Documento di ePolicy

VTIC80100T

I.C. " PAOLO RUFFINI "

VIA DEL POGGIO N.30 - 01018 - VALENTANO - VITERBO (VT)

Rosaria Faina

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

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.

Dirigente scolastico

- Individua attraverso il Collegio dei Docenti un referente del bullismo e cyberbullismo;
- costituisce il Team Antibullismo che presiede di cui fanno parte il referente del Bullismo e Cyberbullismo, l'animatore digitale e altre professionalità presenti all'interno della scuola (funzioni di sistema, esperti interni, DSGA, personale ATA, studenti, psicologo, pedagogista operatori socio-sanitari). A supporto dell'azione di prevenzione e contrasto;
- costituisce il Team per l'Emergenza integrato da figure specializzate del Territorio (agenzie educative accreditate, forze dell'ordine, servizi sanitari).
- promuove interventi di prevenzione primaria e per le scuole secondarie sollecita il coinvolgimento attivo degli studenti anche attraverso modalità di Peer Education.
- organizza e coordina i Team Antibullismo e per l'Emergenza per l'avvio delle istruttorie e dei piani intervento nell'ambito della prevenzione primaria universale, secondaria o selettiva e terziaria o indicata come da Allegato 1.A.
- predispone eventuali piani di sorveglianza in funzione delle necessità della scuola.
- tramite il sito web della scuola fornisce e rende pubbliche le seguenti informazioni:
    - nominativo/i del/i referente/i per il bullismo e cyberbullismo
    - formazione del Team Antibullismo;
    - formazione del Team dell'emergenza;
    - contenuti informativi su azioni e attività di contrasto ai fenomeni di bullismo e cyberbullismo (Regolamento d'istituto, PTOF, Patto di corresponsabilità, Epolicy, PDM) oltre che di educazione digitale.

Referente Cyberbullismo d'Istituto

- Promuove la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale;
- coordina le attività di prevenzione ed informazione sulle sanzioni previste e sulle responsabilità di natura civile e penale;
- collabora con gli insegnanti e propone corsi di formazione al collegio dei docenti;
- coadiuva il Dirigente scolastico nella redazione dei piani di Vigilanza attiva ai fini di prevenzione degli episodi di Bullismo e Cyberbullismo;
- monitora i casi e gli episodi segnalati,
- coordina i Team Antibullismo e per l'Emergenza;
- crea alleanze con il Referente Territoriale e regionale;
- promuove le Reti Territoriali (psicologi, forze dell'ordine. Assistenti sociali, pedagogisti ecc. anche con eventuale affiancamento di genitori e studenti);
- cura rapporti di rete fra scuole per eventuali convegni/seminari/corsi e per la giornata mondiale sulla Sicurezza in Internet, la "Safer Internet Day" (6 FEBBRAIO).
- partecipa agli incontri di coordinamento con la governance regionale.

Animatore digitale e Team dell'innovazione

- Promuovono percorsi di formazione interna all'Istituto relativamente alla "scuola digitale", secondo le azioni indicate nel "Piano Nazionale Scuola Digitale" (PNSD) e si attivano per coinvolgere l'intera comunità scolastica e il territorio in iniziative e progetti inerenti le nuove tecnologie;

- propongono la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola.

Collegio docenti

- Promuove scelte didattiche ed educative, anche in collaborazione con altre scuole in rete, per la prevenzione del fenomeno;
- promuove azioni di sensibilizzazione dei fenomeni del bullismo e cyberbullismo nel territorio in rete con enti, associazioni, istituzioni locali ed altre scuole, coinvolgendo alunni, docenti, genitori ed esperti;
- prevede azioni culturali ed educative rivolte agli studenti, per acquisire le competenze necessarie all'esercizio di una cittadinanza digitale consapevole.

Consiglio di classe

- Favorisce un clima collaborativo all'interno della classe e nelle relazioni con le famiglie;
- propone progetti di educazione alla legalità e alla cittadinanza attiva.

Docente

- Vigila sulla serenità e la correttezza delle relazioni tra compagni di classe;
- vigila sul corretto uso delle TIC da parte degli alunni;
- segnala tempestivamente casi sospetti di bullismo e cyberbullismo al Dirigente Scolastico o al Referente del bullismo e cyberbullismo e al Consigli di Classe;
- utilizza le tecnologie nel rispetto delle regole e della legalità;

Direttore dei Servizi Generali e Amministrativi

- Assicura, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione necessari ad evitare un cattivo funzionamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate.

Personale Amministrativo, Tecnico e Ausiliario (ATA)

- Vigila sulla sicurezza nei locali scolastici (corridoi, androni, piazzali, bagni all'esterno delle classi)
- segnala tempestivamente atteggiamenti sospetti di bullismo e cyberbullismo ai docenti, al Dirigente Scolastico o al Referente del bullismo e cyberbullismo;
- collabora nelle attività di prevenzione e contrasto con la governance di Istituto.

Genitori

- Partecipano attivamente alle azioni di formazione/informazione, istituite dalle scuole, sui comportamenti sintomatici del bullismo e del cyberbullismo;
- sono attenti ai comportamenti dei propri figli;
- vigilano sull'uso delle tecnologie da parte dei ragazzi, con particolare attenzione ai tempi, alle modalità, agli atteggiamenti conseguenti.

Alunni

- Sono coinvolti nella progettazione e nella realizzazione delle iniziative scolastiche al fine di favorire un miglioramento del clima relazionale;
- imparano le regole basilari alle quali attenersi quando sono connessi alla rete, facendo attenzione alle comunicazioni (email, sms, whatsapp) che inviano.
- sono inoltre invitati a contattare i propri docenti ed il Referente quando vengono a conoscenza di casi di bullismo o cyberbullismo.

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).

Nel nostro istituto le organizzazioni/associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve o/e lungo periodo, dovranno prendere atto di quanto stilato nell' ePolicy del nostro istituto e sottoscrivere un'informativa sintetica del documento in questione per la parte di loro interesse, presente nel contratto.

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.

1.5 - Gestione delle infrazioni alla ePolicy

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

Disciplina degli alunni sull'uso delle TIC a scuola

- DIVIETO ACQUISIZIONE IMMAGINI

Non è consentito, durante le attività didattiche o comunque all'interno della scuola, acquisire – mediante telefonini cellulari o altri dispositivi elettronici - immagini, filmati o registrazioni vocali, se non per finalità didattiche e previo consenso del docente e delle persone filmate. La divulgazione del materiale acquisito all'interno dell'istituto è possibile per fini esclusivamente di studio o documentazione, e comunque nel rispetto del diritto alla riservatezza di tutti.

- USO DISPOSITIVI ELETTRONICI

Durante le lezioni o le attività didattiche in genere non si possono usare cellulari, giochi elettronici e riproduttori di musica, se non per finalità didattiche, previo consenso del docente.

- IMMAGINI DESKTOP

È vietato modificare le immagini sul desktop dei computer della scuola (pc di classe o dei laboratori multimediali) inserendo immagini dai contenuti offensivi, ingiuriosi e lesivi della dignità;

- Sono vietati tutti quei comportamenti nell'uso delle TIC che abbiano un contenuto offensivo e che ledano il rispetto e la dignità personale.

Mancanze disciplinari

Sono da considerarsi tipologie persecutorie qualificate come Bullismo:

- la violenza fisica, psicologica o l'intimidazione del gruppo, specie se reiterata;
- l'intenzione di nuocere;
- l'isolamento della vittima.

Rientrano nel Cyberbullismo:

- Flaming: litigi on line nei quali si fa uso di un linguaggio violento e volgare.
- Harassment: molestie attuate attraverso l'invio ripetuto di linguaggi offensivi.
- Cyberstalking: invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità.
- Denigrazione: pubblicazione all'interno di comunità virtuali (newsgroup, blog, forum di discussione, gruppi di messaggistica immediata, siti internet) di pettegolezzi e commenti crudeli, calunniosi e denigratori.
- Outing estorto: registrazione delle confidenze raccolte all'interno di un ambiente privato e in un clima di fiducia poi inserite integralmente in un blog pubblico.
- Impersonificazione: insinuazione all'interno dell'account di un'altra persona con l'obiettivo di inviare dal medesimo messaggi ingiuriosi che screditino la vittima.
- Esclusione: estromissione intenzionale dall'attività on line.
- Ulteriori comportamenti rientranti nelle fattispecie previste dalla Legge 71/2017.

Tipologie di intervento e sanzioni disciplinari

Per le tipologie di intervento si fa riferimento all'allegato 1.A, parte integrante del Regolamento di Istituto.

I comportamenti sopra elencati, opportunamente accertati, che si configurino come forme di bullismo e cyberbullismo verranno considerati mancanze gravi e conseguentemente sanzionati sulla base di quanto previsto nel Regolamento d'istituto. Quando possibile, saranno privilegiate le sanzioni disciplinari di tipo riparativo, convertibili in attività a favore della comunità scolastica. Vista l'imprevedibilità e la complessità del fenomeno che rende difficile regolamentare le misure di contrasto e di intervento per tutte le eventuali casistiche, la scuola, attraverso il Team dell'emergenza/antibullismo sulla base di uno studio del caso, in accordo con il consiglio di classe, individua azioni di contrasto e di intervento "indicato/selettivo".

Disciplina del personale scolastico

Le possibili infrazioni del personale docente sono così di seguito schematizzate:

- utilizzo delle tecnologie della scuola, d'uso comune con gli alunni, non connesso alle attività d'insegnamento o al profilo professionale;
- violazione della privacy nel trattamento dei dati personali degli alunni;
- diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- mancata segnalazione di situazioni critiche rispetto alla e-Policy d'istituto.

L'infrazione della presente e-Policy da parte del personale (docente, ATA) può costituire elemento di contestazione d'addebito disciplinare e per gli esterni (esperti, collaboratori, etc.) può essere causa di risoluzione di eventuali contratti e/o convenzioni in essere.

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.

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.

La revisione, l'aggiornamento e l'implementazione dell'e-Policy saranno a carico del

gruppo di lavoro che ha redatto il documento e poi discussi con il personale docente.

Il nostro piano d'azioni

Azioni da sviluppare nell'arco di tre anni:

- Organizzare un evento o un’attività volti a presentare il progetto dell’ePolicy a docenti, studenti o genitori (presentazione in sede di Collegio Docenti, pubblicazione sul sito della scuola, informativa da dare alle famiglie...).

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.

L'Istituto Comprensivo "Paolo Ruffini" ha elaborato nell'anno scolastico 2016-2017 un curricolo per competenze in cui è presente la competenza digitale, ritenuta dall'Unione Europea chiave e trasversale alle discipline previste dalle Indicazioni Nazionali, per la sua importanza e diffusione nel mondo d'oggi. Possedere una competenza digitale significa padroneggiare le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con "autonomia e responsabilità", con spirito critico, nel rispetto degli altri e sapendone prevenire ed evitare i pericoli. In questo senso, tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione. Nel curricolo per le competenze sono specificati descrittori, livelli di padronanza e modalità valutative. Il nostro istituto, inoltre, si è dotato nell'anno scolastico 2020-2021 di un curricolo di Educazione Civica previsto dalla legge n. 92 del 2019 e dalle Linee guida del 20 agosto 2019 in cui è contemplata la Cittadinanza digitale, ritenuta trasversale alle discipline. A partire dall'a.s. 2020/2021 l'istituto ha anche aderito al progetto ministeriale "Programma il futuro" coinvolgendo molte classi dei vari ordini nella

sperimentazione del coding (Code Week e l'Ora del codice), integrando così le competenze digitali già previste dalle Indicazioni Nazionali, attraverso la promozione dello sviluppo del “pensiero computazionale” negli alunni.

La scuola, per implementare le competenze digitali degli studenti, ha adottato la piattaforma Google Workspace, fornendo le credenziali di accesso e le procedure per attivare e utilizzare gli account personali.

Il nostro istituto prevede, inoltre, il conseguimento della certificazione Eipass Junior per gli studenti e le studentesse della scuola secondaria di primo grado di Valentano e Marta.

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 studenti e 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. Il percorso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica è un processo permanente, che deve prevedere anche momenti di autoaggiornamento, di formazione personale o collettiva. Pertanto l’istituto riconosce e favorisce la partecipazione del personale sia ad iniziative promosse direttamente dalla scuola, dalle reti di scuole e dall’amministrazione, sia quelle liberamente scelte dai docenti (anche online) sulle TIC e si impegna a organizzare momenti di formazione sui metodi e sugli strumenti della didattica digitale. L’istituto ha aderito alle attività formative nell’ambito del PNSD rivolte all’animatore digitale e al team per l’innovazione. I docenti hanno svolto anche i corsi di formazione promossi dal polo formativo dell’Ambito 27 sull’uso delle TIC.

Il Team dell'Innovazione Digitale ha creato anche un sito per i docenti dell’istituto con

la predisposizione di aree dedicate alla condivisione di materiali e di iniziative formative sulle TIC e il PNSD.

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

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

L'Istituto Comprensivo si avvale della figura dell'Animatore Digitale che, con il Dirigente Scolastico e il D.S.G.A., collabora per raggiungere gli obiettivi di innovazione del PNSD nella scuola.Inoltre, a partire dall'anno scolastico 2017-2018, è attiva la figura del Referente d'istituto per le attività di prevenzione e contrasto al bullismo e al cyberbullismo (L.107/2015). La formazione sull'utilizzo consapevole e sicuro delle TIC è stata estesa ad altre figure, in funzione della costituzione di un Team. Si rende, comunque, necessaria la formazione di tutti i docenti sull'uso consapevole e sicuro di Internet e sui rischi della rete.

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.

In considerazione dell'importanza di favorire la sinergia degli interventi educativi di scuola e famiglia, il presente documento è a disposizione dei genitori sul sito web istituzionale, per consentire agli stessi una piena conoscenza delle regole relative all'utilizzo delle nuove tecnologie all'interno dell'istituto e favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso inappropriato del digitale.

Allo scopo di mantenere viva l'attenzione delle famiglie si darà maggiore risalto alla sezione del sito istituzionale dell'istituto dedicata a Generazioni Connesse. Il nostro Istituto Comprensivo ha già organizzato incontri aperti alle famiglie e agli studenti con enti esterni, come la Polizia Postale, per sensibilizzare docenti, alunni e genitori sui temi della sicurezza online. Anche nei prossimi anni si continuerà ad utilizzare questo approccio per la sensibilizzazione delle famiglie, con incontri che offriranno occasione di confronto e discussione sui rischi rappresentati dall'uso inappropriato dei dispositivi digitali.

Tutte le precedenti azioni vengono attuate in continuità anche con l'art. 5 (comma 2) della legge 29 maggio 2017, n.71 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" che prevede l'integrazione, oltre che del regolamento scolastico, anche del "Patto di Corresponsabilità", con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari "commisurate alla gravità degli atti compiuti", al fine di regolamentare l'insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione al fenomeno.

Il nostro piano d'azioni

Azioni da sviluppare nell'arco di tre anni

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

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

Il personale scolastico è "autorizzato al trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni necessarie ai fini dello svolgimento della propria funzione. Tutto il personale incaricato riceve istruzioni particolareggiate applicabili al trattamento degli stessi ed una formazione specifica dal Responsabile della Protezione dei dati (DPO). I dati personali sono protetti secondo la normativa vigente; in occasione di eventi o partecipazione a concorsi ai genitori viene richiesta dagli enti organizzatori, responsabili del trattamento dei dati, specifica autorizzazione per l'utilizzo di foto, video, audio per la documentazione di attività che coinvolgono gli alunni. La pubblicazione sul sito della scuola o sui canali social dell'istituto delle attività didattiche avviene nell'occultamento di immagini e dati che rivelino l'identità degli alunni.

La scuola non si impegna solo a tutelare la privacy degli alunni e delle loro famiglie, ma anche ad informare e rendere consapevoli gli stessi di quanto sia importante il diritto alla riservatezza.

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.

Il nostro istituto possiede un regolamento specifico che disciplina l'uso dei laboratori informatici presenti nei vari plessi.

La rete wi-fi è protetta da password in possesso esclusivo dei docenti che utilizzano quotidianamente i computer all'interno delle classi.

Le impostazioni dei computer presenti nei laboratori e nelle aule sono definite e gestite dai responsabili degli stessi, i quali segnalano eventuali malfunzionamenti e disservizi.

L'accesso ad Internet attraverso i dispositivi della scuola da parte degli studenti avviene solo in presenza dell'insegnante, il quale è responsabile del comportamento degli alunni, delle macchine e del software che utilizzano. I docenti lasciano traccia del proprio accesso al laboratorio informatico, scrivendo su un registro la data e l’orario di utilizzo.

A scuola gli studenti si impegnano a:

- utilizzare la rete nel modo corretto
- rispettare le consegne dei docenti
- non scaricare materiali e software senza autorizzazione
- non utilizzare unità rimovibili personali senza autorizzazione
- tenere spento lo smartphone e/o ogni altro apparato multimediale personale
- segnalare immediatamente materiali inadeguati ai propri insegnanti

I docenti si impegnano a:

- utilizzare la rete nel modo corretto

- a visionare preventivamente siti e contenuti reperibili sul web per l'uso didattico
- formare gli studenti all'uso della rete
- dare consegne chiare e definire gli obiettivi delle attività
- monitorare l'uso che gli studenti fanno delle tecnologie a scuola
- non memorizzare le password nei dispositivi scolastici

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.

Sito web

Il sito Web dell'istituto è raggiungibile all'indirizzo https://www.icvalentano.edu.it/. Sul sito della scuola è possibile trovare il Regolamento d'istituto, avvisi ai genitori, modulistica, pubblicizzazione di eventi, pulsanti attivi che permettono l'accesso a link di interesse (registro elettronico, Generazioni Connesse, EIPASS, Iscrizioni On line, PNSD...).

La scuola, in qualità di ente pubblico, pubblica sul proprio sito web i contenuti valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative.

E-mail

L'account di posta elettronica è quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. Tutti i docenti dell'Istituto e gli alunni possiedono un account generato dalla scuola del tipo nomecognome@ruffini.network , per consentire l'accesso alle applicazioni per la didattica digitale integrata sulla piattaforma Google Workspace for Education. Gli alunni e i genitori sono consapevoli che, nel momento in cui ricevono le credenziali dell'account di posta elettronica, i servizi offerti sono esclusivamente per utilizzo scolastico e didattico.

Registro elettronico

Tutto il personale della scuola e tutti i genitori hanno accesso al registro elettronico tramite un sistema di autenticazione. Attraverso il registro elettronico i docenti comunicano ai genitori le attività svolte, i compiti assegnati, le valutazioni e gestiscono gli appuntamenti per i colloqui. Nella bacheca di classe del registro elettronico sono pubblicati gli esiti finali.

Social network

Dallo scorso anno, come previsto dal progetto “Safer Internet Stories” promosso da MIUR, l’istituto ha creato degli account social Instagram e Twitter. Tutti i contenuti sono pubblicati direttamente e sotto la supervisione dell’Animatore digitale e/o di un membro del Team per l’innovazione digitale, che ne valuta con il Dirigente Scolastico la sicurezza e l’adeguatezza sotto i diversi profili dell’accessibilità, della pertinenza dei contenuti, del rispetto della privacy. I social network utilizzati hanno il solo scopo di trasmettere all’esterno l’identità, i valori, le azioni, i progetti e l’idea di educazione che l’istituto porta avanti.

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.

Come da Regolamento d’Istituto (Art. 23) agli alunni è fatto assoluto divieto di usare all’interno della scuola, se non per scopi esclusivamente didattici autorizzati dal docente, smartphone e/o ogni altro apparato multimediale personale. Il divieto non si applica soltanto all’orario delle lezioni ma all’intera permanenza dell’alunno nella struttura scolastica (intervalli, pausa).

I docenti, ad integrazione di quelli scolastici disponibili, possono utilizzare i dispositivi personali per realizzare tutte le attività connesse alla funzione docente. L'uso delle TIC a scuola è definito anche nella sezione 3 del Regolamento di istituto sul bullismo/ cyberbullismo.

Il nostro piano d'azioni

Azioni da sviluppare nell'arco di tre anni

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, docenti e genitori con l'eventuale coinvolgimento di esperti.

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

4.2 - Cyberbullismo: che cos'è e come prevenirlo

La legge 71/2017 “Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo”, nell’art. 1, comma 2, definisce il cyberbullismo:

“qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d’identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo”.

La stessa legge e le relative **Linee di orientamento per la prevenzione e il contrasto del cyberbullismo** indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
    - Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
    - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d’istituto), atti e documenti (PTOF, PdM, Rav).

Definizione del fenomeno

Il cyberbullismo è una forma di prepotenza virtuale messa in atto attraverso l’uso di Internet e delle tecnologie digitali. Spesso i termini bullismo e cyberbullismo vengono usati impropriamente e si riconducono ad essi i più svariati episodi di violenza o offese fra ragazzi/e. Bullismo e cyberbullismo hanno, però, connotati ben precisi e non vanno confusi con altre problematiche del mondo giovanile.

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.

La convinzione dell'anonimato: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile. 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'assenza di confini spaziali: il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio. Spegnere il cellulare o il computer non basta, così come cancellare tutti i propri profili social.

L'assenza di limiti temporali: può avvenire a ogni ora del giorno e della notte.

L'indebolimento dell'empatia: quando le interazioni avvengono prevalentemente online la funzione speciale dei neuroni a specchio, alla base dell'empatia, viene

Il feedback non tangibile: l'impossibilità di vedere con i propri occhi l'eventuale sofferenza e umiliazione provata dalla vittima fa sì che il tutto venga percepito dal cyberbullo come "uno scherzo" divertente a cui partecipare, di cui ridere o a cui essere indifferenti.

Azioni di prevenzione

A seconda dei casi, si potranno adottare le seguenti azioni di prevenzione:

- Prevenzione Universale

Un programma di questo tipo parte dal presupposto che tutti gli studenti siano potenzialmente a rischio. Si tratta quindi di interventi diretti al grande pubblico o a un intero gruppo di una popolazione che non è stato identificato sulla base del rischio individuale.

- Prevenzione Selettiva

Un programma dedicato ad un gruppo di studenti in cui il rischio online è presente. In questo caso la presenza del rischio è stata individuata tramite precedenti indagini, segnalazioni fatte dalla scuola, oppure dalla conoscenza della presenza di fattori di rischio in quel determinato territorio. In questi casi gli interventi sono mirati e prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem solving.

- Prevenzione Indicata.

Un programma di intervento sul caso specifico è pensato e strutturato per adattarsi

agli/lle studenti/studentesse con l'obiettivo di ridurre i comportamenti problematici, oppure dare supporto alle vittime. Per la sua natura questo tipo di intervento si avvale di professionalità diverse perché spesso affronta problemi legati alla salute mentale del minore per cui è opportuno coinvolgere anche la famiglia del/lla ragazzo/a.

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

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

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

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

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

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

Nell'istituto saranno realizzate, quindi, attività finalizzate soprattutto a:
• fornire agli studenti gli strumenti necessari per decostruire gli stereotipi;
• promuovere la partecipazione civica e l'impegno;
• favorire a tutte le età l'uso di un linguaggio consapevole, rispettoso e empatico da parte degli alunni.

L'istituto si potrà avvalere di consulenti/esperti esterni per organizzare incontri formativi rivolti a docenti, genitori ed alunni (Carabinieri, Polizia Postale, equipe Formazione Territoriale del MIUR, associazioni del Territorio preposte allo scopo...).

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?

Tale dipendenza, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica, che deve attenzionare il fenomeno e fornire gli strumenti agli studenti e alle studentesse affinché questi siano consapevoli dei rischi che comporta l'iperconnessione.

L'istituto si propone di promuovere un uso maggiormente consapevole delle tecnologie per favorire il "benessere digitale", ossia la capacità di creare e mantenere una relazione sana con la tecnologia.

Se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi. È importante non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli studenti e delle studentesse, strutturando chiare e semplici regole condivise.

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.

L'istituto promuove azioni:

- verso i genitori: informazione circa le possibilità di attivare forme di controllo

parentale della navigazione;
- verso gli studenti: inserimento nel curricolo di temi legati all'affettività, alla sessualità e alle differenze di genere.

In casi di sexting, se l'entità è lieve, occorre in primo luogo parlarne con alunne e alunni e rispettivi genitori, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Manca spesso la consapevolezza, tra ragazzi e adulti, che una foto o un video diffusi in rete divengono di pubblico dominio e la diffusione non è controllabile. In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico.

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.

Al fine di prevenire casi di adescamento online è opportuno accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò contribuisce a renderli emotivamente più sicuri e pronti ad affrontare eventuali situazioni a rischio.

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 (Polizia di Stato, Polizia postale e Arma dei Carabinieri). L’intento è quello di facilitare il processo di rimozione del materiale stesso dalla Rete e allo stesso tempo consentire le opportune attività investigative. Parallelamente, per salvaguardare il benessere psicofisico degli alunni coinvolti nella visione di questi contenuti, sarà opportuno ricorrere a un supporto psicologico.

Il nostro piano d'azioni

Azioni da sviluppare nell'arco di tre anni

- Prosecuzione della formazione sul bullismo/ cyberbullismo sulla piattaforma Elisa, rivolta ai membri del Team emergenza/ antibullismo.

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 minori potrebbero riferire all'insegnante fatti o eventi personali o altrui, accaduti anche al di fuori della scuola, che potrebbero mettere in allarme il docente. Pertanto sono da considerare degni di segnalazione:

- contenuti afferenti alla violazione della 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, ecc.);

- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);

- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) 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), ecc.

5.2. - Come segnalare: quali strumenti e a chi

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

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

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

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

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

Strumenti a disposizione di studenti/esse

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

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

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

Per quanto riguarda la gestione dei casi, il nostro istituto ha individuato una figura referente per il cyberbullismo. Il caso sarà segnalato, oralmente o via mail, dallo studente oppure dal genitore o dal docente. Se la segnalazione sarà fatta per iscritto, si potrà utilizzare il modulo allegato al presente documento (Allegato 2). La segnalazione sarà alla Referente, la quale, insieme al Team Antibullismo, si occuperà di raccogliere tutte le informazioni possibili, anche attraverso colloqui di approfondimento con gli attori coinvolti e di segnalare l'accaduto al Dirigente scolastico. Sarà poi il Dirigente, insieme al Team Antibullismo, 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 interessati. Si sceglierà uno o più interventi da attuare a cui seguirà una fase di monitoraggio (cfr. schema di procedura di intervento nell'Allegato 3).

5.3. - Gli attori sul territorio

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

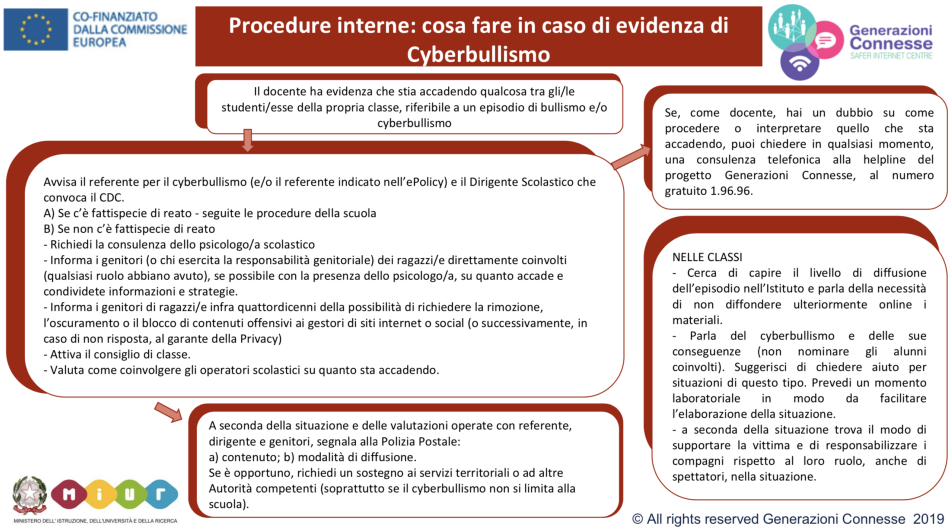
Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse “Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all’utilizzo delle tecnologie digitali da parte dei più giovani” (seconda parte, pag. 31), senza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

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

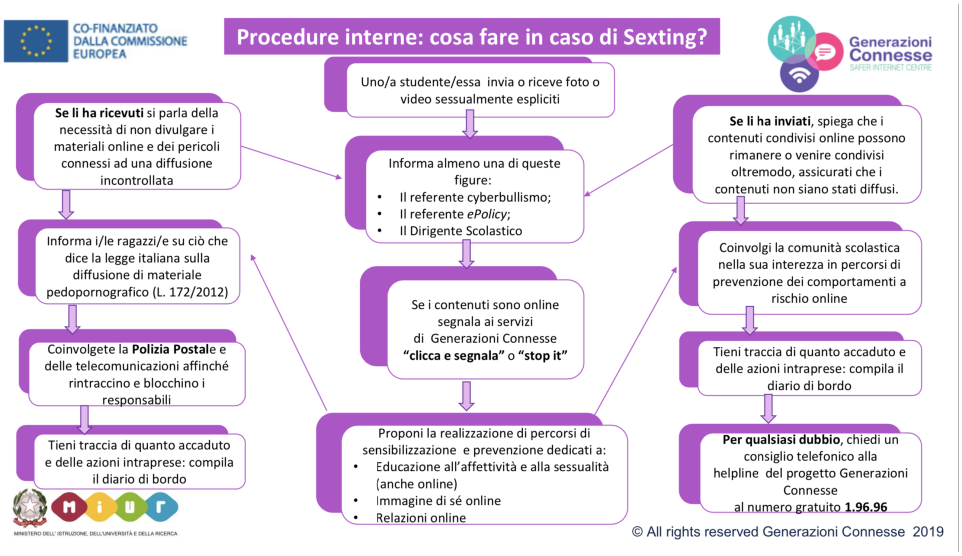
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell’infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

5.4. - Allegati con le procedure

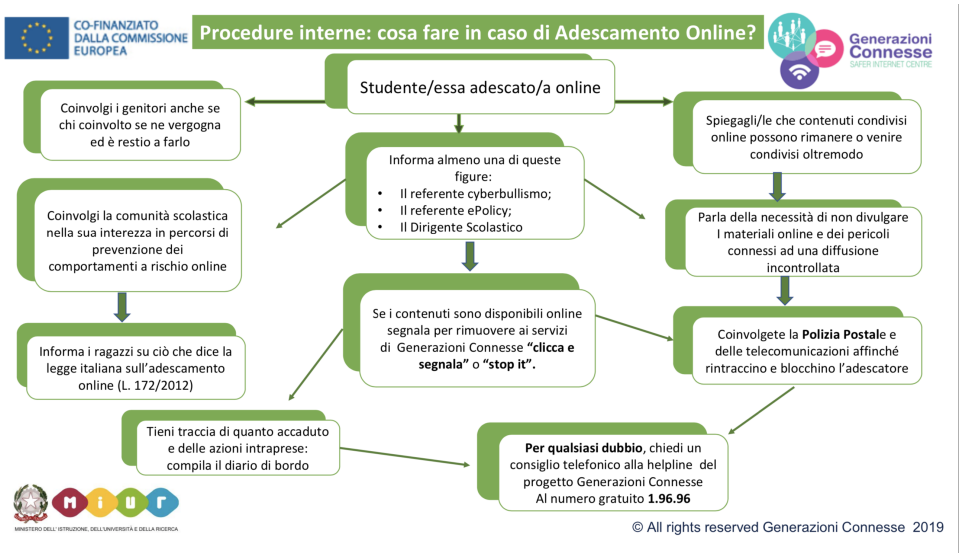
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



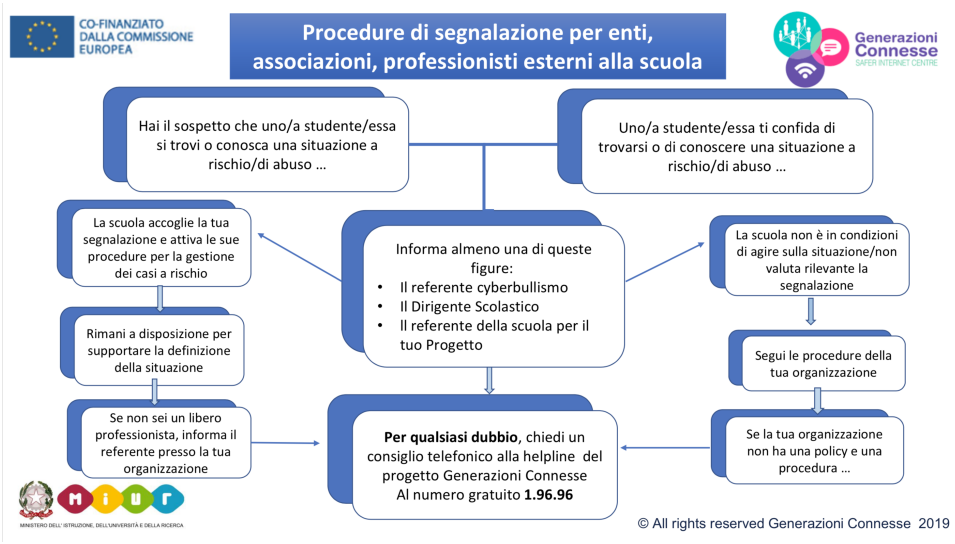
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il nostro piano d'azioni

Non è prevista nessuna azione.