Documento di ePolicy

TOIC865006

I.C. FAVRIA

PIAZZA REPUBBLICA 6 - 10083 - FAVRIA - TORINO (TO)

Valeria Miotti

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

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

5. Gestione delle infrazioni alla ePolicy
6. Integrazione dell'ePolicy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

2. **Formazione e curricolo**
    1. Curricolo sulle competenze digitali per gli studenti
    2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
    3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
    4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
    1. Protezione dei dati personali
    2. Accesso ad Internet
    3. Strumenti di comunicazione online
    4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
    1. Sensibilizzazione e prevenzione
    2. Cyberbullismo: che cos'è e come prevenirlo
    3. Hate speech: che cos'è e come prevenirlo
    4. Dipendenza da Internet e gioco online
    5. Sexting
    6. Adescamento online
    7. Pedopornografia
5. **Segnalazione e gestione dei casi**
    1. Cosa segnalare
    2. Come segnalare: quali strumenti e a chi
    3. Gli attori sul territorio per intervenire
    4. Allegati con le procedure

Perché è importante dotarsi di una 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.

Il presente documento è volto a regolamentare i comportamenti nei confronti dell'utilizzo delle tecnologie dell'informazione e delle comunicazioni nella didattica , in ambito scolastico e anche

extra-scolastico, relativamente alle attività di compiti assegnati a casa o di attività svolta in modalità di didattica a distanza .
L'intento della scuola è quello di promuovere l'uso consapevole e critico da parte degli alunni delle tecnologie digitali e di Internet , di far acquisir loro procedure e competenze tecniche, ma anche corrette norme comportamentali, di prevenire ovvero rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali

---

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.

IL DIRIGENTE SCOLASTICO

Il ruolo del Dirigente Scolastico nel promuovere l'uso consentito delle tecnologie e di internet include i seguenti compiti :

- garantire la sicurezza on line dei membri della comunità scolastica;
- garantire che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione , del rispetto dell'altro e delle differenze , un utilizzo positivo e responsabile delle TIC;
- garantire l'esistenza di un sistema in grado di consentire il monitoraggio ed il controllo interno della sicurezza on line;
- seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.

ANIMATORE DIGITALE , COLLABORATORE DEL DS , RESPONSABILE DEL LABORATORIO DI INFORMATICA, IL TEAM DIGITALE

Il ruolo dei suddetti soggetti consiste in :

- stimolare la formazione interna negli ambiti di sviluppo della scuola digitale e fornire consulenza e informazioni al personale in relazione ai rischi on line ed alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti;
- coinvolgere la comunità scolastica nella partecipazione ad attività e progetti attinenti la

scuola digitale.

REFERENTE BULLISMO E CYBERBULLISMO

Per l'attuazione delle finalità di cui all'articolo 1, comma 1, del disegno di legge del Senato n. 1261 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo" la scuola nomina un docente Referente in merito alle problematiche del bullismo e cyberbullismo.
Il ruolo del referente prevede:

- prendere parte ai corsi di formazione previsti dalla suddetta legge ai fini di garantire l'acquisizione di idonee competenze teoriche e pratiche;
- organizzare attività formative per i docenti;
- promuovere la conoscenza del fenomeno e gli strumenti di prevenzione dello stesso affinché le famiglie possano riconoscerlo ed intervenire in modo corretto
- sostenere la famiglia e i minori vittime del cyberbullismo;
- promuovere, in collaborazione con tutti gli insegnanti, l'educazione all'uso consapevole della rete di bambini e ragazzi, favorendo specifici percorsi didattici finalizzati a responsabilizzare gli stessi minori e a promuoverne la consapevolezza in ordine ai rischi, oltre che alle opportunità;
- garantire, a questo riguardo, la continuità curricolare tra i diversi ordini di scuola e in modo particolare tra la secondaria di primo grado e la secondaria di secondo grado, secondo quanto previsto dal decreto.

PERSONALE ATA E DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI.

Il personale ATA ha il compito di:

- raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo e segnalarli.

Il ruolo del DSGA include i seguenti compiti :

- assicurare nei limiti delle risorse finanziarie disponibili , l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante , sicura e non aperta a uso improprio o a dannosi attacchi esterni;
- garantire il funzionamento dei diversi canali di comunicazione all'interno della scuola e fra la scuola e le famiglie.

DOCENTI

Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti:

- informarsi/ aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola , rispettandone il Regolamento;
- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculo di studio e nelle attività didattiche ed educative delle classi;
- garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo

scorretto e pericoloso delle TIC e di internet;

- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete , ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- controllare l'uso delle tecnologie digitali da parte degli alunni durante le lezioni e in ogni altra attività scolastica;
- nelle lezioni in cui è programmato l'utilizzo di internet , guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su internet siano trovati e trattati solo materiali idonei;
- comunicare ai genitori bisogni , difficoltà o disagi espressi dagli alunni rilevati a scuola e connessi con l'utilizzo delle TIC al fine di approfondire e concordare coerenti linee di interventi educativi;
- segnalare qualsiasi problema o proposta di carattere tecnico organizzativo ovvero esigenza di carattere informativo all'AD ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione di rischi nell'uso delle TIC;
- segnalare al DS e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tic o di internet per l'adozione delle procedure previste nelle norme.

ALLIEVI

Il ruolo degli allievi include i seguenti compiti :

- essere responsabili in relazione al proprio grado di maturità e di apprendimento , nell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
- comprendere l'importanza di adottare buone pratiche di sicurezza on line quando si utilizzano le tecnologie digitali per non correre rischi;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- esprimere domande, difficoltà o richieste di aiuto nell'utilizzo delle tecnologie didattiche o di Internet ai docenti e ai genitori.

GENITORI

Il ruolo dei genitori degli alunni include i seguenti compiti :

- sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle TIC e delle Comunicazioni nella didattica;
- seguire gli alunni nello studio a casa e nelle eventuali attività in Dad, adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare

l'utilizzo del pc e di internet;
- concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet.

GLI ENTI EDUCATIVI ESTERNI E LE ASSOCIAZIONI

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola hanno il compito di:

- conformarsi all'e-policy dell'Istituto riguardo all'uso consapevole della Rete e delle TIC;
- promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

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

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

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

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

Le figure professionali e le organizzazioni coinvolte in progetti, laboratori e attività che entrano in relazione con la scuola devono:

- prendere visione dell'e-policy e sottoscriverla preliminarmente all'avvio dei programmi con gli studenti;
- conformarsi alla politica dell'e-policy riguardo all'uso consapevole della Rete e delle TIC;
- promuovere comportamenti sicuri e assicurare la protezione degli studenti durante le attività

che si svolgono insieme;
- autocertificare l'assenza di condanne penali;
- evitare un uso improprio o comunque deontologicamente scorretto dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, durante le attività con gli studenti;
- rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali.

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.

Condivisione e comunicazione della politica e-safety agli alunni

- Tutti gli alunni saranno informati che la rete , l'uso di internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione.
- Nel Piano triennale dell'Offerta Formativa, in coerenza con il quadro di riferimento europeo DigComp 2.1 e nel curricolo dell'educazione civica verranno inseriti moduli didattici al fine di aumentare la consapevolezza e l'importanza di un uso sicuro e responsabile di Internet tra gli alunni.
- L'istruzione degli alunni riguardo l'uso responsabile e sicuro di internet precederà l'accesso alla rete.
- L'elenco delle regole per la sicurezza on line sarà pubblicato in tutte le aule o laboratori con accesso a Internet.

- Sarà data particolare attenzione nell'educazione alla sicurezza, agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili.
- Sarà consegnata agli alunni una brouchure contenente le linee guida per la sicurezza in rete, scritta dai ragazzi della quinta primaria e quindi con un linguaggio più adatto alla loro comprensione.

Condivisione e comunicazione della politica di e-safety al personale

- La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà discussa negli organi collegiali e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web.
- Per proteggere tutto il personale e gli alunni , la scuola metterà in atto una linea di condotta di utilizzo accettabile , controllato e limitato alle esigenze didattiche .
- Il personale docente sarà reso consapevole del fatto che il traffico internet può essere monitorato e si potrà risalire al singolo utente registrato.
- Un'adeguata informazione/formazione on line del personale docente nell'uso sicuro e responsabile di internet , sia professionalmente che personalmente sarà fornita a tutto il personale , anche attraverso il sito web della scuola.
- Il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC sarà supervisionato dall'AD che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici.
- L'AD metterà in evidenza on line strumenti che il personale potrà usare con i bambini in classe.
- Tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

Condivisione e comunicazione della politica di e-safety ai genitori

- Sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione degli incontri scuola famiglia , assembleari , collegiali e individuali .
- L'Ad e i docenti della classe forniranno ai genitori indirizzi sul web relativi a risorse per lo studio e a siti idonei ed educativi per gli alunni , sistemi di filtraggio gratuiti e attività educative per il tempo libero .
- I genitori esperti potranno collaborare nelle attività di informazione / formazione

---

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.

Disciplina degli alunni

Le infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali , in relazione alla fascia di età considerate, sono prevedibilmente le seguenti :

- uso inappropriato della Rete;
- un uso della rete per giudicare , infastidire o impedire a qualcuno di esprimersi o partecipare;
- l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;
- la condivisione di immagini intime o inadeguate;
- la comunicazione incauta e senza permesso con sconosciuti

Gli interventi correttivi sono rapportati all'età e al livello di sviluppo del bambino.
Sono previsti pertanto, da parte dei docenti, provvedimenti disciplinari proporzionati all'età e alla gravità del comportamento , quali:

- il richiamo verbale;
- il richiamo scritto con annotazione sul diario e sul Registro elettronico;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Ds;
- l'eventuale provvedimento disciplinare deciso dal consiglio di classe o interclasse

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni.

Disciplina del personale scolastico

Le potenziali infrazioni, in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet, sono diverse e alcune possono determinare , favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli alunni :

- un utilizzo delle tecnologie e dei servizi della scuola , d'uso comune con gli alunni , non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei ;
- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi ;
- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile delle tecnologie digitali e di internet;
- una vigilanza elusa degli alunni che può favorire un utilizzo non autorizzato delle TIC e

possibili incidenti;
- insufficienti interventi nelle situazioni critiche di contrasto a terzi , correttivi o di sostegno agli alunni, di segnalazioni ai genitori , al Dirigente scolastico o all'Animatore digitale .

Il Dirigente Scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone copia per eventuali successive investigazioni.
Tutto il personale è tenuto a collaborare con il Ds e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo, gestionale , disciplinare , amministrativo, penale a seconda del tipo o della gravità delle infrazioni commesse . Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

Disciplina dei genitori
In considerazione dell'età dei bambini (fino a 14 anni) e della loro dipendenza dagli adulti , alcune considerazioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola , luogo in cui possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico .
Le situazioni familiari meno favorevoli sono :

- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone;
- un utilizzo del pc, del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria materiali non idonei

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli , se dovessero risultare pericolosi per sé e/o dannosi per altri ,in relazione soprattutto a materiale o situazioni che abbiano ripercussione in ambito scolastico.

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.

Verranno inserite le seguenti norme:

1.DIVIETI

E' vietato installare materiale protetto da copyright. E' vietato l'uso della postazione di lavoro per i collegamenti a Internet a scopi commerciali o di profitto personale o di attività illegali. Ricordando che la responsabilità delle azioni compiute tramite una utenza è sempre del legittimo titolare , anche se compiute in sua assenza , la password ricevuta non deve essere comunicata a nessuno e non deve essere salvata su dispositivi di uso comune . Essa deve essere memorizzata dall'utente che non deve trascriverla in nessun luogo . Ogni contatto ed operazione on line che implica assunzione di impegni o responsabilità per conto della scuola deve essere autorizzata dal legale rappresentante dell'istituzione.

2.USO PERSONALE

E' consentito l'utilizzo della postazione di lavoro , in modo saltuario , a fini personali , solo se compatibile o funzionale al ruolo professionale svolto purchè non sia causa diretta o indiretta, di disservizi dei sistemi elaborativi e dei servizi di collegamento dell'Amministrazione ; non sia causa di oneri aggiuntivi per l'Amministrazione , non interferisca con le attività lavorative dell'utente , delle attività scolastiche o con altri obblighi dello stesso verso l'Amministrazione .

3.USO DIDATTICO

- Ogni allievo è direttamente responsabile della postazione assegnatagli per le ore in cui vi svolge lezione . Agli utenti è fatto assoluto divieto di cancellare ,modificare in qualsiasi modo i files presenti sulla macchina o alterare il sistema operativo o la configurazione dei programmi e dell'hardware della macchina .
- E' fatto obbligo di adottare comportamenti idonei a non provocare danni o pericoli agli strumenti ed alle attrezzature messi a disposizione . In caso di comodato d'uso dei device di proprietà o in concessione all'Istituto si fa riferimento al contratto.
- Gli utenti sono tenuti a non prelevare o depositare informazioni, applicazioni o documenti che possano in qualsiasi modo arrecare danno a persone , cose o istituzioni
- E' vietato inserire file sul server o scaricare da internet software non autorizzati o materiale soggetto a copyright o a diritti di proprietà intellettuale.
- Il riscontro di qualsiasi anomalia deve essere tempestivamente segnalato dagli alunni al docente e dal docente al responsabile del laboratorio.
- Per utilizzare CD-ROM , DVD , penne USB o altri supporti di memorizzazione personali è necessario sottoporli al controllo anti virus.
- Si devono rispettare le regole di decenza e morali, evitare atti e comportamenti che possano recare offesa a cose , persone o istituzioni presenti o meno sulla rete.
- E' fatto assoluto divieto di navigare in siti dai contenuti pornografici o contenenti scene di violenza , razzismo o sfruttamento dei minori.
- Si deve mantenere segreto il nome, l'indirizzo, il telefono di casa, il telefono cellulare , il nome e l'indirizzo della scuola frequentata.
- Non si devono inviare a nessuno fotografie proprie o di amici

I docenti che accompagnano gli allievi in laboratorio o fanno usare i dispositivi di classe o i loro dispositivi (vedasi BYOD) sono tenuti a controllare che vengano rispettati i divieti sopraelencati e

che l'utilizzo delle risorse tecnologiche sia finalizzato agli intenti didattici previsti .

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il monitoraggio sarà curato dal Ds con la collaborazione dell'AD ed ai docenti delle classi , tramite questionari e conversazione. Sarà finalizzato a rilevare l'uso sicuro e responsabile delle TIC e di internet in classi campione. Il monitoraggio sarà rivolto anche agli insegnanti , al fine di valutare l'impatto della policy e le necessità di eventuali miglioramenti . L'aggiornamento della policy sarà curato dal DS , dall'AD , dal Team Digitale , a seconda degli aspetti considerati.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare, in occasione dell' Internet Safer Day, un approfondimento sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- 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 e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti

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 l'aggiornamento dell'ePolicy.

- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- 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.

Traguardi per lo sviluppo delle competenze digitali al termine della SCUOLA DELL'INFANZIA

L'alunno:

- sperimenta situazioni problematiche sviluppando le basi del pensiero computazionale;
- esperisce attività di coding unplugged collegando trasversalmente i vari campi d'esperienza;

Traguardi per lo sviluppo delle competenze digitali al termine della SCUOLA PRIMARIA

L'alunno:

- utilizza le più comuni tecnologie in particolare quelle dell'informazione e della comunicazione individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall' attività di studi fino alla risoluzione di problemi della vita quotidiana;
- è consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie, con particolare riferimento al contesto produttivo, culturale e sociale in cui vengono applicate;

- cerca, utilizza e crea in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità;
- gestisce in modo sicuro i propri dati personali e quelli altrui e utilizza le tecnologie digitali per scopi eticamente accettabili, nel rispetto degli altri.

Traguardi per lo sviluppo delle competenze digitali al termine della SCUOLA SECONDARIA I GRADO

L'alunno:

- reperisce, seleziona e valuta informazioni in internet da fonti e con strumenti diversi;
- utilizza in modo etico gli strumenti per comunicare ed evitare le possibili minacce alla privacy e altri reati in rete;
- ha buone competenze digitali, usa con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati e saper distinguere informazioni attendibili da quelle che necessitano approfondimento;
- è in grado di usare, in modo efficace e responsabile, le nuove tecnologie e i linguaggi multimediali per supportare lo studio e il lavoro progettuale, sia a livello individuale che collaborando e cooperando con i compagni;
- sviluppa particolari abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui doveri nei riguardi di coloro con cui si comunica online.

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

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

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

Il corpo docente ha partecipato a molti corsi di formazione sia nell'ambito di piani nazionali che su iniziative organizzate dall'istituzione o dalle scuola associate in Rete e possiede generalmente una buona base di competenze e nel caso delle figure di sistema , anche di carattere specialistico . E' inoltre disponibile ad aggiornarsi per mantenere al passo la propria formazione . Il percorso complesso della formazione specifica dei docenti per l'utilizzo delle TIC nella didattica prosegue grazie a momenti di aggiornamento (corsi PON e Rete) e autoaggiornamento personale o all'interno dell'Istituto e on line .

Sono disponibili per i docenti varie risorse :

- Programma il futuro;
- CATALOGO FORMATIVO DEL PNFD.

2.3 - Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

Il 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 e a cui accedono sempre di più ed autonomamente anche i ragazzi.
Tramite il sito è possibile l'accesso diretto al progetto GENERAZIONI CONNESSE: MATERIALI informativi sulla sicurezza in Internet per l'approfondimento personale , per le attività con gli studenti e gli incontri con i genitori costituiti da video , guide , manuali , link e contributi della Polizia di Stato, dell'Arma dei carabinieri e di Telefono Azzurro.

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.

L'Istituto ha attivato iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete , promuovendo la conoscenza delle numerose situazioni di rischi on line. A tal fine sono previsti incontri fra docenti e genitori per la diffusione del materiale informativo sulle tematiche trattate , messo a disposizione dei siti specializzati e dalle forze dell'ordine .
Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari o smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo .
Sul sito scolastico sulla bacheca relativa a GENERAZIONI CONNESSE sono già stati messi in condivisione materiali dedicati ad alunni e famiglie che possono servire come spunti di approfondimento e confronto .
La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nell' E-policy per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle tecnologie all'interno dell'Istituto e prevenire i rischi legati a un utilizzo non corretto di internet. Nel Patto di corresponsabilità sottoscritto coi genitori , viene fatto specifico riferimento al Regolamento epolicy.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021)

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo 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.

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

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e

l'integrazione delle TIC nella didattica.

- 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 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.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

personali.

Il personale scolastico è " incaricato del trattamento" dei dati personali nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza. Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali AL MOMENTO DELLA STIPULA DEL CONTRATTO DI LAVORO ai fini della protezione e sicurezza degli stessi. I dati personali sono protetti secondo la normativa vigente, viene richiesta specifica autorizzazione per l'utilizzo di foto, video, testi per la documentazione di attività didattiche, anche in occasione di eventi o manifestazioni, e per la pubblicazione sul sito della scuola, Facebook e Canale YouTube. Specifica informativa viene inviata ai genitori in merito agli strumenti in uso per la realizzazione della Didattica digitale integrata .

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 nel laboratorio multimediale e in classe nel caso di utilizzo delle LIM , dei pc di classe e dei dispositivi personali da parte dei docenti e degli alunni secondo quanto indicato nel regolamento BYOD in vigore nel nostro Istituto .
L'accesso dai pc dell'istituto (laboratorio e pc classi) è schermato da filtri che dal server impediscono il collegamento a siti appartenenti a black list , secondo le impostazioni date dal team digitale che provvede periodicamente alla manutenzione e aggiornamento del sistema informatico del laboratorio, ove necessario richiedendo l'intervento di tecnici esterni .
Per quanto riguarda i dispositivi degli alunni, portati da casa , si rimanda al Regolamento BYOD; riguardo alla navigazione sicura con i dispositivi personali si specifica che i filtri dei dispositivi personali devono essere installati a cura dei genitori tutori dell'alunno su ciascun dispositivo.
L'accesso al sistema informatico per la didattica è consentito al personale attraverso l'assegnazione di una password . La password è comune e permette di accedere al server . Le postazioni del laboratorio e nelle classi funzionano come stazioni di lavoro e non come archivio.

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.

STRUMENTI DI COMUNICAZIONE ESTERNA

SITO DELLA SCUOLA
La scuola attualmente ha un sito web . Tutti i contenuti del settore didattico sono pubblicati sotto la supervisione del DS , che ne valuta la sicurezza e l'adeguatezza sotto il profilo dell'accessibilità , della pertinenza dei contenuti , del rispetto della privacy.

SOCIAL NETWORK
L'Istituzione scolastica ha creato, col profilo della posta istituzionale del primo collaboratore, una pagina youtube per la pubblicazione di video di attività didattiche particolarmente significative , anche per diffonderle attraverso questo canale , sul sito dell'Istituto .
Nel caso di video in cui siano ripresi gli alunni durante le attività didattiche , eventi o manifestazioni verrà acquisita specifica autorizzazione scritta dei genitori di ciascun alunno coinvolto . L'istituto è

presente su Facebook , con pagina gestita dal Dirigente scolastico, per comunicazione e divulgazione di eventi dell'Istituto.

STRUMENTI DI COMUNICAZIONE INTERNA

REGISTRO ELETTRONICO
Il nostro registro elettronico "Nuvola" adotta gli stessi criteri di sicurezza delle banche e degli istituti di credito: connessioni cifrate (HTTPS tramite certificato SSL) e rispetto della privacy sui dati. Consente di gestire a 360° tutto il lavoro del Docente: valutazioni, assenze, note didattiche, argomenti di lezione, compiti, modulistica, colloqui, comunicazioni per le famiglie.

E-MAIL
L'account di posta elettronica è solo quello istituzionale utilizzato dagli uffici amministrativi (toic865006@istruzione.it) , mentre per i docenti, per gli alunni delle classi quarte e quinte della scuola primaria e della scuola secondaria sono state create delle e-mail con il dominio edu.it

PIATTAFORMA “GOOGLE SUITE FOR EDUCATION”
I genitori degli alunni sottoscrivono l’informativa ex art. 13 del regolamento ue 2016/679, per il trattamento dei dati personali ai fini dell’iscrizione ed utilizzo della piattaforma “Google suite for education”.

WHATSAPP O TELEGRAM
Nella normativa vigente l’utilizzo di Whatsapp o Telegram per comunicazioni istituzionali non è contemplato perché non sussistono strumenti di protezione e protocolli tali che possono garantire la sicurezza e la privacy delle comunicazioni che si svolgono in loco. I numeri di telefono personali sono privati e comunicati alla scuola dal personale scolastico solo per fini istituzionali. Questi numeri non possono essere utilizzati senza il consenso preventivo degli interessati all’interno di qualsiasi applicazione, in mancanza di consenso preventivo si potrebbe registrare una violazione della normativa in materia di Privacy. È importante ricordare quello che si può definire “diritto alla disconnessione”. L’art. 22 (Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola) del CCNL 2016/2018, infatti, fa riferimento ai criteri generali per l’utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione fra vita lavorativa e vita familiare. È importante sottolineare però che per le chat informali fra colleghi, o fra docenti e genitori, non esiste una vera e propria regolamentazione, e per tale ragione è fondamentale, a partire dal buon senso e da una riflessione sulle peculiarità del mezzo, che si elaborino regole condivise sull’uso delle stesse. Fra queste, ad esempio, si dovrebbe:

- Evitare che gli insegnanti siano inseriti nei gruppi di classe dei genitori;
- Rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità;
- Usare sempre un linguaggio adeguato e il più possibile chiaro e preciso (come già sottolineato la comunicazione online si presta spesso a non pochi fraintendimenti);
- Evitare di affrontare in chat argomenti troppo complessi e controversi (la comunicazione online in una chat di gruppo non è adatta per la gestione di problematiche di questo tipo, che certamente è più opportuno affrontare in presenza o in un Consiglio di classe);
- Evitare discussioni di questioni che coinvolgono due o pochi interlocutori, onde evitare di

annoiare e disturbare gli altri componenti del gruppo;
- Evitare di condividere foto di studenti in chat;
- Indirizzare solo domande precise e chiare, a cui si possano dare risposte altrettanto brevi e precise;

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.

STRUMENTAZIONE PERSONALE DEGLI STUDENTI
Per la gestione degli strumenti personali –notebook, cellulari, tablet degli studenti si rimanda al regolamento BYOD.

STRUMENTAZIONE PERSONALE DEI DOCENTI
Durante le ore di lezione non è consentito l'utilizzo del cellulare , mentre è consentito l'uso di altri dispositivi elettronici personali a scopo didattico ed integrativo di quelli scolastici disponibili. Durante il restante orario è consentito l'utilizzo del cellulare per comunicazioni di carattere urgente mentre è permesso l'uso di altri dispositivi elettronici personali per attività funzionali all'insegnamento , ad integrazione di quelli scolastici disponibili.

STRUMENTAZIONE DEL RESTANTE PERSONALE DELLA SCUOLA
Durante l'orario di servizio al restante personale scolastico è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021).

Scegliere almeno 1 di queste azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione degli studenti/studentesse suindicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare una o più attività volte a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più 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)

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
- Organizzare attività per la consultazione degli studenti/studentesse suindicazioni/regolamenti sull'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 una o più attività volte 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 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.*

La sensibilizzazione costituisce il primo passo verso un cambiamento positivo, ma per far sì che l'intervento sia efficace, è importante che sia chiara l'azione verso cui i soggetti devono impegnarsi. Bisogna fornire tutte le informazioni necessarie sul contenuto che si sta trattando, le motivazioni per cui è necessario impegnarsi verso un cambiamento e illustrare le possibili soluzioni o comportamenti da adottare.
Per prevenzione si intende un insieme molto ampio di strategie che coinvolgono le famiglie e le forze sociali che operano sul territorio per l'educazione formativa dei ragazzi. Nello specifico l'IC FAVRIA integra nel curricolo temi legati al corretto utilizzo delle TIC e di Internet, per prevenire e contrastare bullismo e cyberbullismo, e attiva inoltre uno sportello di ascolto al quale la componente

studentesca si può rivolgere per avere consigli e sostegno psicologico.

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).

Le novità introdotte dalla recente legge e i compiti affidati dalla stessa alle scuole comportano delle modifiche al Regolamento di Istituto e al Patto di Educativo di Corresponsabilità. I regolamenti scolastici dovranno prevedere misure di prevenzione ed esplicite sanzioni disciplinari, commisurate alla gravità degli atti compiuti. Il Dirigente attiva, nei confronti dello/gli studente/i che ha/hanno

commesso atti di cyberbullismo, azioni non di carattere punitivo ma educativo. Il Dirigente Scolastico che venga a conoscenza di atti di cyberbullismo informa tempestivamente i genitori e possono essere segnalati al servizio Helpline di Telefono Azzurro 1.96.96, una piattaforma integrata finalizzata ad aiutare i ragazzi e le ragazze a comunicare il proprio disagio e alla Hotline “Stop-It" di Save the Children, all’indirizzo www.stop-it.it. Le segnalazioni vengono successivamente trasmesse al Centro Nazionale per il Contrasto alla Pedopornografia su Internet, istituito presso la Polizia Postale e delle Comunicazioni, per consentire le attività di investigazione necessarie.
Chi compie atti di bullismo e cyberbullismo può anche essere responsabile di reati penali e danni civili. I ragazzi e le ragazze che fanno azioni di bullismo possono commettere reati. Secondo il codice penale italiano i comportamenti penalmente rilevanti in questi casi sono:

- percosse (art. 581),
- lesione personale (art. 582),
- ingiuria (art. 594),
- diffamazione (art. 595),
- violenza privata (art. 610),
- minaccia (art. 612),
- danneggiamento (art. 635).

Nei casi più gravi, basta la denuncia ad un organo di polizia o all’autorità giudiziaria per attivare un procedimento penale (per es. lesioni gravi, minaccia grave, molestie); negli altri casi, la denuncia deve contenere la richiesta che si proceda penalmente contro l’autore di reato (querela).

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.

SEGNALAZIONE

Per il telefono cellulare ci si può assicurare che l'alunno vittima salvi sul suo telefono ogni messaggio/voce/testo/immagine , conservando così il numero del mittente. Gli insegnanti anche con l'ausilio tecnico dell'AD provvedono a conservare le prove della condotta scorretta o dell'abuso rilevate sui pc della scuola: la data e l'ora , il contenuto dei messaggi , e , se possibile , l'ID del mittente o l'indirizzo web del profilo e il suo contenuto. Qualora ci si dovesse accorgere che l'alunno , usando il computer , si sta servendo di un servizio di messaggeria istantanea , l'insegnante può copiare e incollare e stampare la conversazione . Per gli eventuali collegamenti non autorizzati a siti social network, video-hosting site e altri website, l'insegnante può conservare il link, stampare la pagina o salvare la schermata su documento word. Per le mail si può stampare la mail o conservare l'intero messaggio , compresa l'intestazione del mittente. Conservare la prova è utile per far conoscere l'accaduto in base alla gravità ai genitori degli alunni, al DS e per le condotte criminose alla Polizia . Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno , le notizie raccolte sono comunque comunicate ai genitori e al DS ; per quelle criminose anche alla Polizia. In particolare la segnalazione viene fatta a entrambe le famiglie, se oltre alla vittima anche l'autore della condotta negativa è un altro alunno.

GESTIONE DEI CASI

Per prevenire L'HATE SPEECH si programmeranno attività di analisi e produzione mediale, finalizzate soprattutto a:

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

Per affrontare il cyberbullismo i docenti non solo identificano vittime e prepotenti in divenire , ma affrontano e intervengono sul gruppo classe coinvolgendo anche i genitori .
Vengono intrapresi anche percorsi di sostegno alle vittime volti a incrementarne l'autostima , mentre i prevaricatori sono destinatari di interventi mirati a smuoverne le competenze empatiche e a favorire una loro condivisione delle norme morali . In relazione alle manifestazioni socio affettive fra pari i docenti intervengono per favorire nei ragazzi un buon rapporto con il proprio corpo e per far percepire meglio eventuali violazioni dei limiti di prossimità o di confidenza ed imparare ad apporvisi , per far acquisire fiducia nelle proprie sensazioni e nel proprio intuito e determinazione nel rifiutare i contatti anche " a distanza" sgradevoli e strani , per rendere consapevoli gli alunni del diritto al rispetto dei propri limiti e di quelli altrui, per far capire che l'interazione on line deve sottostare a delle regole di buon comportamento, né più né meno di quelle della vita reale. Qualora la scuola rilevi una situazione psico-socio-educativa particolarmente problematica , convoca i genitori per valutare con loro a quali risorse territoriali possono rivolgersi.

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?

Secondo uno studio del King's College di Londra più del 23% dei giovani intervistati ha una relazione disfunzionale con il proprio smartphone. Stati d'ansia provocati dalla ricerca e dall'uso compulsivo del cellulare che, nei casi più gravi, si associano a veri e propri stati depressivi. In Italia, secondo una ricerca, ben il 45% degli studenti (6.671 giovani tra gli 11 e i 25 anni) dichiara di passare sul web almeno 5-6 ore ogni giorno e il tempo trascorso online raggiunge picchi più alti nel fine settimana: 1 intervistato su 5 dice di sentirsi a disagio o comunque va in ansia quando manca la connessione alla Rete e cresce in contemporanea la percentuale di coloro che manifestano attacchi di panico quando finiscono i giga e le promozioni tariffarie a cui sono abbonati (circa 1 su 3). Ancora, secondo l'Istat, "nel 2018, l'85,8% dei ragazzi tra 11 e 17 anni di età utilizza quotidianamente il telefono cellulare. Il 72% dei ragazzi in quella stessa fascia di età naviga in Internet tutti i giorni. Questa quota è cresciuta molto rapidamente passando dal 56,2 al 72,0% nell'arco di un quadriennio. Le più frequenti utilizzatrici del cellulare e della rete sono le ragazze, l'87,5% delle quali usa il cellulare quotidianamente e il 73,2% accede a Internet tutti i giorni (quota che sale all'84,9% se ci si concentra sulle adolescenti tra i 14 e i 17 anni). L'accesso ad Internet è fortemente trainato dalla diffusione degli smartphone. Soltanto il 27,7% dei ragazzi, infatti, usa il pc tutti i giorni e questa quota è in forte calo rispetto al 40,5 del 2014".
La dipendenza da Internet, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica che deve attenzionare il fenomeno e fornire gli strumenti agli studenti e alle studentesse affinché questi siano consapevoli dei rischi che comporta l'iperconnessione. La S.I.I.Pa.C., la Società Italiana Intervento Patologie Compulsive, definisce la dipendenza da Internet come progressivo e totale assorbimento del soggetto alla Rete e i segnali patologici di questo comportano un "un vero e proprio abuso della tecnologia", anche denominato "Internet Addiction Disorder" (I.A.D. coniato dallo psichiatra Ivan Goldberg 1996).
Il nostro Istituto si impegna quindi a fornire al personale della scuola, agli studenti e alle loro famiglie strumenti finalizzati al riconoscimento e alla prevenzione del fenomeno con percorsi sul benessere digitale.

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.

I contenuti sessualmente espliciti, possono diventare materiale di ricatto assumendo la forma di “revenge porn” letteralmente “vendetta porno” fenomeno quest’ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l’altra parte (la Legge 19 luglio 2019 n. 69, all’articolo 10 ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti. Si rimanda all’articolo 612 ter del codice penale rubricato “Diffusione illecita di immagini o video sessualmente espliciti”.

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.

PREVENZIONE
Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all’affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di

aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e perché no, della sessualità. L'IC FAVRIA dispone poi di uno sportello di ascolto e della figura del referente problematiche bullismo al quale la componente studentesca si può rivolgere.
La problematica dell'adescamento online (come quella del sexting), si inquadra in uno scenario più ampio di scarsa educazione emotiva, sessuale e di assenza di competenza digitale, in riferimento al modo in cui i/le ragazzi/e vivono la propria sessualità e la propria immagine online, al loro desiderio di esprimersi e affermare se stessi.
Fondamentale quindi, è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è).

GESTIONE DEI CASI
Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad esempio, all'adescatore. È importante che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove.
Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video…).
L'adescamento, inoltre, può essere una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.
I minori vittime di adescamento riferiscono, generalmente, di sentirsi traditi, ma anche di provare un senso di colpa per essere caduti in trappola ed essersi fidati di uno sconosciuto.
Inutile sottolineare che nei casi più estremi in cui l'adescamento porta ad un incontro fisico e ad un abuso sessuale un sostegno psicologico esperto per il minore è da considerarsi prioritario e urgente.
Per consigli e per un supporto è possibile rivolgersi alla Helpline di Generazioni Connesse (19696): operatori esperti e preparati sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che dei bambini, degli adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti l'utilizzo dei nuovi media.

4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, **concrete o simulate** o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

La legge n. 269 del 3 agosto 1998 *"Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella* ***legge n. 38 del 6 febbraio 2006*** *"Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"*, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 - *Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.*

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione **"Segnala contenuti illegali"** (Hotline).

Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children.

Per le segnalazioni di fatti rilevanti si applica il Regolamento di istituto per INFRAZIONI GRAVI. Gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria o più semplicemente agli organi di polizia competenti. Ai fini della denuncia , la relazione deve essere fatta nel modo più dettagliato possibile indicando : il fatto , il giorno dell'acquisizione del fatto , nonché le fonti di prova , e , per quanto possibile , le generalità , il domicilio e quant'altro di utile a identificare la persona alla quale il reato è attribuito, la persona offesa e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021).

Scegliere almeno 1 di queste azioni:

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

☐ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

☐ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

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

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.

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

☐ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.

☐ 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/studentesse.

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

☐ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

☐ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle

studenti/studentesse.

☐ Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

☐ 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.

I docenti sono chiamati a predisporre delle rilevazioni e qualora si rendano conto che si trovano di fronte a situazioni di criticità dovranno rivolgersi ai Referenti che avvieranno le procedure con le istituzioni preposte nonché la segnalazione alla Dirigenza Scolastica. Tali rilevazioni avvengono secondo i protocolli suggeriti dalla piattaforma messa a disposizione da "Generazioni Connesse",

come da schemi allegati.

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.

Per il telefono cellulare ci si può assicurare che l'alunno vittima salvi sul suo telefono ogni messaggio/voce/testo/immagine , conservando così il numero del mittente. Gli insegnanti anche con l'ausilio tecnico dell'AD provvedono a conservare le prove della condotta scorretta o dell'abuso rilevate sui pc della scuola : la data e l'ora , il contenuto dei messaggi , e , se possibile , l'ID del mittente o l'indirizzo web del profilo e il suo contenuto. Qualora ci si dovesse accorgere che l'alunno , usando il computer, si sta servendo di un servizio di messaggistica istantanea , l'insegnante può copiare e incollare e stampare la conversazione . Per gli eventuali collegamenti non autorizzati a siti social network, video-hosting site e altri website, l'insegnante può conservare il link, stampare la pagina o salvare la schermata su documento word. Per le mail si può stampare la mail o conservare l'intero messaggio , compresa l'intestazione del mittente.
Conservare la prova è utile per far conoscere l'accaduto in base alla gravità ai genitori degli alunni, al DS e per le condotte criminose alla Polizia .
Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno , le notizie raccolte sono comunque comunicate ai genitori e al ds ; per quelle criminose anche alla Polizia.
In particolare la segnalazione viene fatta a entrambe le famiglie, se oltre alla vittima anche l'autore della condotta negativa è un altro alunno. Per le segnalazioni di fatti rilevanti si applica il Regolamento di istituto per INFRAZIONI GRAVI. Per questi (es pedopornografia) gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria o più semplicemente agli organi di polizia competenti. Ai fini della denuncia , la relazione deve essere fatta nel modo più dettagliato possibile indicando :
il fatto , il giorno dell'acquisizione del fatto , nonché le fonti di prova , e , per quanto possibile , le generalità , il domicilio e quant'altro di utile a identificare la persona alla quale il reato è
attribuito, la persona offesa e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto. Nell' l'IC FAVRIA è attivo inoltre uno sportello di ascolto al quale la componente studentesca si può rivolgere per avere consigli e sostegno psicologico e il gruppo NOI.

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.

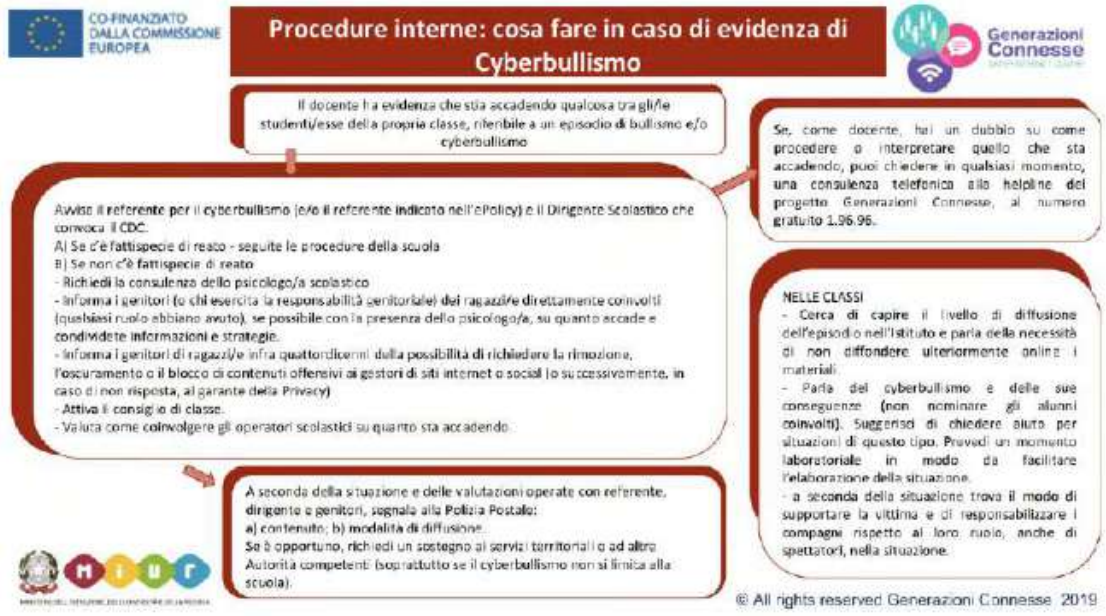
Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse “Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all’utilizzo delle tecnologie digitali da parte dei più giovani” (seconda parte, pag. 31), senza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

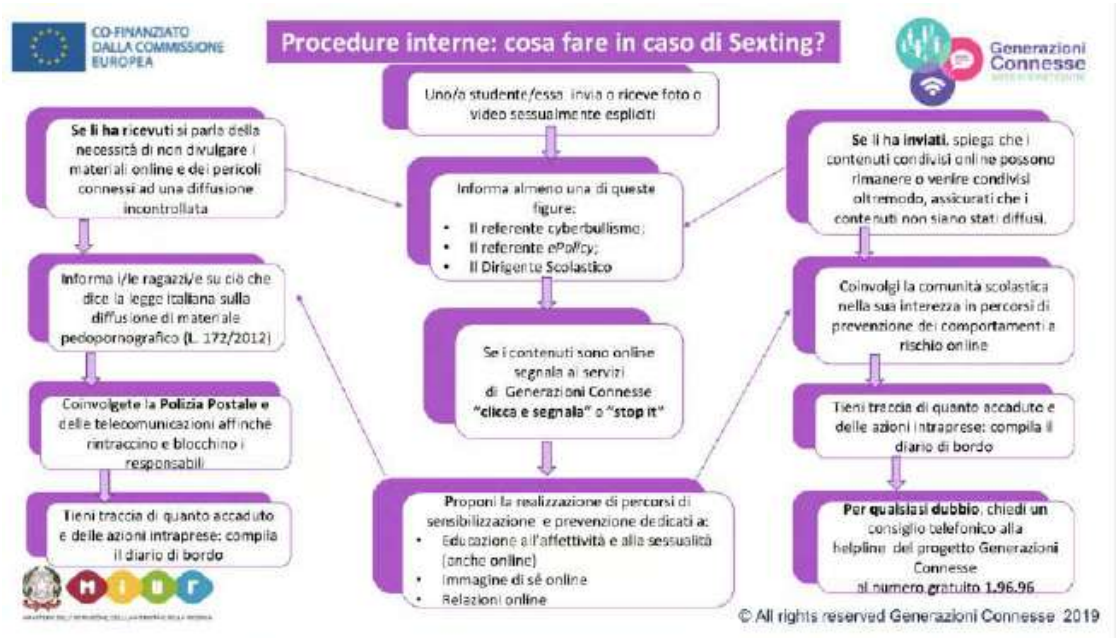
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

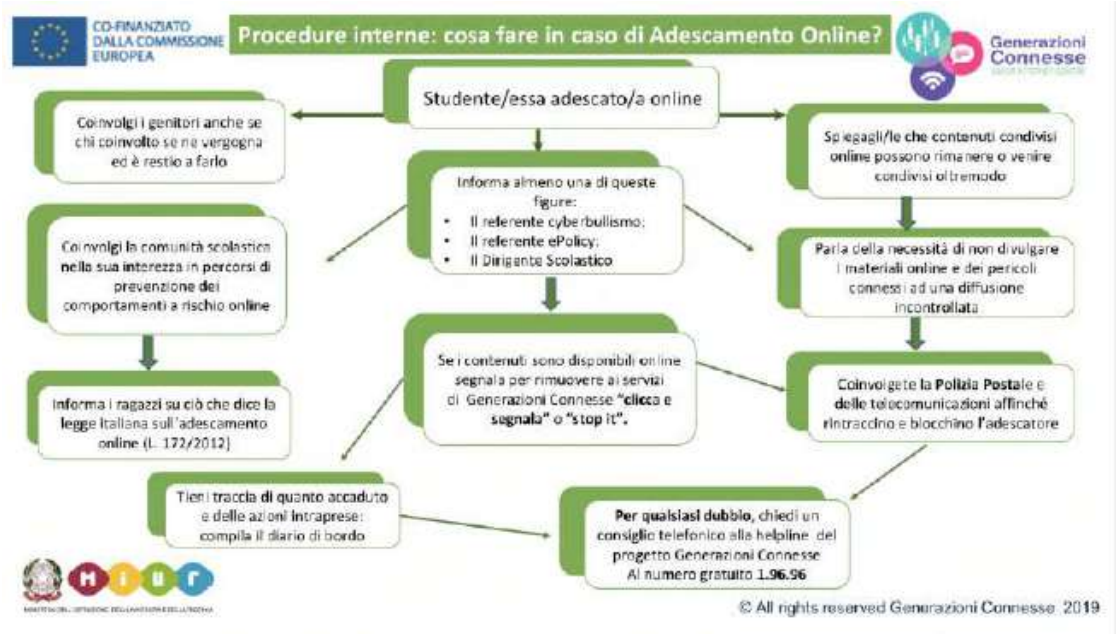
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



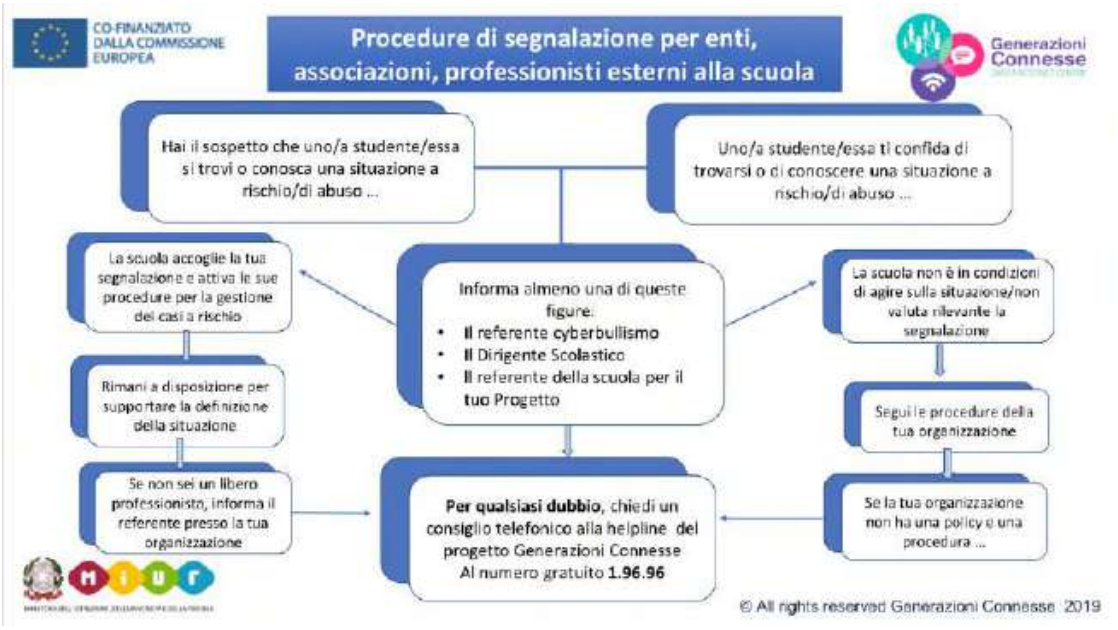
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il nostro piano d'azioni

La Scuola si impegna ad organizzare le seguenti attività di prevenzione al fenomeno: organizzazione di Corsi di formazione per docenti, genitori, operatori del settore socioeducativo; partecipazione da parte di docenti, studenti e genitori a convegni e seminari sul tema del bullismo e del cyberbullismo; interventi di consulenza e supporto - su richiesta da parte della scuola - relativamente a casi di cyberbullismo. Sulla base delle Linee guida per l'uso positivo delle tecnologie digitali e della prevenzione dei rischi nelle scuole, vengono assunti i seguenti punti quali indicatori di co-costruzione tra scuola-famiglia-servizi territoriali, al fine di creare un modello composito e 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 ed ASP per servizi specialistici; - promozione dell'educazione al rispetto; - sviluppo del pensiero critico; - promozione dell'Educazione Civica Digitale.