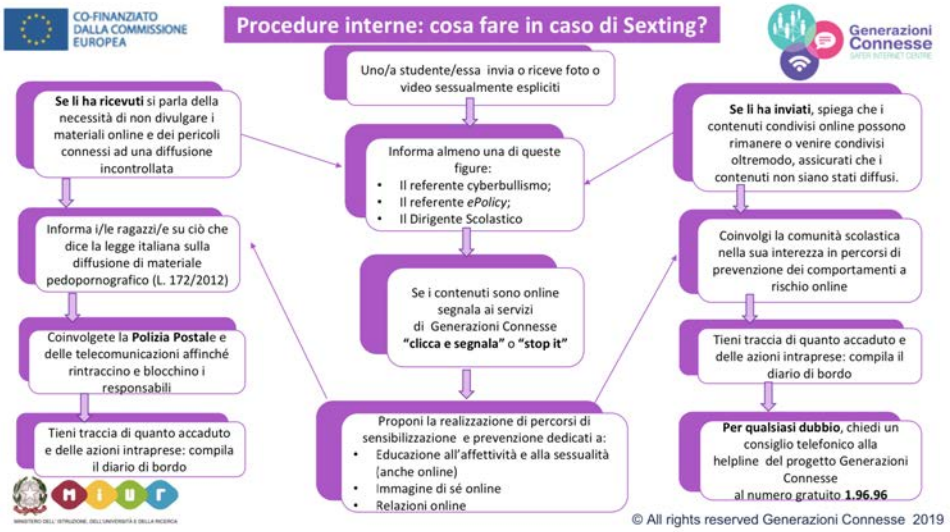
La scuola si avvale da anni della collaborazione di associazioni ed enti territoriali per attivare progetti didattico educativi e formativi rivolti ad allieve e allievi, sulle tematiche dell'Educazione Civica, la gestione delle emozioni e la mediazione dei conflitti. Tuttavia l'utilizzo sempre maggiore delle tecnologie digitali da parte dei bambini per ragioni ludiche e didattiche ha focalizzato la nostra attenzione sull'educazione digitale soprattutto in merito alle problematiche connesse all'accesso sicuro alla Rete, alla tutela della salute e del benessere, all'uso consapevole delle TIC. Sono dunque realizzati all'interno della scuola laboratori didattici e incontri di formazione con l'intervento di figure professionali qualificate.

5.4. - Allegati con le procedure

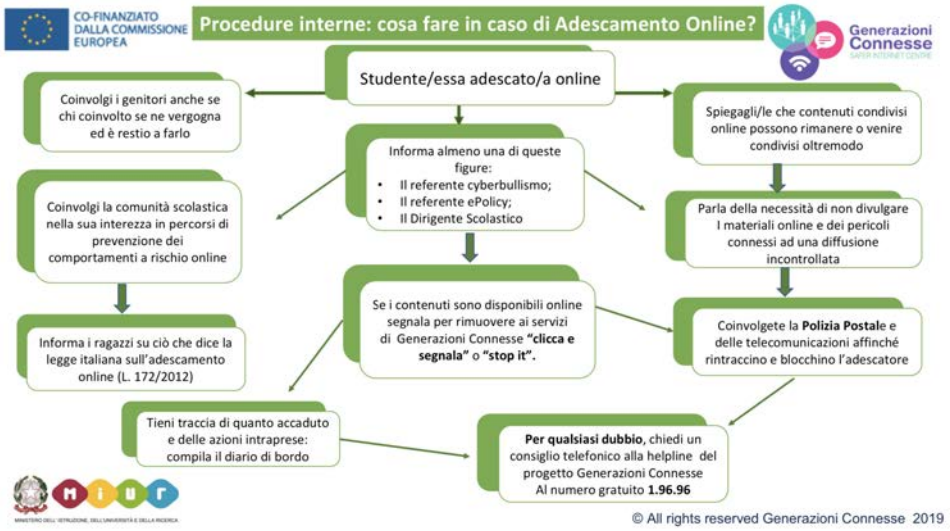
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



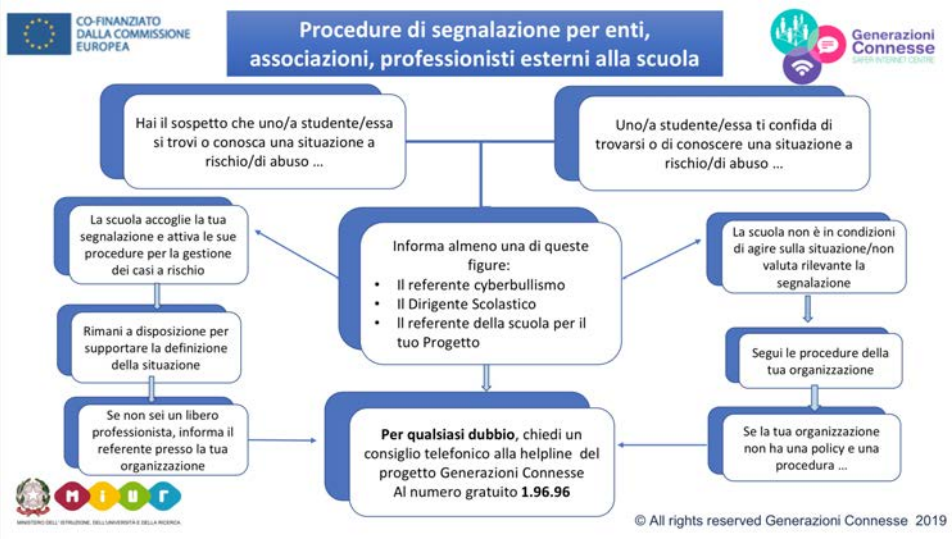
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

netiquette servizi di messaggistica

Il nostro piano d'azioni

Sulla base delle "Linee guida per l'uso positivo delle tecnologie digitali e della prevenzione dei rischi nelle scuole", vengono assunti i seguenti punti per una collaborazione sinergica tra scuola-famiglia-servizi territoriali, al fine di creare un modello lineare di azioni condivise:

- coinvolgimento di tutti gli attori della scuola: studenti e studentesse, docenti, genitori e personale ATA, per l'affermazione di un modello di scuola come comunità;
- alleanza educativa tra scuola e famiglia;

- interventi educativi ed azioni di supporto, quale prevenzione per eventuali comportamenti a rischio;
- misure preventive specifiche di tutela anche con l'ausilio di attori territoriali, come Polizia postale ed ATS per servizi specialistici regionali;
- promozione dell'educazione al rispetto;
- sviluppo del pensiero critico;
- promozione dell'Educazione Civica Digitale.