Documento di ePolicy

AVIS023003

ISTITUTO SUPERIORE "RUGGERO II"

VIA COVOTTI - 83031 - ARIANO IRPINO - AVELLINO (AV)

Massimiliano Bosco

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.

La vita quotidiana di ciascuno è pervasa in modo sempre più capillare dalle nuove tecnologie. L'ingresso delle TIC nel tessuto sociale ed economico delle comunità umane ha rappresentato senz'altro un'importante opportunità di crescita e di sviluppo; il mondo virtuale del web informa la nostra vita quotidiana al pari del mondo reale, ma proprio come quest'ultimo nasconde pericoli ed insidie.

Il mondo digitale rappresenta sempre più la realtà in cui sono immersi i ragazzi, fin dalla più tenera età, influenzandone le modalità di relazione con gli altri e il processo di apprendimento, con crescenti rischi di dipendenza.

L'accesso a Internet, soprattutto per i bambini e adolescenti, rappresenta da una parte un'opportunità di accrescimento del sapere, di incremento delle capacità comunicative, di sviluppo delle competenze e di miglioramento delle prospettive di lavoro, ma dall'altra può esporre a situazioni di vulnerabilità che richiedono interventi specifici. In questi ultimi anni, è diventato sempre più forte il bisogno di adottare una strategia che si faccia carico di fornire risposte adeguate a "nuovi" bisogni.

Le TIC hanno modificato il modo di vivere e di pensare delle persone, ma spesso questa libertà di accesso alla conoscenza non è proporzionale alla padronanza e la governance degli strumenti digitali.

Da anni il nostro Istituto attua una seria riflessione sul proprio approccio alle tematiche legate alla sicurezza online e all'integrazione delle tecnologie digitali nella didattica. Per tutti gli studenti e le studentesse dell'Istituto Ruggero II, e per i docenti, le tecnologie digitali e Internet fanno parte della vita scolastica. Tutti i nostri studenti hanno accesso alle reti informatiche e possono avvalersi della tecnologia in qualsiasi momento della giornata scolastica e sempre con la guida del personale docente. La lunga quarantena dovuta all'emergenza sanitaria causata dal Covid-19 ha segnato un momento storico per la scuola e le famiglie, sconvolgendo la quotidianità didattica, familiare e personale. In questo scenario Internet, i social network, le app di messaggistica ed in generale le tecnologie digitali hanno assunto una valenza senza precedenti. Per gli studenti e le studentesse sono aumentati i rischi legati all'iperconnessione e quelli all'esposizione in rete.

Questi motivi hanno reso necessario l'elaborazione di un efficace strumento di e Policy. Gli obiettivi che ci proponiamo con questo documento sono, prima di tutto, di regolamentare l'utilizzo delle tecnologie digitali affinché gli studenti e le studentesse ne dispongano in maniera positiva, critica e consapevole; e, in secondo luogo, di formare i docenti, i discenti e la comunità educanda tutta, per accrescere e

consolidare le competenze di cittadinanza digitale e favorire un uso sicuro e creativo della rete e delle sue risorse.

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.

Nella scuola le varie figure si interfacciano in una molteplicità di compiti per il miglioramento delle condizioni e del clima scolastico.

Nel farsi carico della formazione globale dell'individuo nella fase evolutiva, l'Istituto individua in maniera chiara e inequivocabile ruoli e responsabilità di ciascuno degli attori del percorso formativo.

Il Dirigente Scolastico

Egli, in quanto garante del diritto all'apprendimento degli studenti e delle studentesse, ha la responsabilità di promuovere e sostenere l'innovazione nella didattica, garantendo la sicurezza, anche online, di tutti i membri della comunità scolastica, pertanto:

- è adeguatamente formato sulla sicurezza e sulla prevenzione di problematiche offline e online (secondo il Quadro normativo di riferimento e le indicazioni del MI), predisponendo un sistema per monitorare e controllare la sicurezza online; segue le procedure previste dalle norme in caso di reclami, attribuzione di responsabilità al personale scolastico in relazione a incidenti, gestisce ed interviene nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali;
- promuove l'uso delle Tecnologie Digitali e la cultura della sicurezza online, garantendo, insieme all'Animatore Digitale e al docente referente, sulle tematiche del Bullismo/Cyberbullismo, corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo responsabile e consapevole delle TIC.

L' Animatore Digitale

supporta il personale scolastico da un punto di vista non solo tecnico-

informatico, ma anche in riferimento ai rischi online e alla protezione e gestione dei dati personali;

è uno dei promotori dei percorsi di formazione interni all'Istituto negli ambiti dello sviluppo della "Scuola Digitale", fornisce consulenza e informazioni al personale in relazione ai rischi online alle misure di prevenzione e gestione degli stessi;

si occupa di monitorare e rilevare le problematiche relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché di proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;

si assicura che gli utenti possano accedere alla rete della scuola solo tramite password personali applicate e regolarmente cambiate, cura la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (Istruzione e formazione);

pubblica il presente documento E-Safety Policy sul sito della scuola.

Il Referente prevenzione bullismo e cyberbullismo

"Ogni Istituto scolastico, nell'ambito della propria autonomia, individua tra i docenti un referente con il compito di coordinare iniziative di prevenzione e di contrasto del cyberbullismo" (Art. 4 Legge n.71/2017, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo). Egli, sicché:

coordina e promuove iniziative per la prevenzione e il contrasto del bullismo e del cyberbullismo. Raccoglie, diffonde le buone pratiche educative, organizzative e le azioni di monitoraggio. Facilita la formazione e la consulenza di tutto il personale;

può avvalersi della collaborazione delle Forze di Polizia, delle associazioni e dei centri di aggregazione giovanile del territorio (L.71/2017, art. 4, c 3); può coinvolgere, con progetti e percorsi formativi specifici, gli studenti, le studentesse, i colleghi e i genitori;

supporta il DS per la revisione/stesura del documento di valutazione dei rischi di bullismo e cyberbullismo, delle linee guida e del piano di prevenzione di tali fenomeni, nonché della definizione di un sistema sanzionatorio.

cura i rapporti di rete fra scuole per confronti su iniziative, seminari, corsi riguardanti il fenomeno del bullismo e del cyberbullismo.

Il Gruppo di lavoro "E- Safety Policy"

Nel nostro Istituto è stato inoltre costituito il gruppo di lavoro "E-Safety Policy", coordinato dal referente bullismo e cyberbullismo, a supporto di un percorso di individuazione dei punti di forza e debolezza della scuola, nonché degli ambiti di miglioramento e delle azioni da adottare per la sicurezza online e per un uso positivo

delle tecnologie digitali nella didattica e nell'ambiente scolastico.

Il gruppo, composto da alcuni docenti e dal dirigente, ha tra i suoi compiti quelli di:

utilizzare la piattaforma del progetto Generazioni Connesse (www.generazioniconnesse.it) per seguire il percorso di formazione online sui temi dell'Educazione Civica Digitale e acquisire competenze finalizzate ad insegnare un uso consapevole della rete;
elaborare il documento di ePolicy, monitorarne attuazione ed efficacia, aggiornarlo periodicamente.

I Docenti

hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle Tic e della Rete, garantiscono che le modalità di un utilizzo corretto e sicuro siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;

si informano e si aggiornano sulle problematiche di sicurezza nell'utilizzo delle TIC e di Internet;
conoscono la politica di sicurezza adottata dalla scuola. Rispettano il regolamento condiviso e si assicurano che gli studenti e le studentesse capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di Internet;
valorizzano presso le classi le opportunità di ricerca offerte dalle tecnologie digitali e dalla rete, ma sottolineano anche la necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
rispettano il codice di comportamento professionale nelle comunicazioni digitali con gli alunni o i genitori, utilizzando i sistemi scolastici ufficiali e rispettando la riservatezza dei dati personali trattati ai sensi della norma vigente; controllano l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc, da parte degli studenti e delle studentesse durante le lezioni e ogni attività scolastica, secondo il Regolamento d'Istituto;
segnalano ai vari Referenti problemi e proposte di carattere tecnico organizzativo, al DS abusi o violazioni rilevati a scuola nei confronti degli alunni in relazione all'utilizzo delle TIC, della rete ed episodi critici legati ad atti di bullismo o cyberbullismo, che vedono coinvolti studenti e studentesse.

Il Direttore dei Servizi Generali e Amministrativi

assicura, 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;

garantisce il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.), al suo interno e fra la stessa e le famiglie degli alunni, per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

Il Tecnico informatico

può controllare ed accedere a tutti i file della intranet;

è l'unico a poter installare nuovi software;
coordina con il referente la prenotazione dei laboratori informatici consentendo di tenere traccia di ore e laboratorio utilizzati da ciascuno.

Il Personale Amministrativo, Tecnico e Ausiliario (ATA)

svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il dirigente scolastico e con il personale docente tutto. È coinvolto nelle attività di formazione e autoformazione in tema di bullismo e cyberbullismo. Il personale ATA può essere coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo.

Gli Studenti e le studentesse

Agli alunni è richiesto di:

essere responsabili, in relazione al proprio grado di maturità e di apprendimento, nell'utilizzo dei sistemi delle tecnologie digitali in coerenza 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 o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori;
rispettare il Regolamento d'Istituto e il Patto di corresponsabilità; segnalare ogni abuso, violazione e atti riconducibili ad episodi di bullismo e cyberbullismo nei confronti di se stessi o altri compagni.

I Genitori

I genitori, in continuità con l'Istituto scolastico, devono:

- sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica; essere partecipi e attivi nelle azioni di promozione ed educazione sull'uso consapevole delle TIC e della rete, nonché sull'uso responsabile dei device personali;
- relazionarsi in modo costruttivo con i docenti sulle linee educative riguardanti le TIC e la rete;
- 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;
- accettare e condividere quanto scritto nell'e-Policy dell'Istituto.

È molto importante che tutti gli attori della comunità scolastica (docenti, personale, alunni) si facciano promotori del documento di ePolicy.

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

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

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

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti

e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

Tutti gli enti educativi esterni e le varie associazioni presenti sul territorio che entrano in relazione con il nostro Istituto si conformano alla politica riguardo all'uso consapevole e responsabile della Rete e delle TIC che la scuola ha condiviso. Essi promuovono comportamenti sicuri e assicurano la protezione degli alunni durante le attività che si svolgono insieme, segnalando ai docenti preposti e al Dirigente Scolastico eventuali comportamenti problematici o casi di abuso nell'uso della rete e delle TIC.

L'Istituto si riserva di richiedere ai soggetti esterni il casellario giudiziario come fattore ulteriore di protezione nei confronti dei minori (Condanne per alcuni reati previsti dal Codice penale e nello specifico gli articoli 600-bis (prostituzione minorile), 600-ter (pornografia minorile), 600-quater (detenzione di materiale pornografico), 600- quinquies (iniziative turistiche volte allo sfruttamento della prostituzione minorile), 609-undecies (adescamento di minorenni), o l'irrogazione di sanzioni interdittive all'esercizio di attività che comportino contatti diretti e regolari con i minori).

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.

Al fine di condividere e comunicare al meglio il documento di ePolicy a tutta la comunità

scolastica, sono previste le seguenti azioni, da ripetersi con cadenza annuale:

- presentazione e discussione del documento e di altro materiale informativo, inerente la linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet, nelle adunanze degli organi collegiali e durante uno specifico incontro di aggiornamento interno;

- presentazione del documento al personale A.T.A. durante uno specifico incontro di aggiornamento interno;

- presentazione del documento ai rappresentanti dei genitori e ai rappresentanti degli studenti

durante incontri appositamente organizzati ad inizio anno scolastico;

- presentazione del documento a tutte le classi, ad inizio anno scolastico, e inserimento dei contenuti dello stesso nella programmazione didattica, nell'ambito dell'educazione alla cittadinanza digitale;

- organizzazione di momenti di formazione rivolti alle famiglie sulla conoscenza del documento di ePolicy e sull'approfondimento dell'uso corretto delle TIC, anche in presenza di esponenti delle Forze dell'ordine o della Polizia postale.

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.

Infrazioni degli alunni

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola utilizzando

le TIC e la rete internet, messe a loro disposizione per fini puramente didattici, sono prevedibilmente le seguenti:

uso improprio della rete per giudicare, infastidire o impedire a qualcuno di esprimersi liberamente o partecipare al dialogo didattico-educativo; invio incauto e non autorizzato di foto o dati personali, quali l'indirizzo di casa o il telefono;
condivisione di immagini non appropriate, violente, intime o troppo spinte;
comunicazione incauta e senza permesso con sconosciuti o soggetti comunque estranei all'azione didattico-educativa;
collegamento a siti web non indicati e, dunque, non autorizzati dai docenti durante le attività laboratoriali di qualsiasi genere.

I provvedimenti "disciplinari" da adottare da parte dei consigli di classe nei confronti degli alunni che abbiano commesso una o più infrazione al documento E-policy, secondo quanto sopra, saranno proporzionati all'età e alla gravità del comportamento e si sostanzieranno nei seguenti:

- richiamo verbale

- richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);

- richiamo scritto con annotazione sul Registro Elettronico;

- nota informativa ai genitori o tutori mediante registro elettronico; -

convocazione dei genitori o tutori da parte degli insegnanti;

- convocazione dei genitori o tutori da parte del Dirigente scolastico. Le

denunce di bullismo online saranno trattate in conformità alla legge.

Contestualmente sono previsti interventi educativi di rinforzo rispetto a comportamenti corretti e riparativi dei disagi causati, di ridefinizione delle regole sociali di convivenza, di prevenzione e gestione positiva dei conflitti, di pro-socialità, di conoscenza e gestione delle emozioni. Possono essere presi in considerazione percorsi di formazione per tutta la classe, assegnazione di attività aggiuntive da svolgere a casa sui temi di Cittadinanza e Costituzione.

Infrazione del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico, in particolare i

docenti, incorra nell'utilizzo delle tecnologie digitali e di internet sono prevedibilmente le seguenti:

- utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di docenza o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiale non idoneo; utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- trattamento dei dati personali e dei dati sensibili degli alunni non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- diffusione delle password assegnate e incauta custodia degli strumenti e degli accessi di cui possono approfittare terzi;
- assente o carente istruzione preventiva degli alunni sull'uso corretto e responsabile delle TIC e di internet;
- vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili rischi connessi;
- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente Scolastico, all'Animatore digitale.

Il Dirigente scolastico può disporre il controllo 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 non adeguati o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali approfondimenti successivi.

Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio dei procedimenti che possono avere carattere organizzativo-gestionale, disciplinare, amministrativo, penale, a seconda del tipo e della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

Infrazioni dei genitori

In considerazione dell'età degli studenti e delle studentesse, anche talune condizioni e condotte dei genitori medesimi possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli allievi a scuola. Gli atteggiamenti da parte della famiglia meno favorevoli sono:

- l'idea che nell'uso del pc a casa il figlio sia al sicuro e che non corra alcun rischio;
- una posizione del computer in una stanza o in un posto non visibile a tutti e non controllabile dall'adulto;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'uso di cellulare o smartphone;

un utilizzo di cellulari e smartphone in comune con gli adulti che possono conservare in memoria indirizzi di siti o contenuti non idonei a minori.

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionati a norma di legge in base alla gravità dei comportamenti dei loro figli.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

Il presente documento va ad integrare le norme già vigenti nell'Istituto e costituisce modello di riferimento per ulteriori regolamenti futuri. Si integra pienamente con obiettivi e contenuti dei seguenti documenti:

PTOF

Regolamento interno di Istituto

Regolamento per la Didattica Digitale Integrata

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 dell'implementazione dell'ePolicy, e del suo eventuale aggiornamento, sarà svolto ogni anno. L'aggiornamento del documento sarà curato dal Dirigente Scolastico, con la collaborazione dell'animatore digitale, dal docente Referente di Istituto per la prevenzione e il contrasto del bullismo e cyberbullismo e dal gruppo di lavoro e Safety-Policy d'Istituto.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

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 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 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 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.

Tale curricolo digitale interesserà tutte le classi e tutti gli indirizzi e verterà sui temi della cittadinanza digitale e dell'uso sicuro e consapevole della rete.

Il percorso verrà progettato e realizzato sia da docenti interni alla scuola, con lo specifico supporto dei docenti di diritto e di informatica, sia da professionisti esterni, facenti capo a enti, associazioni o forze dell'ordine, con cui approfondire, per esempio, il tema delle fake news e dell'informazione sui social network e in rete.

In particolare l'Istituto intende sviluppare le seguenti tematiche:

Bullismo, cyberbullismo e reati digitali;
utilizzo sicuro della rete;
privacy e utilizzo dei dati personali;
gestione della propria "identità digitale";
Netiquette", ovvero le norme di comportamento online;

diritto all'informazione in rete, fake news, hate speech.

Per lo svolgimento delle attività, per reperire via via risorse, contenuti multimediali, strumenti idonei alla progettazione, ci avvarremo di documentazione e siti di validata affidabilità, in particolare del sito del Progetto 'Safer Internet Centre – Generazioni Connesse', co-finanziato dalla Commissione Europea e coordinato dal MI con il partenariato di alcune delle principali realtà italiane che si occupano di sicurezza in Rete (Autorità Garante per l'Infanzia e l'Adolescenza, Polizia di Stato, il Ministero per i Beni e le Attività Culturali, gli Atenei di Firenze e 'La Sapienza' di Roma, Save the Children Italia, Telefono Azzurro, la cooperativa EDI onlus, Skuola net e l'Agenzia di stampa DIRE e l'Ente Autonomo Giffoni Experience). Faremo riferimento anche ad altri siti rilevanti in questo contesto, come l'E-Safer Center stesso e il sito del progetto 'Parole Ostili'.

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.

La competenza digitale, oggi, è imprescindibile per i docenti così come per gli studenti e le

studentesse e permette di integrare la didattica con strumenti che la diversificano, la rendono

innovativa e in grado di venire incontro ai nuovi stili di apprendimento.

Per tale motivo, l'Istituto riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola (ad es. con l'aiuto dell'animatore digitale), dalle reti di scuole e dall'amministrazione, sia a quelle liberamente scelte dai docenti (anche online) sulle TIC, impegnandosi ad organizzare ogni anno momenti di

formazione sui metodi e sugli strumenti della didattica digitale.

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.

Presso il nostro Istituto è stata incentivata la formazione dei docenti sulle tematiche dell'inclusione, dell'uso consapevole delle TIC (uso della Lim, uso del Registro Elettronico). Negli anni passati sono stati realizzati incontri con la Polizia Postale e la Polizia di Stato sui rischi on line e sul bullismo e sul cyberbullismo.

Presso la scuola, in considerazione della normativa vigente, saranno implementati diversi tipi di interventi.

L'animatore e il team Digitale, insieme alla FS dell'area Formazione, promuoveranno o organizzeranno nell'arco del triennio i seguenti interventi formativi mirati:

1. azioni di formazione strutturate dall'Animatore e il team digitale , con l'ausilio di esperti

esterni, sui rischi della rete;

2. percorsi di autoaggiornamento individuali e/o collettivi con interventi mirati su specifici argomenti (ad es. webinar) tramite piattaforme collaborative, di cui verrà fatto apposito richiamo sul sito web della scuola.

3. azioni di sensibilizzazione ed informazione, a mezzo Circolari, rivolte ai docenti tutti sulle attività intraprese a livello ministeriale (MI USR, USP), dagli Osservatori regionali sul bullismo, dalle scuole Polo anche da enti formatori accreditati e qualificati;

4. interventi di consulenza e supporto relativamente ai casi di bullismo e cyberbullismo.

Tali azioni verranno inserite nel Piano Triennale dell'Offerta Formativa e nel Piano di

Formazione; saranno promosse anche tramite una pagina dedicata alla formazione sul sito web della scuola.

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 metterà in atto una campagna di sensibilizzazione delle famiglie per promuovere la conoscenza delle situazioni di rischio in rete e favorire l'uso consapevole di internet, mediante:

- Pubblicazione della ePolicy sul sito e condivisione della stessa con i genitori;
- Condivisione del materiale digitale messo a disposizione dal sito Generazioni Connesse.

Il nostro piano d'azioni

AZIONI (da sviluppare nell’arco dell’anno scolastico 2019/2020)

Scegliere almeno 1 di queste azioni

Effettuare un’analisi del fabbisogno formativo su un campione di

studenti e studentesse in relazione alle competenze digitali. Effettuare un’analisi del fabbisogno formativo del corpo docente sull’utilizzo 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.

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

Scegliere almeno 1 di queste azioni

Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell’ambito dell’educazione alla cittadinanza digitale.

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.

Come riportato nell’informativa privacy policy d’Istituto, la scuola può trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali oppure quelli espressamente previsti dalla normativa di settore, tutelandone la segretezza come previsto dalle leggi vigenti. I dati saranno trattati con o senza ausilio di strumenti elettronici e comunque automatizzati secondo le modalità e le cautele, come riportato nell’Informativa ex art. 13 e 14 GDPR 2016/679, pubblicata sul sito della scuola, e conservati per il tempo necessario all’espletamento delle attività amministrative e istituzionali.

Lo studente e/o la propria famiglia hanno il diritto di conoscere quali informazioni che li riguardano sono conservate presso la scuola, di rettificare o aggiornare il contenuto. Per esercitare questi diritti è possibile rivolgersi direttamente al “titolare del trattamento” (la scuola) anche tramite suoi incaricati “responsabili del trattamento”.

Per le attività di ampliamento dell’offerta formativa, organizzate in collaborazione con Enti ed esperti esterni, viene richiesto preventivamente ai genitori il consenso alle riprese audio/ video e al loro eventuale utilizzo per scopi didattici, informativi e divulgativi.

L’istituto gestisce il complesso e delicato aspetto della protezione dei dati personali con l’ausilio di

una società di consulenza esterna e, per quanto riguarda la gestione del sito web istituzionale, con il supporto dell’animatore digitale.

Nell'istituto, inoltre, è stato attivato un sistema di cifratura per la gestione dei file personali degli

studenti che consente la protezione dei dati sensibili.

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' istituzione scolastica garantisce il diritto di ogni studente a connettersi ad Internet, in quanto in ogni aula delle tre sedi dell'Istituto è presente una postazione informatica composta da: notebook, webcam, casse audio e LIM collegate alla rete LAN con connessione a banda larga. I dispositivi sono configurati in modo da permettere l'accesso come amministratore solo al personale addetto alla gestone degli stessi, mentre agli alunni è consentito l'accesso solo come utenti standard. L'Istituto è dotato di laboratori informatici, linguistici e di due aule 3.0, di cui possono disporre le diverse classi, forniti di postazioni PC, LIM e collegamento ad internet. L'Istituzione scolastica, inoltre, mette a disposizione degli alunni che non hanno la possibilità di acquistare un proprio dispositivo diversi notebook.

La scuola è cablata per assicurare l'accesso da tutti i dispositivi presenti nelle aule. Le infrastrutture di rete all'interno dell'edificio raggiungono ogni aula, laboratorio, ufficio e ambiente ricreativo delle tre sedi. Il collegamento avviene sia tramite cavo che

tramite access point; alla rete wifi si accede attraverso password fornita dalla scuola. L'Istituto ha di recente potenziato la propria rete Wi-Fi, al fine di garantire un migliore servizio per tutte le classi. Esso è impegnato, attraverso bandi europei, a reperire fondi per potenziare/aggiornare la rete internet e acquistare nuovi devices quali pc, tablet e postazioni mobili.

Per le sedi di Cardito e via Covotti, è stato sottoscritto un contratto di fornitura per assicurare alle stesse una banda minima garantita (BMG). I docenti hanno piena autonomia nel collegamento ai siti web nelle postazioni loro riservate. Agli alunni, invece, durante l'attività didattica, è consentita la navigazione guidata da parte degli insegnanti e la scrittura di documenti collaborativi.

Nell'utilizzo della rete internet gli studenti si impegnano a:

- utilizzare in modo consapevole e corretto la Rete e i dispositivi telematici, nel rispetto della privacy e della dignità propria e altrui;
- rispettare le consegne dei docenti;
- non scaricare materiali e software senza autorizzazione;
- non utilizzare unità removibili personali senza autorizzazione;
- segnalare immediatamente materiali inadeguati ai propri insegnanti.

I docenti, a loro volta, si impegnano a:

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

monitorare l'uso delle tecnologie da parte degli studenti.

Periodicamente vengono svolte le seguenti attività:

la ricognizione dello status quo della tecnologia e della connettività per ottimizzare acquisti e utilizzo;
l'analisi dei bisogni della scuola in relazione alle reali esigenze didattiche e agli obiettivi prefissati.

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.

Gli strumenti di comunicazione online utilizzati dalla scuola curano sia la comunicazione interna che quella esterna.

Per la comunicazione esterna la scuola utilizza il sito web d'Istituto: www.istitutosuperioreruggerosecondo.edu.it, costantemente aggiornato, al fine di valorizzare e promuovere le attività didattiche, di diffondere all'interno informazioni di servizio o contenuti importanti fra i diversi attori scolastici, nonché di trasmettere all'esterno i valori, le azioni, i progetti e il percorso educativo che l'Istituzione scolastica porta avanti.

Per la comunicazione interna la scuola si serve dei seguenti strumenti:

registro elettronico, Portale Argo di Argo Software S.r.l, tramite il quale i genitori e gli studenti possono verificare l'andamento scolastico (controllando la frequenza, i voti, le eventuali note disciplinari) ed essere aggiornati sullo svolgimento delle programmazioni disciplinari e sulle attività organizzate dalla scuola. Tale strumento permette, inoltre, ai dipendenti di richiedere e gestire permessi di lavoro e comunicare le assenze;
posta elettronica (email istituzionale) per tutte le comunicazioni e per l'organizzazione dei turni del personale A.T.A.;
piattaforme come Classroom e Google - Suite for Education, applicativi per lo

svolgimento della DID, che hanno favorito un lavoro collaborativo e condiviso, rendendo possibile un agevole passaggio alla didattica a distanza nel periodo di lockdown;

comunicazione telefonica;

chat informali tra colleghi, tra docenti e genitori, docenti ed alunni.

Gli studenti e le studentesse dell' Istituto Ruggero II hanno ricevuto un indirizzo di posta elettronica personale, con il quale poter accedere ai servizi offerti esclusivamente per un uso didattico. Le famiglie sono responsabili, in accordo con i docenti, dell'utilizzo degli account.

È vietato utilizzare l' account scolastico per registrarsi su piattaforme di gioco online o sui social network ad uso personale (Facebook, Twitter,Tik-Tok, ecc). In caso di violazione accertata, l'account viene sospeso dall'amministratore del dominio e ripristinato dopo ulteriori accertamenti.

Gli studenti devono utilizzare l'account personale per accedere alle piattaforme e learning e tutte le attività TIC della scuola stessa.

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.

La nostra scuola favorisce approcci di tipo BYOD- Bring your own device, promuovendo l'uso dei dispositivi elettronici durante lo svolgimento dell'attività didattica.

Come esplicitato nel patto di corresponsabilità e nel Regolamento d'istituto, l'uso dei

dispositivi elettronici è vietato durante le attività didattiche e all'interno dell'Istituto, se non per finalità scolastiche.

Durante le lezioni gli studenti sono autorizzati ad utilizzare la strumentazione personale quali pc, tablet solo ed esclusivamente per uso didattico e sotto il controllo del docente; non è permesso loro utilizzare i telefoni cellulari per telefonare, scattare foto, registrare filmati . È vietato inviare messaggi illeciti o inappropriati, nonché fotografie o filmati. Agli alunni con BES o DSA, la scuola garantisce il supporto tecnologico idoneo, ma su richiesta dell'interessato; agli stessi è consentito l'uso della strumentazione personale con la costante supervisione del docente eventualmente anche con l'accesso alla rete wi-fi dell'istituto.

Ai docenti è consentito l'uso di altri dispositivi elettronici personali (PC, tablet) sempre solo a scopo didattico ed integrativo di quelli scolastici disponibili; la scuola consente l'accesso alla rete wi-fi negli spazi comuni previsti dalla logistica della rete stessa.

Per tutto il personale scolastico, l'uso dei dispositivi è ammesso solo per attività

funzionali al servizio.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022).

Scegliere almeno 1 di queste azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- 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)

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 incontri per la consultazione degli studenti/studentesse suindicazioni/regolamenti sull'uso dei dispositivi digitali personali

Organizzare incontri per la consultazione dei genitori su indicazioni/regolamentisull'uso dei dispositivi digitali personali
Organizzare uno o più eventi o attività volti a formare 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.*

Scuola e famiglia rivestono un ruolo fondamentale nella educazione alla convivenza democratica, al rispetto dell'altro, ad una società sempre più policentrica, stratificata e mutevole. La capacità di vivere in maniera positiva e formativa, la presenza di compagni distanti per provenienza sociale, economica, geografica, per tradizioni o percorsi di vita, è la sfida più grande cui sono chiamate le comunità educanti. La

scuola è chiamata ad adottare misure di prevenzione e contrasto di ogni forma di violenza e di prevaricazione; la famiglia è chiamata a collaborare, educando i propri figli e vigilando sui loro comportamenti. Senza demonizzare gli strumenti tecnologici o il gioco, è necessario entrare in relazione con il mondo degli studenti e delle studentesse, stabilendo chiare e semplici regole di utilizzo di tali strumenti.

Educare alla diversità, innanzitutto, è la grande opportunità di prevenzione.

La nostra scuola intende sviluppare una riflessione sul tema dei rischi online e promuovere negli alunni, nei docenti e nelle famiglie la consapevolezza dei comportamenti pericolosi attraverso la diffusione di informazioni. Si impegna, inoltre, a fornire possibili soluzioni con la collaborazione di altri enti territoriali (Polizia postale, Asl, Servizi sociali, Sportello d'ascolto interno). Promuove azioni di formazione per sviluppare le competenze digitali degli studenti e dei docenti al fine di garantire un uso consapevole e sicuro delle TIC.

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).

Il cyberbullismo o bullismo elettronico è una forma di prepotenza virtuale messa in atto attraverso l'uso di internet e delle tecnologie elettroniche e informatiche. Come il bullismo tradizionale è una forma di prevaricazione e di oppressione ripetuta nel tempo, perpetrata da una persona o da un gruppo di persone più potenti nei confronti di un'altra percepita come debole. A differenza del bullismo tradizionale, in cui il bullo esercita direttamente nei confronti della vittima violenze di tipo fisico o sociale, in questa nuova forma di aggressività il cyberbullo molesta "indirettamente" la vittima attraverso la messaggistica istantanea, i blog, gli sms, condivisioni e altre azioni fatte per umiliare la vittima davanti al pubblico della rete.

4.2.1. Le caratteristiche del fenomeno

L'impatto: la diffusione di materiale tramite Internet è incontrollabile e non è possibile prevederne i limiti. Un contenuto offensivo e denigratorio online può,

quindi, diventare virale e distruggere in alcuni casi la reputazione della vittima. Nelle situazioni più gravi, le vittime di cyberbullismo si trovano costrette a dover cambiare scuola o addirittura città, ma questo spesso non le aiuta. La Rete, si sa, è ovunque.

La convinzione dell'anonimato: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile. Sentendosi protetti dall'anonimato ci si sente liberi e più forti nel compiere atti denigratori, senza il timore di essere scoperti. È importante tenere bene a mente, però, che quello dell'anonimato è un "falso mito della Rete". Ogni nostra azione online è, infatti, rintracciabile e riconducibile a noi con gli strumenti opportuni o con l'intervento della Polizia Postale. L'anonimato del cyberbullo, inoltre, è causa di forte stress per la vittima, la quale molte volte non può dare né un nome e né un volto al proprio aggressore.

Assenza di confini spaziali: il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo di un qualsiasi rifugio. La vittima è sempre raggiungibile anche a casa e vive nella costante percezione di non avere vie di fuga. Spegnere il cellulare o il computer non basta, così come cancellare tutti i propri profili social. Il solo pensiero che

eventuali contenuti denigratori continuino a diffondersi online è doloroso e si accompagna ad un senso costante di rabbia e impotenza.

Assenza di limiti temporali: può avvenire a ogni ora del giorno e della notte. La vittima, dal canto suo, vede enormemente amplificati i soprusi subiti, primo perché possono raggiungerla in qualunque momento, secondo, perché, come nel caso delle chat di gruppo o dei social network, messaggi verbali, immagini o video che la riguardano possono diventare visibili a un vasto pubblico di spettatori.

Indebolimento dell'empatia: esistono cellule chiamate neuroni specchio che ci permettono di "leggere" gli altri quando li abbiamo di fronte, capirli e di provare emozioni simili a quelle che loro provano, proprio come se fossimo di fronte ad uno specchio. Tale sensazione è data dall'attivazione di una particolare area del cervello. Quando le interazioni avvengono prevalentemente online la funzione speciale di questi neuroni viene meno (mancando la presenza fondamentale dell'altro che è sostituito dal dispositivo). La riduzione di empatia che ne consegue può degenerare nei comportamenti noti messi in atto dai cyberbulli.

Feedback non tangibile: il cyberbullo non vede in modo diretto le reazioni della vittima e, ancora una volta, ciò riduce fortemente l'empatia e il riconoscimento del danno provocato. Per questo il cyberbullo non è mai totalmente consapevole delle conseguenze delle proprie azioni. L'impossibilità di vedere con i propri occhi l'eventuale sofferenza e umiliazione provata dalla vittima fa sì che il tutto venga percepito come "uno scherzo" divertente a cui partecipare, di cui ridere o a cui essere indifferenti. Inoltre, il cyberbullismo non lascia segni fisici evidenti sulla vittima e si consuma in un contesto virtuale che spesso viene percepito dai ragazzi come non "reale", come un mondo ludico a sé stante.

È possibile suddividere gli atti di cyberbullismo in due grandi gruppi:

1. **cyberbullismo diretto**: il bullo utilizza strumenti di messaggistica istantanea che hanno un effetto immediato sulla vittima;
2. **cyberbullismo indiretto**: il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico.

Il bullismo cibernetico è un fenomeno sociale e di gruppo. Infatti, centrale è il ruolo delle agenzie educative e di socializzazione (formali e informali) più importanti per gli adolescenti: la famiglia, la scuola e il gruppo dei pari.

Willard ha identificato sette categorie attraverso le quali esso si manifesta:

Flaming: spedire messaggi rabbiosi, rudi o volgari ad una persona in un forum online o via e-mail o tramite qualsiasi altro sistema elettronico di messaggistica;

Molestie online: spedire ripetutamente messaggi offensivi via e-mail tramite qualsiasi altro dispositivo elettronico di messaggistica;
Cyberstalking: molestie online che includono minacce fisiche o che sono eccessivamente intimidatorie;
Denigrazione: spedire dichiarazioni o postare materiale online relativo ad una persona che sia dannoso, falso o crudele per danneggiarne la reputazione;
Mascheramento: assumere identità altrui e spedire messaggi o postare materiale per fare in modo che quella persona sembri cattiva;
Divulgazione: spedire o postare online del materiale che contiene informazioni private, delicate o imbarazzanti, incluse immagini o messaggi privati; **Esclusione**: escludere crudelmente qualcuno da una community o da un gruppo online

Ecco alcuni segnali generali che può manifestare la potenziale vittima di cyberbullismo:

Appare nervosa quando riceve un messaggio o una notifica;
Sembra a disagio nell'andare a scuola o finge di essere malata (ha spesso mal di stomaco o mal di testa);
Cambia comportamento ed atteggiamento in modo repentino;
Mostra ritrosia nel dare informazioni su ciò che fa online;
Soprattutto dopo essere stata online, mostra rabbia o si sente depressa; Inizia ad utilizzare sempre meno Pc e telefono (arrivando ad evitarli); Perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;
Il suo rendimento scolastico peggiora.

4.2.2 Minori e responsabilità dei genitori e della scuola per culpa in educando e vigilando

Una definizione tecnico-giuridica del termine cyberbullismo è desumibile dalla Legge 29

maggio 2017, n. 71 in materia di ***"Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo".***

Al 2° comma dell'art. 1 si legge testualmente:

"Ai fini della presente legge, per «cyberbullismo» si intende 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".

Il cyberbullismo può essere un illecito civile, penale, del Codice della privacy (D.Lgs 196 del 2003) e dei fondamentali precetti dei diritti umani e costituzionali.

Gli illeciti penali sono racchiusi in:

-Sostituzione di persona (art. 494 c.p.);

-Percosse (art. 581 c.p.);

-Lesione personale (art. 582 c.p.);

-Ingiuria (art. 594 c.p.);

-Diffamazione (art. 595 c.p.);

-Violenza privata (art. 610 c.p.);

-Minaccia (art. 612 c.p.);

-Atti persecutori – (art. 612 bis c.p.);

-Estorsione (art. 629 c.p.);

-Danneggiamento alle cose (art. 635 c.p.);

-Molestia o Disturbo alle persone (art. 660 c.p.).

L'art 167 del Codice della privacy rubricato ***"Trattamento illecito di dati"*** dispone:

1° comma: ***"Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi".***

2° comma: "***Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni".***

Le violazioni delle norme Costituzionali sono ascrivibili a

– Art. 2 Cost.: sono riconosciuti e garantiti i diritti inviolabili dell'uomo come la dignità della persona;

– Art. 3 Cost.: principio di uguaglianza formale (1° comma) e sostanziale (2° comma);

– Art. 15 Cost.: libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione;

– Art. 28 Cost.: responsabilità degli insegnanti e dello Stato;

– Art. 30 Cost.: è dovere e diritto dei genitori mantenere, istruire ed educare i figli (culpa in educando e in vigilando);

– Art. 33 Cost.: libertà di insegnamento (1° comma) ed istituzione di scuole statali (2° comma);

– Art. 34 Cost.: libero accesso all'istruzione scolastica (1° comma), obbligatorietà e gratuità dell'istruzione dell'obbligo (2° comma), riconoscimento del diritto di studio (3° comma).

4.2.3.Responsabilità e conseguenze

Nel definire responsabilità e conseguenze del bullismo dobbiamo però partire ricordando i capisaldi del nostro ordinamento giuridico.

La responsabilità penale, quella cioè conseguente al compimento di un reato, è solo personale: ricade cioè unicamente su chi commette l'azione illecita. Questi ne risponde se ha compiuto almeno 14 anni, subendo così tanto il processo quanto le relative sanzioni. Mai la responsabilità penale può essere scaricata su altri soggetti come genitori o insegnanti: neanche quella di un minorenne.

Discorso diverso vale per la responsabilità civile ossia per l'obbligo di risarcire la vittima: questa scatta solo al compimento dei 18 anni. A rispondere invece delle conseguenze della condotta illecita di un minorenne sono i suoi genitori o coloro che ne hanno la custodia (gli insegnanti dal momento in cui questi entra a scuola sino a quando ne esce). Il minore quindi non paga mai i danni dei suoi reati, pur subendone le relative sanzioni penali.

Dunque, in relazione a un reato come il bullismo posto da un minorenne, sarà questi – se ha almeno 14 anni – a rispondere penalmente della propria condotta, mentre i danni alla

vittima vanno pagati dai suoi genitori.

Se il bullo ha meno di 13 anni il reato non può essere punito, fermo restando l'obbligo di risarcimento in capo al padre e alla madre.

Una volta analizzati i principi generali della responsabilità civile e penale possiamo vedere, più nel dettaglio quali sono le responsabilità e le conseguenze penali del bullismo.

Bullismo: responsabilità degli insegnanti

Ai sensi dell'articolo 2048 del Codice civile, gli insegnanti sono responsabili ,civilmente, del danno cagionato dai loro allievi nel tempo in cui sono sotto la loro vigilanza a meno che provino di non aver potuto impedire il fatto, ossia di aver fatto

tutto il possibile per anticipare la condotta illecita ed eliminarne le conseguenze dannose.

A seguito della riforma del 2017, per dimostrare di aver fatto tutto il possibile al fine di evitare le condotte lesive, l'insegnante non può più limitarsi a dimostrare di aver vigilato sugli studenti, ma deve provare di aver messo in atto anche strumenti educativi e preventivi come i corsi e i laboratori pratici contro il bullismo. Così, è legittima la sanzione disciplinare irrogata a un'insegnante che isola la vittima di bullismo anziché sostenerla, «dimostrando di non rendersi conto della gravità dei fatti» Come detto, il ministero dell'Istruzione e la scuola (per conto degli insegnanti) devono risarcire il danno alla vittima del bullismo se l'atto violento viene posto dall'inizio alla fine delle lezioni o meglio da quando l'alunno entra nell'istituto a quando ne esce, intervallo compreso.

Responsabilità dei genitori

La responsabilità non è solo della scuola.

Sui genitori ricade un obbligo ancora più pregnante rispetto a quello di vigilanza degli insegnanti: quello di fornire una ferrea educazione al figlio.

Come per i professori, anche per i genitori vale l'esonero della responsabilità se dimostrano di «non aver potuto impedire il fatto», ma la prova è estremamente difficile. Difatti, nel compiere l'atto di bullismo, il giovane dimostra di non aver ricevuto una corretta educazione. È proprio nel gesto stesso che è implicita la responsabilità dei genitori. Del resto, se il giovane fosse stato educato per come si deve non avrebbe mai commesso il reato, sicché il problema non si sarebbe posto già alla radice.

4.2.4. Come intervenire?

La Legge 71/2017 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 statuiscono:

- 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

In questo processo la scuola gioca un ruolo fondamentale, infatti, individua un referente per il contrasto del cyberbullismo, deputato a coordinare le iniziative di sensibilizzazione e prevenzione rapportandosi con le Forze di Polizia, le associazioni e i centri di aggregazione giovanile presenti sul territorio.

Tuttavia, una solo persona non è sufficiente: è fondamentale che tutti coloro che operano all'interno dell'ambiente scolastico (Docenti, Dirigente Scolastico e personale) conoscano le modalità di sviluppo di questi fenomeni e siano in grado di gestirli, comprendendo le dinamiche, i rischi e le sanzioni a essi collegati.

La scuola, con il suo compito educativo e didattico, è infatti chiamata a vigilare, secondo diverse modalità e secondo diversi gradi di responsabilità, sull'operato dei ragazzi, e ad assicurarsi che non si verifichino episodi di violenza ai danni degli studenti, ma anche degli insegnanti stessi.

L'IISS Ruggero II, sensibile alla prevenzione dei fenomeni di Bullismo e Cyberbullismo, promuove da anni, in collaborazione con soggetti esterni alla scuola (Servizi sociali e sanitari, Polizia Postale, associazioni ed esperti operanti sul territorio), attività laboratoriale di sensibilizzazione e di informazione, al fine di favorire tra gli studenti un dibattito sulle tematiche in oggetto. La nostra scuola, nell'a.s. 2020/21, ha preso parte al monitoraggio online della piattaforma ELISA, attività finalizzata a valutare la presenza e l'andamento nel tempo del bullismo, cyberbullismo e della qualità delle relazioni sociali.

L'azione è stata effettuata con la compilazione di un questionario online da parte di tutti gli alunni e dei docenti del Ruggero II.

Il sistema di monitoraggio offrirà alla scuola un report sintetico personalizzato che permetterà di approfondire la situazione del contesto scolastico rispetto ai fenomeni del bullismo e del cyberbullismo. E' stata attivata, inoltre, la casella di posta elettronica d'istituto help@istitutosupereiorebruno-dorso.it, attraverso la quale gli studenti possono comunicare il proprio disagio, inoltrare segnalazioni e richieste di aiuto.

E' stato predisposto un modello per la segnalazione dei casi di bullismo, cyberbullismo e di ogni altra forma di prevaricazione e creato lo sportello d'ascolto. Tutti gli alunni delle classi seconde dell'Istituto hanno preso parte agli eventi multimediali nazionali in diretta streaming organizzati dalla Polizia Postale e delle Comunicazioni, nell'ambito del progetto

#Cuoriconnessi.

L’istituzione scolastica, in ottemperanza alle nuove linee di Orientamento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo, si impegna a realizzare le seguenti azioni:

Revisionare e integrare il regolamento d’istituto con definizione di un “sistema

sanzionatorio antibullismo”, che preveda specifici riferimenti a condotte di bullismo e cyberbullismo, sanzioni disciplinari e organi deputati ad irrogarle; Organizzare incontri con studenti e genitori realizzati da soggetti esterni alla scuola, quali servizi sociali e sanitari, Polizia Postale, associazioni ed esperti operanti sul territorio, per affrontare la tematica del cyberbullismo ai tempi della “scuola digitale”.

Inserire tra i referenti degli alunni, come formatori, gli ex alunni e quelli delle classi quinte.

Formare/informare docenti, studenti, famiglie e personale ATA, sui temi dei regolamenti e delle procedure adottate dal referente per il bullismo e il cyberbullismo e dal gruppo “E-Policy.

Realizzare un spazio sul sito della scuola dedicato alla problematica del cyberbullismo dal quale poter attingere materiale informativo e formativo, sitografia, buone prassi, materiale strutturato per i docenti.

Pianificare e realizzare progetti di peer-education, sui temi della sicurezza online nella scuola, al fine di promuovere un ruolo attivo degli studenti nella prevenzione e nel contrasto al bullismo e al cyberbullismo.

Implementare corsi di formazione, con l’intervento di esperti esterni, sui fenomeni di bullismo e cyberbullismo, sui principali strumenti utilizzati per lo studio e la prevenzione degli stessi, sui temi dello sviluppo affettivo e dell’intelligenza emotiva.

Promuovere percorsi formativi per insegnanti volti a favorire l’acquisizione delle competenze necessarie alla costruzione di un clima scolastico cooperativo e solidale e alla gestione delle dinamiche di gruppo, al fine di prevenire ed arginare il fenomeno bullismo nelle sue diverse manifestazioni.

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.

Come riconoscerlo e prevenirlo:

● Il discorso d’odio procura sofferenza. La parola ferisce, e a maggior ragione l’odio. Il discorso può violare i diritti umani. Il discorso d’odio online non è meno grave della sua espressione offline, ma è più difficile da individuare e da combattere.

● Gli atteggiamenti alimentano gli atti. Il discorso dell’odio è pericoloso anche perché può condurre a più gravi violazioni dei diritti umani, e perfino alla violenza fisica. Può contribuire a inasprire le tensioni razziali e altre forme di discriminazione e di violenza.

● L’odio online non è solo espresso a parole. Internet ci permette di comunicare rapidamente e in modi svariati, ad esempio, mediante i social media e i giochi online, molto spesso, d’altronde, in maniera anonima. L’odio online può esprimersi sotto forma di video e foto, come pure, più solitamente, di contenuto testuale. Le forme visive o multimediali hanno sovente un impatto più forte sugli atteggiamenti (consci e inconsci).

● L’odio prende di mira sia gli individui che i gruppi. L’odio online può prendere di mira dei gruppi che spesso sono già vulnerabili sotto altri aspetti, come i richiedenti asilo, le minoranze religiose o le persone con disabilità. Tuttavia, anche i singoli individui sono sempre maggiormente oggetto di attacchi. Le conseguenze sono talvolta fatali, come dimostrato da numerosi fatti di cronaca riferiti dai media, riguardanti giovani vittime di cyberbullismo che sono state spinte al suicidio.

● Internet è difficilmente controllabile. La diffusione di messaggi di incitamento all’odio è maggiormente tollerata su Internet rispetto al mondo offline ed è sottoposta a minori controlli. È ugualmente più facile (e comporta meno rischi) insultare o molestare online, perché le persone spesso si esprimono sotto la copertura dell’anonimato.

● Ha radici profonde. Gli atteggiamenti e le tensioni sociali che suscitano sentimenti di

odio online affondano le loro radici nella società, e non sono diversi, in genere, da quelli che alimentano il discorso dell'odio offline.

● Impunità e anonimato. Sono le due presunte caratteristiche delle interazioni sociali in rete: l'impunità e l'anonimato. Queste abbassano le remore etiche. In realtà, però, qualsiasi azione

compiuta sul web consente di rintracciare il suo autore.

Il contenuto e il tono

Certe espressioni di odio sono più estreme, utilizzano termini più offensivi e possono perfino istigare altri ad agire. All'altra estremità della scala, troviamo insulti più moderati o generalizzazioni eccessive, che presentano certi gruppi o individui sotto una cattiva (e perfino sotto falsa) luce.

Il bersaglio i bersagli potenziali

Alcuni gruppi, o individui, possono essere più vulnerabili di altri alle critiche. Può dipendere dal modo in cui sono globalmente considerati nella società, o da come sono rappresentati nei media, oppure dalla situazione personale, che non permette loro di difendersi efficacemente. Il contesto di una particolare espressione di odio è legato talvolta a circostanze storiche e culturali specifiche. Può includere altri fattori, come il mezzo utilizzato e il gruppo preso di mira, le tensioni o i pregiudizi esistenti, l'autorità del suo autore, ecc.

Occorre valorizzare la dimensione relazionale dei più giovani, sensibilizzandoli verso capacità di analisi e discernimento, per fornire strumenti idonei tanto comunicativi quanto educativi sotto l'aspetto civico e morale, in tal modo:

- fornendo agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di "hate speech", in particolare legati al gruppo etnico/religioso, al genere, all'orientamento sessuale, alla disabilità;
- promuovendo la partecipazione civica e l'impegno, anche attraverso i media digitali ed i Social Network;
- favorendo un'espressione consapevole e costruttiva da parte dei giovani.

A tal uopo, Il processo formativo degli alunni sarà implementato con percorsi educativi finalizzati a valorizzare la parità di genere, la diversità vissuta come originalità e identità di ogni persona. Sarà promossa una politica di inclusione estesa a tutta la comunità scolastica, alle famiglie e al il territorio.

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?

L'internet addiction (dipendenza dal web), espressione coniata dallo psichiatra americano Ivan Goldberg nel 1995, è annoverata tra le nuove psicopatologie degli ultimi decenni. La dipendenza dal web è paragonata a quella provocata dagli stupefacenti, sia per le ripercussioni sulle relazioni sociali del soggetto che ne sia affetto, sia per le "crisi" di astinenza che essa può innescare. Una persona viene valutata dipendente dal web se è sopraffatta da una sorta di "subordinazione" nei confronti dell'oggetto. D'altra parte, non è solo l'Internet Addiction, cioè il pericolo diretto , a spaventare, ma anche il rischio di isolamento sociale ad esso connesso. Le testimonianze dei ragazzi che dichiarano di sentirsi sol, nonostante siano sempre connessi in comunicazioni virtuali, sono moltissime. Altra conseguenza derivata dall'Internet Addiction è la confusione tra web e realtà, mentre dovrebbe essere sempre ben chiaro che le azioni virtuali producono sempre conseguenze reali. I "sintomi" della dipendenza dal web possono essere diversi: l'ossessione di essere sempre presenti in Rete, definita over sharing, oppure la sensazione di disagio o di vera e propria ansia provata di fronte all'eventualità di non aver accesso alla Rete (nomofobia) o, ancora, la "mania" di scattare e postare continuamente dei selfie.

Nelle sue forme più gravi l'Internet Addiction viene trattata al pari delle altre dipendenze patologiche, come quelle da droghe o da alcol.

Anche in questo caso, l'Istituto Ruggero II è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul "benessere digitale" (cioè la capacità di creare e mantenere una relazione sana con la tecnologia), e ad attuare una seria riflessione su come rendere gli studenti e le studentesse più consapevoli delle proprie abitudini online, degli atteggiamenti da modificare per creare un ambiente equilibrato tra gioco e gestione della rete.

Esso intende fornire al personale docente, non docente, agli studenti e alle loro famiglie strumenti finalizzati al riconoscimento e alla prevenzione del fenomeno, attraverso la realizzazione delle azioni di seguito indicate:

attività formative rivolte a docenti e discenti;
conferenze di varia natura rivolte a genitori, docenti, studenti, studentesse;
partecipazione ad eventi e incontri con la Polizia Postale;
supporto psicologico e attivazione dello sportello d'ascolto.

4.5 - Sexting

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

Il sexting (abbreviazione di sex – sesso e texting – messaggiare, inviare messaggi) consiste nel girare video oppure scattarsi selfie intimi, senza vestiti o a sfondo sessuale, per poi inviare il file al proprio partner, agli amici, e in chat di gruppo. Si tratta di una pratica attuata dal 6% dei ragazzi tra gli 11 e i 13 anni (il 70% ragazze). Le percentuali aumentano al crescere dell’età: se si considera al fascia 14-19 anni, si sale al 10%.

Oltre ad essere le più esposte per quanto attiene al fenomeno del sexting, le ragazze sono spesso vittime anche del cosiddetto revenge porn (“vendetta pornografica” , Legge 19 luglio 2019 n. 69, art.10): l’ex partner, lasciato o tradito, pubblica per vendetta (all’interno di chat o sui social network) foto o video privati della propria ex al solo scopo di umiliarla.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell’altro e depressione.

Le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica sono:.

- partecipazione ad eventi e incontri con Polizia Postale, la Polizia di Stato, Arma dei Carbinieri, magistrati.;

- formazione degli studenti e delle studentesse sui rischi del sexting legati al revenge porn;

- fornire al personale della scuola gli strumenti finalizzati al riconoscimento e alla prevenzione del fenomeno;

supporto psicologico e attivazione dello sportello d’ascolto.

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.

Potenziali vittime dell'adescamento online possono essere sia bambini che bambine, sia ragazzi che ragazze. Il fenomeno, infatti, non conosce distinzione di genere. Gli adolescenti sono particolarmente vulnerabili, poiché si trovano in una fase della loro vita in cui è molto importante il processo di costruzione dell'identità sessuale. Anche per questo potrebbero essere aperti e curiosi verso nuove esperienze e, talvolta, attratti da relazioni intime e apparentemente rassicuranti. In questa fase è importante, infatti, il bisogno di avere attenzioni esclusive da un'altra persona, di ottenere rinforzi esterni di approvazione per il proprio corpo e la propria immagine. È proprio in ragione della fiducia costruita nella relazione che le vittime di adescamento online riferiscono di sentirsi umiliate, usate, tradite e tendono a sentirsi in colpa e ad autosvalutarsi per essere cadute nella trappola.

La psicologa Rachel O'Connell ha descritto le fasi di questo reato, inserito da qualche anno nel codice penale.

1. La prima fase è definita **friendship forming stage** (cioè la parte in cui si instaura un'amicizia). In questo momento iniziale il groomer o adescatore studia la Rete in

cerca della sua vittima, con la quale cercherà di entrare in confidenza quasi certamente fingendosi qualcun altro.

2. La seconda fase è chiamata **relationship forming stage** (l'amicizia diventa più intensa). Il rapporto si è orami consolidato e l'adulto comincia con le domande sugli sport, sul tipo di vacanza preferito ecc. In questa fase il groomer cerca di accorciare le distanze con la vittima, entra nel suo campo di amicizie e usa il suo linguaggio.
3. Questa fase è chiamata del **risk assesment stage** (cioè della valutazione del

rischio). Il groomer cerca di vagliare, in base al grado di confidenza raggiunto e alle informazioni fornite dal minore, se vale la pena compiere il salto al reale. Ha bisogno di capire se la ragazza o il ragazzo hanno parlato con qualcuno di lui e se il computer è controllato dai genitori.

4. La quarta fase è l'**exclusivity stage** (cioè la fase esclusiva di amicizia). Questo è un ulteriore approfondimento del legame tra abusante e vittima. 5. Infine c'è la **sexual stage** (la fase sessuale), con la richiesta di una video chat o del numero di telefono la trasmissione di foto ambigue.

L'obiettivo finale è chiaramente l'incontro reale, quando il molestatore tenterà di ottenere i favori sessuali della vittima.

È proprio in ragione della fiducia costruita nella relazione che le vittime di adescamento online riferiscono di sentirsi umiliate, usate, tradite e tendono a sentirsi in colpa e ad autosvalutarsi per essere cadute nella trappola.

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).

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.

La nostra scuola ha già realizzato dei progetti sull'affettività, la sessualità e sulle malattie

sessualmente trasmissibili.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per

prevenire ed affrontare la delicata problematica dell'adescamento.

-Fornire al personale docente e non docente, agli studenti, alle studentesse, ai genitori strumenti finalizzati al riconoscimento e alla prevenzione del fenomeno

- Predisporre per gli studenti e le studentesse dei percorsi guidati sull'educazione

all'affettività e alla sessualità, anche attraverso il ricorso a medici e psicoterapeuti.

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.

Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia. L'intento è quello di facilitare il processo di rimozione del materiale stesso dalla Rete e allo stesso tempo consentire le opportune attività investigative finalizzate ad identificare chi possiede quel materiale, chi lo diffonde e chi lo produce, ma, soprattutto e primariamente, ad identificare i minori abusati presenti nelle immagini e video, assicurando la fine di un abuso che potrebbe essere ancora in corso e il supporto necessario.

Parallelamente, per salvaguardare il benessere psicofisico degli alunni coinvolti nella visione di questi contenuti, sarà opportuno ricorrere a un supporto psicologico anche passando per una consultazione presso il medico di base o pediatra di riferimento.

Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza: Consultori Familiari, Servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, etc.

Se si è a conoscenza di tale tipologia di reato è possibile far riferimento alla: Polizia di Stato –

Compartimento di Polizia postale e delle Comunicazioni; Polizia di Stato – Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato – Commissariato online.

Studi in materia dimostrano come l'utilizzo di materiale pedopornografico possa essere propedeutico all'abuso sessuale agito ed è quindi fondamentale, in termini preventivi, intervenire per ridurre l'incidenza di tale possibilità. L'abuso sessuale online rappresenta una particolare declinazione dell'abuso sessuale su bambini/e, ragazzi/e, la cui caratteristica fondante è il ruolo ricoperto dalle tecnologie digitali, le quali diventano il

mezzo principale attraverso cui l'abuso viene perpetrato, documentato e diffuso in Rete con immagini e/o video. Le dinamiche attraverso cui l'abuso sessuale online si manifesta producono effetti sulle vittime che si aggiungono e moltiplicano a quelli associati all'abuso sessuale.

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.

Anche in questo caso, il nostro Istituto si impegna:

a promuovere percorsi di Educazione civica, Educazione all'affettività e alle emozioni, Educazione sessuale;
a sensibilizzare all'uso corretto e consapevole di Internet.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022).

□ 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.

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

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

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

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

□ Promuovere incontri e laboratori per studenti e studentesse dedicati all'

Educazione Civica Digitale.

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

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

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

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

segnalare la presenza di materiale pedopornografico online.

I contenuti da segnalare, considerati “pericolosi” per gli alunni perché scaturenti da un utilizzo non responsabile e non consapevole dei social network, sono tutte quelle azioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o un piccolo gruppo) .

Essi si concretizzano in:

1. contenuti afferenti alla privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà di eventi privati, etc.);

2. contenuti afferenti all’aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti o che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, etc.), la partecipazione a giochi pericolosi quali Blue Whale e Cutting;

3.contenuti afferenti alla sessualità, quali messaggi molesti, conversazioni in chat o vocali che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), etc..

I docenti, chiamati a realizzare azioni preventive del fenomeno di bullismo/cyberbullismo, si impegnano ad essere osservatori attenti, capaci di cogliere e valutare possibili segnali anomali inviati, più o meno consapevolmente, dagli allievi. In quest’ottica, parallelamente all’imprescindibile e capillare azione formativa/informativa che l'Istituto intende promuovere, diventa importante attivare un efficace canale di comunicazione docenti-discenti, ispirato ai principi della fiducia e della stima reciproca.

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.

Il nostro Istituto ha predisposto gli strumenti di segnalazione dei presunti atti di bullismo/cyber bullismo e, in particolare, ha previsto l'attivazione di registri, di moduli e di un apposito indirizzo e-mail per le denunce di situazioni anomale.

È stato anche programmato uno sportello di ascolto presso le sedi dell'IISS Ruggero II che si occuperà di raccogliere tutte le informazioni possibili, anche attraverso colloqui di approfondimento con gli attori coinvolti.

A supporto del Dirigente scolastico e del Referente dell'area bullismo e cyber bullismo, opererà un gruppo di lavoro. La segnalazione del caso potrà essere effettuata dal docente, dallo studente o da altro operatore scolastico, tramite modulo allegato al presente documento (Allegato 2), alla referente, la quale, con il supporto del Gruppo di lavoro per la prevenzione ed il contrasto di tali fenomeni, si occuperà di raccogliere tutte le

informazioni possibili, e di segnalarle al Dirigente. Sarà poi il Dirigente,

insieme al Team, a valutare se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali o se il caso vada gestito all'interno della scuola con il coinvolgimento del Consiglio di Classe e delle famiglie degli alunni coinvolti, alla luce dei Regolamenti di Istituto e di Disciplina degli Studenti. Si sceglierà uno o più interventi da attuare a cui seguirà una fase di monitoraggio. (cfr. schema di procedura di intervento nell'Allegato 3). Le rilevazioni e la gestione dei casi avverranno seguendo i protocolli suggeriti dalla piattaforma messa a disposizione da Generazioni Connesse, come dagli schemi delle procedure riportati al punto 5.4

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.

Attori sul territorio – recapiti utili:

Comitato regionale UNICEF:

comitato.campania@unicef.it
Tel: 081 7147057 - Fax: 081 645895

Ufficio scolastico regionale:

direzione-campania@istruzione.it

Tel:081.5576001- Fax:081-5576569

Polizia Postale e delle Comunicazioni:

sezione di Avellino : Tel: 0825 34103

Aziende sanitarie locali:

Distretto Sanitario 01 – Ariano Irpino

dsarianoirpino@aslavellino.it

Tel: 0825 877665

Garante Regionale per l'Infanzia e l'Adolescenza :

garante.infanzia@cr.campania.it

Numero di Emergenza : 114

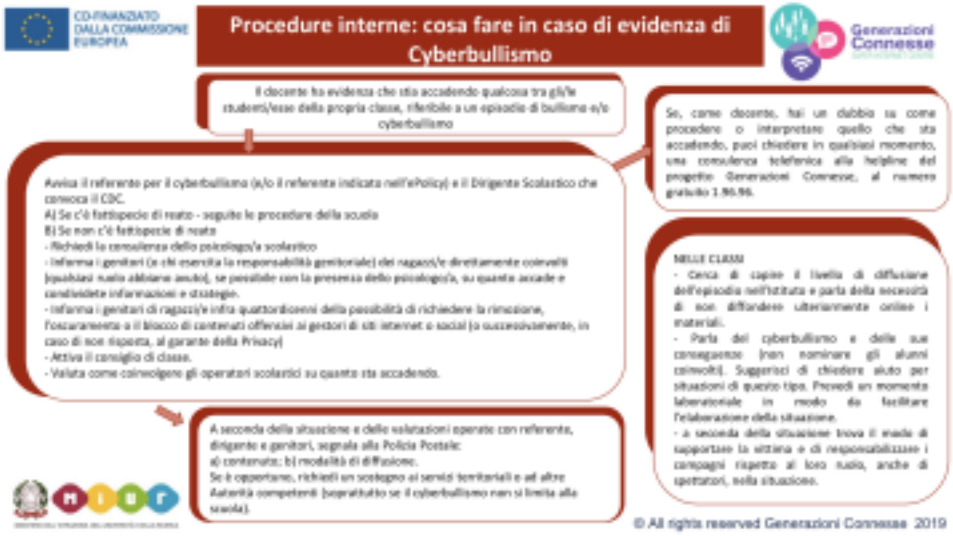
Tribunale per i minorenni di Napoli:

tribmin.napoli@giustizia.it

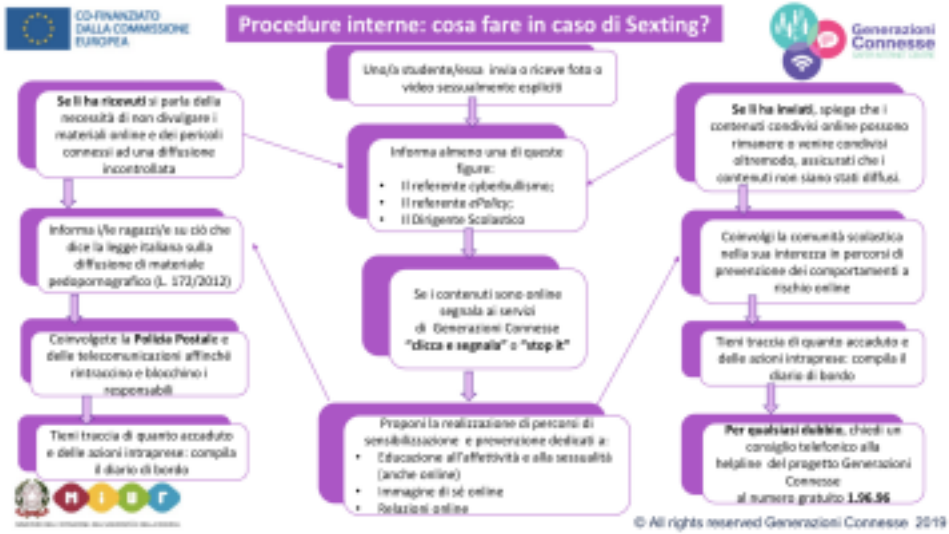
Tel. 081/ 744 9111- Fax: 081/ 741 9132

5.4. - Allegati con le procedure

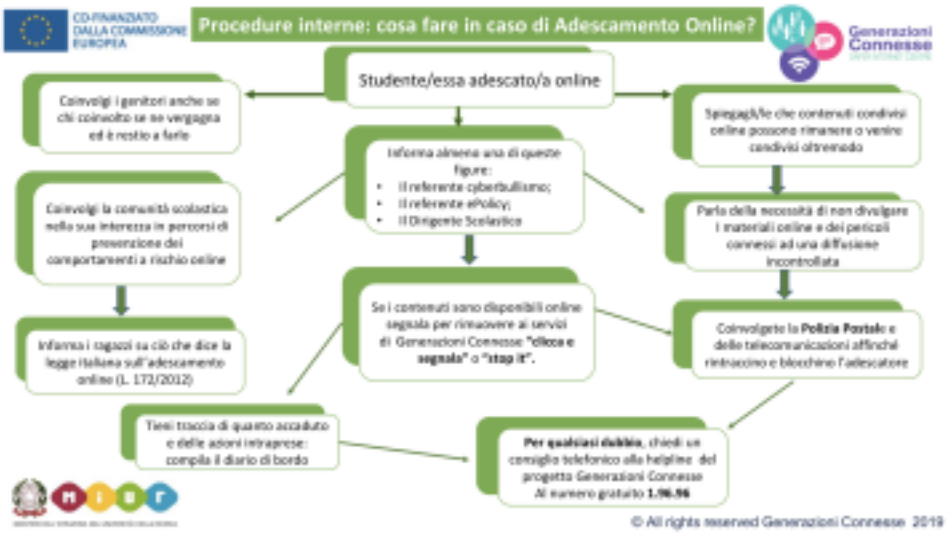
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



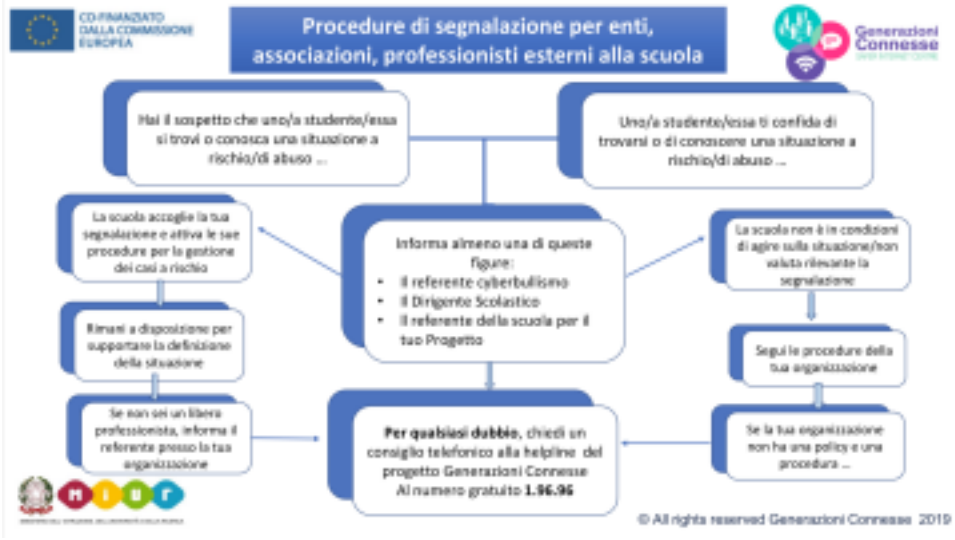
Procedure interne: cosa fare in caso di sexting?



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

Come indicato nei paragrafi precedenti, annualmente si procederà ad interventi di formazione, sensibilizzazione e monitoraggio dei risultati raggunti:

monitoraggio dei comportamenti attraverso la somministrazione di questionari con utilizzo della piattaforma Elisa e realizzazione di report periodici;
realizzazione di progetti di peer education sui temi della sicurezza online.