Documento di ePolicy

MIIC8D9008

I.C.S. BONVESIN DE LA RIVA

VIA BONVESIN DE LA RIVA 1 - 20025 - LEGNANO - MILANO (MI)

Elena Osnaghi

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. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
    4. Gestione delle infrazioni alla ePolicy
    5. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
    6. Integrazione dell'ePolicy con regolamenti esistenti
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

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 scuola elabora questo documento seguendo le indicazioni delle LINEE DI' ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo e cyberbullismo elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con "Generazioni Connesse" e il Safer Internet Center per l'Italia.

L'obiettivo è quello di educare e sensibilizzare gli adolescenti, gli insegnanti e i genitori all'uso sicuro e consapevole di internet. Si tiene in considerazione il fatto che il curricolo scolastico prevede che gli studenti imparino a trovare materiale, recuperare documenti e scambiare informazioni utilizzando le TIC. Internet, d'altra parte, offre sia agli studenti che agli insegnanti una vasta scelta di risorse diverse e opportunità di scambi culturali con gli studenti di altri paesi. Gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività on-line, di stabilire obiettivi chiari per un uso responsabile di internet. L'obiettivo principale resta quello di arricchire ed

ampliare le attività didattiche, secondo quanto prevede il curricolo scolastico, l'età e la maturità degli studenti.

Questo documento ha lo scopo di descrivere la linea di condotta della scuola secondaria di 1° grado " **Bonvesin de la Riva**" di Legnano nei confronti dell'utilizzo delle tecnologie dell'informazione e della comunicazione (TIC) nella didattica, nonchè di educare e sensibilzzare gli adolescenti, i docenti e i genitori all'uso consapevole di internet.

Negli ultimi anni la scuola ha cercato di dotarsi di strumenti tecnologici su approvazione dei progetti didattici e di favorire la formazione del personale per far crescere le competenze professionali specifiche nell'impiego delle nuove tecnologie. A tal fine è stato stilato un Regolamento per l'utilizzo e il corretto funzionamento delle aule e delle postazioni informatiche, tramite l'indicazione di prassi opportune e l'invito ad un uso sempre più professionale da parte di tutto il personale. Le apparecchiature presenti nella Scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto. Gli insegnanti sono responsabili delle TIC nell'ambito dell'attività didattica e hanno il compito di responsabilizzare gli alunni per divenire consapevoli dell'importanza della salvaguardia di un bene comune, seguendo le corrette norme di utilizzo.

Grazie ad un percorso guidato e al materiale di supporto messo a disposizione sul sito del progetto www.generazioniconnesse.it si definiscono le misure che l'Istituto intende adottare.

Nello specifico il documento è uno strumento fondamentale che permette di:

- riflettere sul proprio approccio alle tematiche legate alla sicurezza online e all'integrazione delle tecnologie digitali nella didattica;
- usufruire di strumenti e materiali per giungere alla realizzazione di progetti personalizzati;
- coinvolgere l'intera Comunità Scolastica.

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.

Nell'ambito di questa E-Policy sono individuati i seguenti ruoli e le principali responsabilità correlate:

Il Dirigente scolastico ha il compito di:

- garantire la sicurezza di tutti i membri della comunità scolastica (tra cui la sicurezza online);
- garantire che tutti gli insegnanti ricevano una formazione adeguata per un utilizzo positivo e responsabile delle TIC;
- garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza online;

- comprendere e seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.

Il Referente per il cyberbullismo (legge 71-2017) e l'animatore digitale hanno il compito di:

- stimolare la formazione del personale sui temi del PNSD (Piano Nazionale Scuola Digitale) e fornire consulenza al personale della scuola, agli alunni e alle loro famiglie in relazione ai rischi online e alle misure di prevenzione e gestione degli stessi;
- individuare soluzioni metodologiche, tecnologiche, innovative e sostenibili da diffondere nella scuola;
- coinvolgere il più possibile tutta la comunità scolastica nella partecipazione ad attività e progetti attinenti il PNSD.

Il docente ha il compito di:

- formarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- controllare l'uso delle tecnologie digitali (audio/video, dispositivi mobili) da parte degli alunni durante le lezioni;
- guidare le ricerche degli alunni su Internet;
- segnalare all'Animatore Digitale qualsiasi problema di carattere tecnico-organizzativo;
- segnalare al Dirigente Scolastico e ai genitori qualsiasi abuso rilevato a scuola riguardante gli alunni in relazione all'utilizzo delle tecnologie digitali o di Internet, per l'adozione delle procedure previste dalle norme.

L'alunno ha il compito di:

- essere responsabile nell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- comprendere l'importanza di adottare buone pratiche di sicurezza online quando si utilizzano le tecnologie digitali per non correre rischi;
- adottare condotte rispettose degli altri anche quando si comunica in Rete (Netiquette).

Il genitore ha il compito di:

- sostenere la linea di condotta adottata dalla scuola nei confronti dell'utilizzo delle Tic nella didiattica;
- concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso di internet;
- fissare delle regole generali per l'utilizzo del computer, degli altri strumenti digitali quali smartphone, tablet.

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).

Allo scopo di condividere regole comuni per l'utilizzo sicuro di Internet sia a casa che a scuola, si invitano tutti i genitori a prestare la massima attenzione ai principi e alle regole contenute nel presente documento. Si richiede che ogni genitore e/o tutore si impegni a farle rispettare ai propri figli anche in ambito domestico, primariamente assistendo i minori nel momento dell'utilizzo della rete e poi ponendo in atto tutti i sistemi di sicurezza che aiutino a diminuire il rischio di imbattersi in materiale indesiderato.

La scuola promuove eventi e/o dibattiti informativi e formativi, in momenti diversi dell'anno, rivolti a tutto il personale, agli alunni e ai loro genitori, con il coinvolgimento di esperti, sui temi oggetto di codesto Documento.Tra le misure di prevenzione che la scuola mette in atto ci sono, inoltre, azioni finalizzate a promuovere una cultura dell'inclusione, del rispetto dell'altro e delle differenze così che l'utilizzo di Internet e dei cellulari oltre che collocarci all'interno di un sistema di relazioni, ci renda consapevoli di gestire con un certo grado di trasparenza i rapporti che si sviluppano in tale ambiente, giungendo a riconoscere e gestire le proprie emozioni.
Al fine di rendere l'ePolicy uno strumento efficace per la tutela degli studenti e delle studentesse, intesa in senso ampio, è utile condividere le regole per un uso consapevole di Internet anche con le organizzazioni/associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative,

È importante garantire che tutti i soggetti esterni che erogano attività in ambito scolastico siano sensibilizzati e resi consapevoli dei rischi online che possono correre gli studenti e le studentesse e dei comportamenti corretti che devono adottare a scuola.

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.

Il documento verrà condiviso e comunicato agli alunni, a tutto il personale della scuola e ai genitori. Le regole relative all'accesso ad Internet vengono approvate dal Collegio dei Docenti e pubblicate sul sito istituzionale. Gli alunni saranno istruiti riguardo l'uso responsabile e sicuro di internet e saranno informati che per l'utilizzo della Rete a scuola e di ogni altro dispositivo digitale gli insegnanti ne autorizzeranno e controlleranno l'uso.

Il personale della scuola sarà informato/formato sulla politica della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet tramite il presente documento, materiale informativo, incontri e riunioni istituzionali (consigli di interclasse/intersezione, collegio dei docenti). Il personale docente sarà informato del fatto che l'utilizzo di internet attraverso le infrastrutture scolastiche (di tipo hardware e software) sarà monitorato e si potrà risalire al singolo utente registrato. I genitori degli alunni saranno informati/formati sulla politica della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet tramite il presente documento, materiale informativo e incontri di vario genere (assemblee, seminari, riunioni scuola-famiglia).

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.

In relazione a quanto specificato in questa policy, e in modo particolare nella definizione dei ruoli e delle responsabilità, le infrazioni saranno gestite in modo graduale rispetto alla gravità.

Le violazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali e di internet per fini didattici sono le seguenti:

• condivisione di immagini intime o “contrarie al decoro”;

. • comunicazione incauta e senza permesso con sconosciuti;

. • collegamento a siti web non indicati dai docenti;

. • diffusione impropria (con o senza il consenso della persona interessata) di dati in formato audio, video o immagine che riproducono registrazioni vocali o filmati o fotografie digitali riconducibili a persone, alunni e docenti, o altri soggetti, che operano o si trovino all’interno della scuola.

Sono previsti i seguenti provvedimenti disciplinari così come indicato nel regolamento d’istituto:

• richiamo verbale;

• richiamo scritto sul registro di classe o con annotazione sul diario;

• convocazione dei genitori da parte degli insegnanti.;

• convocazione dei genitori da parte del Dirigente scolastico.

In presenza di situazioni e/o episodi gravi, il Dirigente Scolastico provvederà alle opportune segnalazioni alle autorità competenti secondo le indicazioni della legge 71.2017. 2.

Le infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell’utilizzo delle tecnologie digitali e di internet sono:

• utilizzo delle tecnologie e dei servizi della scuola non connesso alle attività di insegnamento o al profilo professionale, come ed a titolo esemplificativo e non esaustivo l’installazione di software o lo scaricamento e il salvataggio di materiali non idonei o non consentiti dalla legge;

• trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un’adeguata protezione degli stessi;

• diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;

• scarsa vigilanza degli alunni che può favorire un utilizzo non autorizzato delle TIC.

Il Dirigente scolastico può controllare l’utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola. Tutto il personale è tenuto a collaborare con il Dirigente scolastico e con l'Animatore digitale, con la funzione strumentale e il referente per il cyberbullismo e a fornire ogni informazione utile per la risoluzione di eventuali situazioni problematiche connesse all’uso delle TIC e Internet.

Alcune condotte dei genitori possono favorire o meno l’uso corretto e responsabile delle TIC da parte degli alunni a scuola. Per esempio alcune famiglie sottovalutano i potenziali rischi a cui espongono i figli se permettono loro di:

• rimanere a casa da soli ad usare il computer.

• avere un computer nella propria stanza o in un posto non visibile.

• navigare sul web, utilizzare il cellulare o lo smartphone senza nessun controllo.

• utilizzare il pc o cellulare o smartphone in comune con gli adulti che possono conservare in

memoria materiali non idonei. I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

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 si integra pienamente per obiettivi e contenuti con il PTOF, incluso il piano per l'attuazione del PNSD e con i regolamenti già in vigore nell'Istituto Comprensivo quali:

- Regolamento interno d'Istituto;
- Regolamento per l'utilizzo dei laboratori di informatica;
- Patto di corresponsabilità.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il monitoraggio sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore Digitale, del Referente del Bullismo e dei Collabotori scolastici; sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di internet. Il monitoraggio sarà rivolto anche agli insegnanti, al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Creazione del gruppo di lavoro ePolicy
- Realizzazione di un sistema di monitoraggio delle attività

Azioni da svolgere nei prossimi 3 anni:

- Attività di prevenzione e contrasto al bullismo e cyberbullismo (intero anno scolastico)
- Formazione docenti riguardo uso corretto delle TIC (intero anno scolastico)

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.

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

Il Curricolo della scuola del primo ciclo di istruzione sulle competenze digitali per gli alunni è trasversale alle discipline previste dalle Indicazioni Nazionali: la competenza digitale è ritenuta dall'Unione Europea competenza chiave per la sua importanza nel mondo d'oggi.

In quest'ambito si seguono le indicazioni contenute nel PNSD (azione 14), in cui si individuano alcuni framework di riferimento per la definizione e lo sviluppo delle competenze digitali, tra cui il framework DIGCOMP, che prevede 21 competenze, di cui alcune specifiche nell'area della sicurezza:

- Dimensione tecnologica a) riconoscere le criticità tecnologiche b) selezionare la tecnologia adeguata per ciascun compito c) operare logicamente d) distinguere tra reale e virtuale.
- Dimensione cognitive o information literacy a) saper trattare (sintetizzare, rappresentare, analizzare) i testi, i dati, le tabelle e i grafici b) saper valutare la pertinenza dell'informazione e la sua affidabilità.
- Dimensione etica a) conoscere i concetti di tutela della privacy b) rispettare i diritti intellettuali dei materiali reperiti in Internet e l'immagine degli altri c) comprendere il

dislivello sociale e tecnologico che può esistere tra paesi, persone, generazioni, e il problema dell'accessibilità.

Al termine della scuola primaria e al termine del primo ciclo di istruzione le competenze digitali vengono certificate sulla base dei seguenti profili:

• primaria: usa le tecnologie in contesti comunicativi concreti per ricercare dati e informazioni e per interagire con soggetti diversi;

• secondaria di primo grado: usa con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo.

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.

Al fine di promuovere la condivisione di buone pratiche per un uso consapevole delle risorse digitali, prevenendo e contrastando "ogni forma di discriminazione e del bullismo, anche informatico" (Legge 107/2015, art. 1, c. 7, l), il nostro Istituto ha aderito quest'anno, come già detto nel primo capitolo della policy, al progetto "Generazioni Connesse", coordinato dal MIUR, in partenariato col Ministero dell'Interno-Polizia Postale e delle Comunicazioni e delle Comunicazioni e con altre importanti associazioni per la tutela dei diritti dei minori, come Children Italia e Telefono Azzurro.

L'Animatore digitale ed il suo team predispongono un piano di formazione progettato a partire dai bisogni formativi dei docenti. I corsi attivati riguardano l'utilizzo di metodologie multimediali nella didattica quotidiana e iniziative formative finalizzate a :

- alla gestione delle dinamiche relazionali in classe e dei gruppi difficili;
- alla prevenzione e identificazione precoce del disagio giovanile;
- ad interventi per l'uso corretto delle TIC e per il contrasto del cyberbullismo.

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.

I docenti sono invitati a completare i corsi di aggiornamento disponibili sulla Piattaforma di Generazioni Connesse dedicata alle scuole che hanno aderito al progetto (http://piattaforma.generazioniconnesse.it.)

Verranno inoltre organizzati dei laboratori/eventi destinati ai docenti, studenti e genitori relativi a tali tematiche in modo da sensibilizzare l'intera comunità scolastica sui rischi della navigazione non controllata e su un corretto uso delle tecnologie digitali**.**

2.4. - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

Il nostro istituto ha organizzato già negli anni passati incontri aperti alle famiglie e agli studenti con enti esterni, come la Polizia Postale o Carabinieri, 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 di cellulari, smartphone e chat line senza un'adeguata formazione in merito ai rischi derivanti da un uso inappropriato di tali dispositivi.

Il nostro piano d'azioni

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

- Organizzare e promuovere per il corpo docente incontri formativi sull’utilizzo e l’integrazione delle TIC nella didattica.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull’educazione alla cittadinanza digitale.

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

- 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.

Nelle scuole di ogni ordine e grado vengono trattate giornalmente numerose

informazioni sugli studenti e le studentesse, sulle loro famiglie, sui loro problemi sanitari o di disagio sociale, o ad esempio sulle abitudini alimentari. A volte può bastare una lettera contenente dati sensibili di un minorenne, o un avviso scolastico con riferimenti indiretti sulle condizioni di salute degli/lle studenti/esse, per violare anche involontariamente la riservatezza e la dignità di una persona.

Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali che si trovano a trattare, in particolare quando sono coinvolti soggetti minorenni.

La protezione dei dati personali è, infatti, 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 particolare, la scuola non ha solo il compito di tutelare la privacy degli/lle studenti/esse e delle loro famiglie, ma anche quello di informare e soprattutto rendere consapevoli gli/le studenti/esse di quanto sia importante tutelare il diritto alla riservatezza di sè stessi e degli altri.

La diffusione sempre maggiore di smartphone tra i giovanissimi, l'uso di tablet a scopo didattico, la condivisione online di contenuti didattici, l'uso del registro elettronico, l'eventualità di gruppi whatsapp tra studenti/esse, genitori, docenti o tra insegnanti e studenti/esse, obbliga la scuola ad avere un'attenzione particolare non solo alla privacy in generale, ma anche alla gestione della privacy legata all'uso dei nuovi dispositivi.

Sono dati personali :

- i dati che permettono l'identificazione diretta di una persona, come i dati anagrafici (ad es. nome e cognome);
- i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad es. il codice fiscale, l'indirizzo IP, il numero di targa);
- i dati rientranti in particolari categorie: si tratta dei dati cosiddetti sensibili, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale di una persona. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale.
- i dati relativi a condanne penali e reati: si tratta dei dati cosiddetti giudiziari, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale.

L'Istituto comprensivo " Bonvesin de la Riva" rispetta la privacy e si impegna a proteggere i dati personali che gli stessi conferiscono ad esso. La raccolta ed il trattamento dei dati personali avvengono, quando necessari, in relazione all'esecuzione dei servizi richiesti dall'utente, o quando l'utente stesso decide di

comunicare i propri dati personali; in tali circostanze, la presente politica della privacy ne illustra le modalità: in caso di raccolta di dati personali, l'Istituto informerà l'utente sulle finalità della raccolta al momento della stessa e, ove necessario, richiederà il consenso all'utente. Inoltre:

- il personale non deve condividere numeri di telefono personali o indirizzi di posta elettronica privati con la componente studentesca e con i genitori.
- le fotografie o i video da pubblicare sul sito che includano allieve e allievi saranno selezionati con cura e non permetteranno a singoli di essere chiaramente identificati a meno che non si tratti di eventi particolari per cui le famiglie potranno concedere opportuna autorizzazione. La scuola cercherà di utilizzare fotografie o video di gruppo piuttosto che foto integrali di singoli.
- i nomi completi di alunne e alunni saranno evitati sul sito web in particolare se in associazione con le loro fotografie.

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. *'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.

Accesso ad internet: filtri, antivirus

Tutte le aule della scuola secondaria dell'Istituto sono dotate di una infrastruttura informatica completa utilizzando la rete locale WLAN.

Tale sistema provvede a monitorare il traffico web nelle diverse postazioni dei pc delle aule didattiche e dell'Aula Robolab oltre che dell'aula di informatica, aggiornare gli antivirus e bloccare l'accesso a siti inappropriati al contesto scolastico, garantendo un buon livello di sicurezza on-line.

I computer della segreteria sono invece collegati al server.

La scuola, inoltre, è in possesso di tablet, ognuno dei quali è dotato di un proprio codice identificativo, è protetto da filtri appositi e si collega alle reti wi-fi scolastiche solo attraverso password che i docenti di volta in volta inseriscono e non rendono note agli alunni.

Disposizioni per l'utilizzo degli strumenti tecnologici della scuola e sull'uso dei locali dei laboratori informatici:

Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto senza modificare lo sfondo del desktop, la risoluzione del video, le impostazioni del mouse, la configurazione originale dell'hardware e le connessioni di rete, senza inviare dati e fotografie personali o di altre persone.

- I laboratori informatici e le postazioni informatiche dell'Istituto possono essere utilizzati esclusivamente per attività d'insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.
- i laboratori informatici sono fruibili previa definizione orario settimanale di utilizzo o compilazione di apposito registro.
- quando un insegnante, da solo o con la classe, usufruisce del laboratorio deve obbligatoriamente compilare l'apposito registro delle presenze con il proprio nome, l'eventuale classe, indicando la data, l'orario di ingresso, quello d'uscita, l'apparecchiatura utilizzata e gli eventuali malfunzionamenti riscontrati. Questo allo scopo di poter risalire alle cause di eventuali inconvenienti o danneggiamenti e per comprovare l'effettivo utilizzo dell'aula.
- l'ingresso degli alunni nei laboratori è consentito solo in presenza dell'insegnante. Gli alunni, quando prendono posto e prima di iniziare a lavorare, devono segnalare eventuali danneggiamenti, scritte o qualsiasi altra anomalia riscontrata nella loro postazione, onde evitare di essere considerati responsabili del danno.
- il docente accompagnatore è responsabile del corretto uso didattico di

hardware e software.
- nei laboratori è vietato utilizzare dispositivi di archiviazione personali se non dopo opportuno controllo con antivirus.
- è' vietato cancellare o alterare files-dati presenti in hard-disk, salvare files personali nelle cartelle condivise.
- è' vietato iscriversi a qualche sito web e scaricare materiale di vario tipo senza autorizzazione del docente.
- prima di terminare la propria sessione di lavoro, verificare di non aver lasciato delle code di stampa.
- il laboratorio non deve mai essere lasciato aperto e incustodito quando nessuno lo utilizza.
- all'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il mobilio in ordine, le macchine spente correttamente (i monitor rimangono accesi e i PC vanno spenti mediante apposito comando chiudi sessione…).
- le stampanti devono essere utilizzate secondo criteri di efficacia ed economicità.
- in caso di malfunzionamento non risolvibile dal responsabile incaricato si contatterà personalmente l'ufficio di segreteria.

Gestione accessi

Tutte le aule sono dotate di pc a disposizione dei docenti per la compilazione del registro elettronico e come supporto alla didattica. Questi pc sono protetti da password personali riservate ai docenti. I computer dell'aula informatica , sempre collegati alla rete WLAN, non hanno password ma il loro utilizzo è possibile solo sotto stretta vigilanza da parte dei docenti. La connessione alla rete wi-fi è riservata agli insegnanti per fini didattici ed è possibile accedervi solo attraverso una password.

Sito web della scuola

Il nostro Istituto possiede un sito istituzionale, che è gestito da un docente esperto e che viene costantemente aggiornato e arricchito con le attività svolte e le news.

Esso offre al proprio interno i seguenti servizi alle famiglie ed agli utenti esterni:

- consultazione elenchi libri di testo;
- piano dell'offerta formativa;
- regolamento d'Istituto;
- informazioni generali sull'Istituto;
- informazioni sui progetti attivati dall'Istituto;
- informazioni sull'amministrazione dell'Istituto;
- avvisi e comunicazioni;
- moduli vari.

E-mail

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. Le credenziali sono in possesso del personale amministrativo.

Registro elettronico

Ogni famiglia riceve le credenziali per l'accesso riservato al registro elettronico, in cui il corpo docente è tenuto a registrare assenze, valutazioni, note e osservazioni. L'uso del registro elettronico è spiegato alle famiglie tramite circolare. Coloro che non possono accedere a Internet e di conseguenza non possono consultare il registro elettronico sono pregati di darne segnalazione al coordinatore del consiglio di classe, che verificherà la trascrizione delle comunicazioni sul diario e la firma dei genitori.

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.

Nella pratica didattica, il docente è ovviamente il primo soggetto che favorisce l'uso corretto della rete, guidando gli studenti nelle attività online, stabilendo obiettivi chiari di ricerca, insegnando le strategie appropriate nella definizione e gestione della risorsa informatica.
Gli alunni accedono alla rete, sotto precisa responsabilità e controllo del docente, dai terminali presenti nei laboratori, mentre l'uso della rete nelle singole classi (così come del resto di tutta la strumentazione presente nelle aule) non è loro consentito.
Tutte le famiglie firmano a inizio anno una liberatoria relativa all'apparizione dei loro figli in immagini o video prodotti dalla scuola.
Per quanto riguarda specificamente i video, essi vengono pubblicati sul canale Youtube della scuola e la maggior parte di essi viene realizzata introducendo un file audio protetto da copyright: l'operazione avviene seguendo le norme in merito di Youtube, accettando dunque il riconoscimento di contenuto di terze parti e le conseguenti azioni del sistema di amministrazione del canale.

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.

Per gli studenti della Scuola primaria e Secondaria : è vietato l'utilizzo di cellulari per l'intera durata delle attività scolastiche. È consentito agli alunni con Bisogni Educativi Speciali utilizzare il proprio notebook o tablet. È consentito a tutti gli studenti, in casi concordati con il docente (uscite didattiche, produzioni multimediali, uso di Classroom) l'utilizzo di dispostivi elettronici personali per scopi didattici. Nel caso in cui gli alunni debbano comunicare con la famiglia durante l'orario scolastico possono utilizzare la linea fissa della scuola chiedendo ad un collaboratore; allo stesso modo le famiglie devono chiamare al numero telefonico della scuola se hanno assoluta necessità di parlare con i figli.

Per i docenti: durante il loro orario di servizio è consentito l'utilizzo di dispostivi elettronici personali solo ed esclusivamente per fini educativo-didattici.

Per il personale della scuola: è consentito l'utilizzo di dispostivi elettronici personali solo ed esclusivamente per esigenze di servizio**.**

Il nostro piano d'azioni

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

- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto 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).**
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali;
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul

tema delle tecnologie digitali e della protezione dei dati personali

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

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

4.1 - Sensibilizzazione e Prevenzione

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

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

È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e contenerli, ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. Ciò è possibile lavorando su aspetti di ampio raggio che possano permettere una riduzione dei fattori di rischio e di conseguenze 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.*

Le misure di sensibilizzazione e di prevenzione comprendono l'integrazione nel curricolo dei temi legati al corretto utilizzo delle TIC e di Internet: la progettazione di unità didattiche specifiche deve essere pianificata a livello di dipartimenti disciplinari, garantendo un intervento su ogni classe. La scuola si avvale della collaborazione di enti e associazioni per realizzare incontri rivolti alla componente studentesca e alle famiglie con l'intento di fornire ogni elemento utile alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica; le famiglie sono invitate a proporre tematiche di particolare interesse su cui la scuola focalizzerà il proprio intervento.

L'Istituto comprensivo Bonvesin attiva inoltre uno sportello di ascolto al quale la componente studentesca si può rivolgere per avere consigli e sostegno psicologico anche relativamente alle tematiche del cyber-bullismo. La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti. A partire dalla corretta formazione e sensibilizzazione di tutti gli adulti coinvolti, docenti e personale ATA sono

invitati a essere confidenti e custodi, diretti o indiretti, di ciò che le ragazze e i ragazzi vivono. Accorgersi tempestivamente di quanto accade e compiere azioni immediate di contrasto verso gli atti inopportuni -quando non illegali- diviene fondamentale per poter evitare conseguenze a lungo termine che possano pregiudicare il benessere e una crescita armonica dei soggetti coinvolti. La gestione dei casi rilevati va differenziata a seconda della loro gravità; fermo restando che è opportuna la condivisione a livello di Consiglio di Classe di ogni episodio rilevato, anche minimo, alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e come rimediare. Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico.

AZIONI

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

- diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web, condividendo materiali messi a disposizione sul sito del progetto "Generazioni connesse";

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

- far rispettare il divieto di utilizzo di dispositivi digitali propri, quali cellulare, agli studenti in orario scolastico.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

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

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

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;

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

Le responsabilità per atti di bullismo e cyberbullismo compiute dal minorenne possono ricadere anche su:

- i genitori, perché devono educare adeguatamente e vigilare, in maniera adeguata all'età del figlio, cercando di correggerne comportamenti devianti. Questa responsabilità generale persiste anche per gli atti compiuti nei tempi di affidamento alla scuola (culpa in educando).
- gli insegnanti e la scuola: perché nei periodi in cui il minore viene affidato all'Istituzione scolastica il docente è responsabile della vigilanza sulle sue azioni e ha il dovere di impedire comportamenti dannosi verso gli altri/e ragazzi/e, insegnanti e personale scolastico o verso le strutture della scuola stessa. A pagare in primis sarà la scuola, che poi potrà rivalersi sul singolo insegnante. La responsabilità si estende anche a viaggi, gite scolastiche, manifestazioni sportive organizzate dalla scuola (culpa in vigilando).
- esiste poi una culpa in organizzando, che si ha quando la scuola non mette in atto le azioni previste per la prevenzione del fenomeno o per affrontarlo al meglio (così come previsto anche dalla normativa vigente).

Azioni da intraprendere:

Gli interventi che la scuola mette in atto sono tesi a far conoscere e sensibilizzare gli alunni verso un uso responsabile e consapevole della rete, al fine di assicurare loro il rispetto del diritto ad essere tutelati da abusi e violenze da un lato e, allo stesso tempo, suscitare atteggiamenti di rispetto nei confronti degli altri utenti.

Le nuove tecnologie si pongono quale strumento attraverso cui sviluppare pratiche di collaborazione tra gli studenti per riconoscere e accettare la diversità e favorire la partecipazione finalizzata alla costruzione dei diversi percorsi formativi a cui sono chiamati tutti gli alunni.

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.

Si tratta di attività di analisi e di produzione mediale, finalizzate soprattutto a:

- riflettere sull'uso del linguaggio usato per comunicare facendo riferimento al "Manifesto" di Parole Ostili;
- creare un clima di collaborazione fra compagni contrastando il linguaggio dell'odio;
- riflettere sulla libertà di espressione e di linguaggio senza trasformarla in occasione di offesa;
- utilizzare il linguaggio mediatico come veicolo di inclusione.

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?

Il provvedimento approvato dalla Giunta regionale con dgr 2609 del 9.12.2019 si propone di diffondere un modello organizzativo ed efficace per l'attuazione di interventi di prevenzione e contrasto alla Ludopatia. Le risorse destinate al territorio saranno destinate al potenziamento dell'attività di prevenzione e contrasto del gioco d'azzardo patologico nei luoghi di

lavoro, nelle scuole e nelle comunità locali.

OBIETTIVI

- promuovere il contrasto al Gioco d'azzardo patologico nei luoghi di lavoro, nelle scuole e nelle comunità locali sensibilizzando, informando e formando operatori e cittadini;
- regolamentare in modo uniforme le disposizioni comunali per il contrasto al gioco d'azzardo;
- sensibilizzare e disseminare le informazioni a studenti, genitori e docenti, coordinate dalle ATS, concordate con le scuole capofila della Rete di Ambito;
- coinvolgere le scuole, attraverso la Rete delle Scuole che Promuovono Salute;
- sostenere i processi di alfabetizzazione sanitaria sul gioco d'azzardo nei diversi target;
- aumentare le opportunità di diagnosi precoce, cura e riabilitazione, anche con azioni sperimentali.

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.

Le azioni da intraprendere in tal caso sono:

Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione.

V**erso la componente studentesca**: inserimento nel curricolo di temi legati all'affettività, alla sessualità e alle differenze di genere. In casi simili, 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. Chi è immerso dalla nascita nelle nuove tecnologie spesso non è consapevole che una foto o un video diffusi in rete potrebbero non essere tolti mai più né è consapevole di scambiare o diffondere materiale pedopornografico. In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico per gli adempimenti del caso.

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.

Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e perché no, della sessualità.

Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad esempio, all'adescatore. È importante che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove.

Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video…).

L'adescamento, inoltre, può essere una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.

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.

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.Risulta utilissima l'attività educativa sull'affettività e le relazioni, sottolineando sempre la necessità di rivolgersi ad un adulto quando qualcosa online mette a disagio.

Azioni da intraprendere:

Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli.

Verso la componente studentesca: inserimento nel curricolo di temi legati alla affidabilità delle fonti online, all'interculturalità e al rispetto delle diversità. Qualora si venga a conoscenza di casi simili, occorre convocare i genitori per richiamarli a un maggiore controllo sulla fruizione di Internet da parte dei propri figli e/o sulla necessità di non usufruirne in presenza degli stessi.

Il nostro piano d'azioni

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

□ 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.

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 ai genitori e ai docenti, con il coinvolgimento di esperti.

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

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 un/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 dai/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 "pericolosi" per gli alunni possono essere i seguenti:

1. contenuti che violino la 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.)
2. contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus);
3. contenuti razzisti, che inneggiano al suicidio (immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.)
4. contenuti che implichino la sfera della sessualità.

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 docente informato del caso di (cyber)bullismo, dopo aver ricostruito fatti e responsabilità in colloqui separati coi protagonisti, redige un modulo di segnalazione (allegato n.4) che viene

protocollato, e informa:

- Coordinatore / Docenti di Classe (Primaria)
- Referente del cyberbullismo
- Dirigente scolastico

A. Nei casi a bassa intensità (linguaggio offensivo non reiterato, litigi online, esclusione da chat, molestie, «scherzi», lievi prepotenze), dove non è necessario avvertire le Autorità:

il Dirigente convoca gli alunni coinvolti direttamente (bullo/i, vittima/e), i genitori degli stessi (d'accordo con il CdC) alla presenza del Coordinatore / Docenti di Classe (Primaria) e/o altro docente.

B. Nei casi a media intensità (linguaggio offensivo reiterato, litigi online, esclusione da chat, molestie, «scherzi», prepotenze che coinvolgono minori di scuole diverse), dove è necessario avvertire la Polizia postale per rimuovere i contenuti dalla rete:

il Dirigente convoca gli alunni coinvolti direttamente (bullo/i, vittima/e), i genitori degli stessi (d'accordo con il CdC) alla presenza del Coordinatore / Docenti di Classe (Primaria), del referente del cyberbullismo e/o altro docente.

C. Nei casi ad alta intensità (grave ripercussione fisica e/o psicologica: sexting, flaming, cyberstalking, outing estorto, impersonificazione), dove è necessario avvertire la Polizia postale e l'Autorità giudiziaria, occorre agire con tempestività:

il Dirigente convoca gli alunni coinvolti direttamente (bullo/i, vittima/e) e i genitori degli stessi il giorno successivo alla segnalazione (d'accordo con il CdC), alla presenza del Coordinatore / Docenti di Classe (Primaria) (che redige verbale dell'incontro da allegare al registro dei verbali e inviare al referente cyberbullismo), del referente cyberbullismo e/o altro docente.

In tutti e tre i casi (A - B - C)

il Dirigente, se lo ritiene opportuno, convoca un Consiglio di classe straordinario, per stabilire gli interventi educativi e le misure delle sanzioni disciplinari;

il Dirigente, in accordo con il Consiglio di Classe, informa le famiglie degli alunni coinvolti e attiva:

- gli interventi individuali: misure di supporto per la vittima
- le sanzioni disciplinari e percorsi rieducativi per il/i (cyber)bullo/i,
- gli interventi nel gruppo classe.

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.

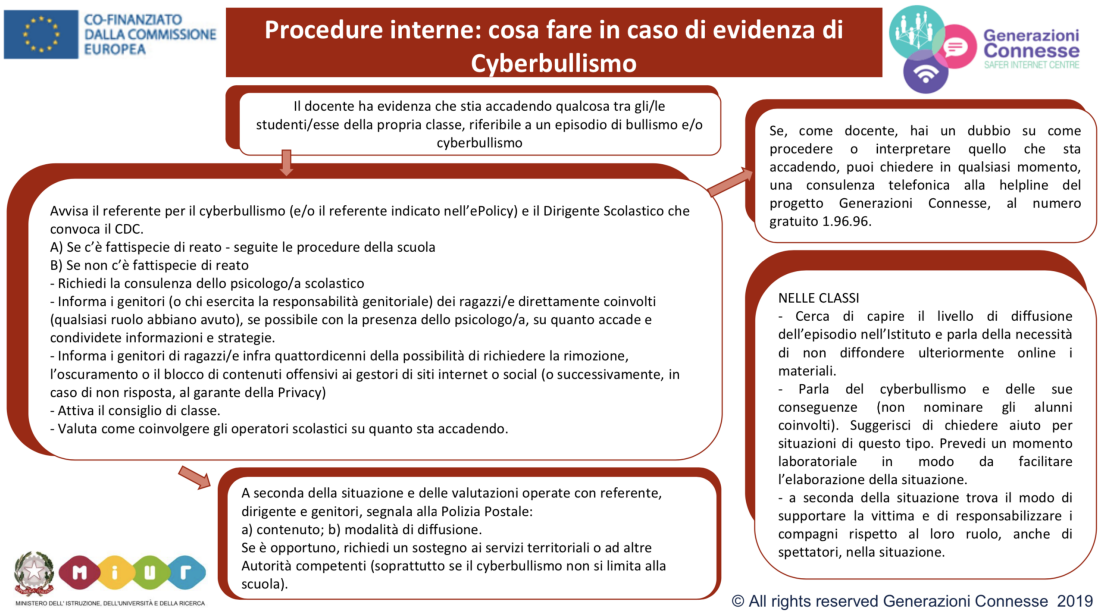
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

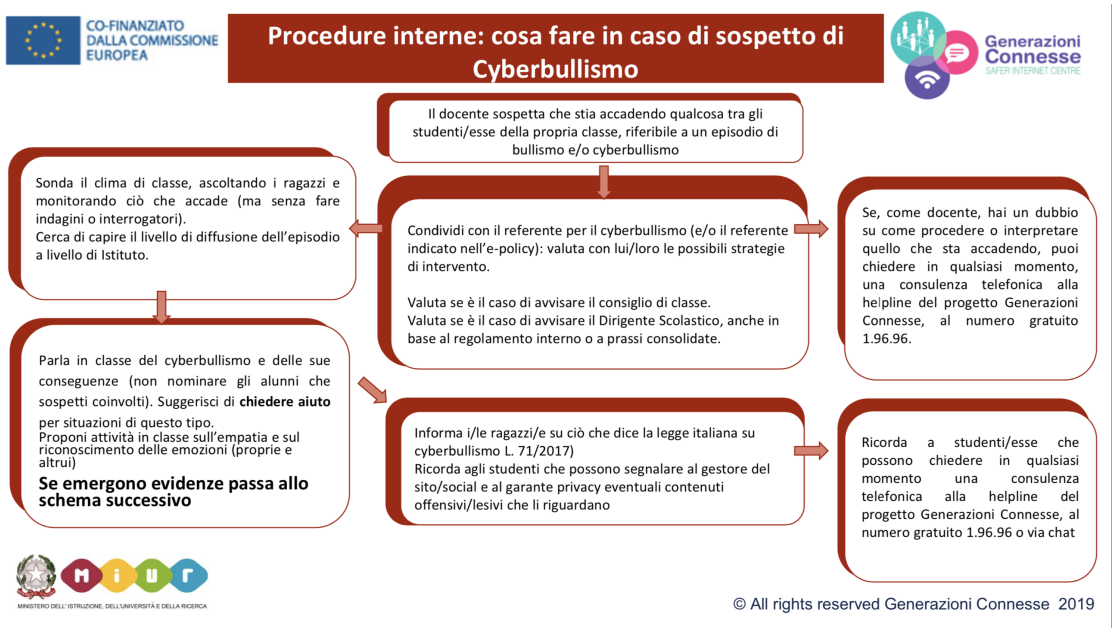
psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.

- **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.

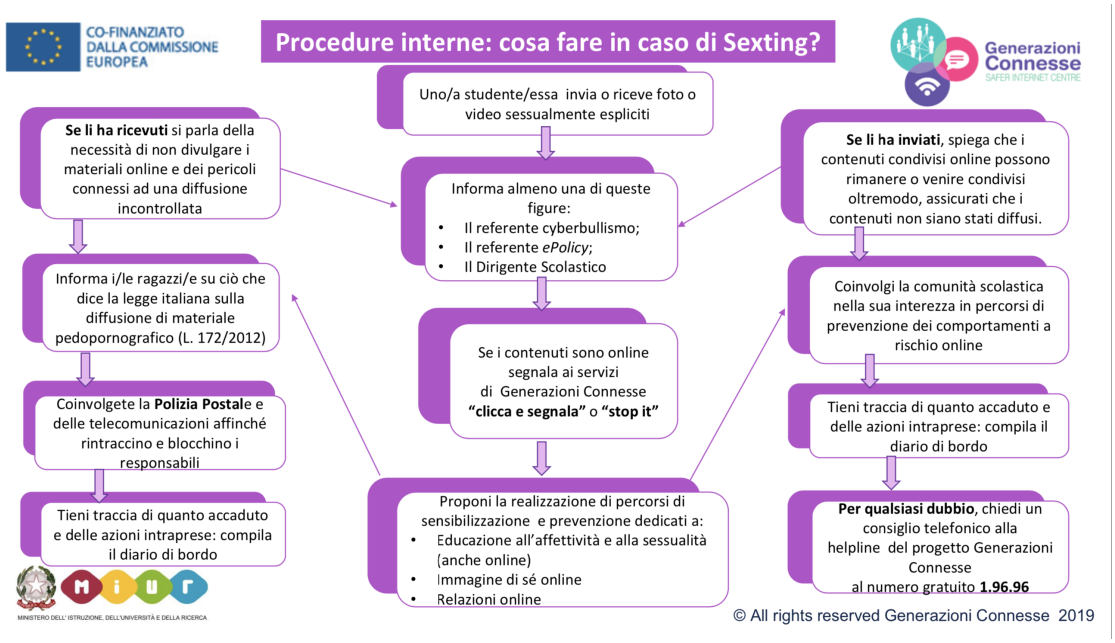
5.4. - Allegati con le procedure

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

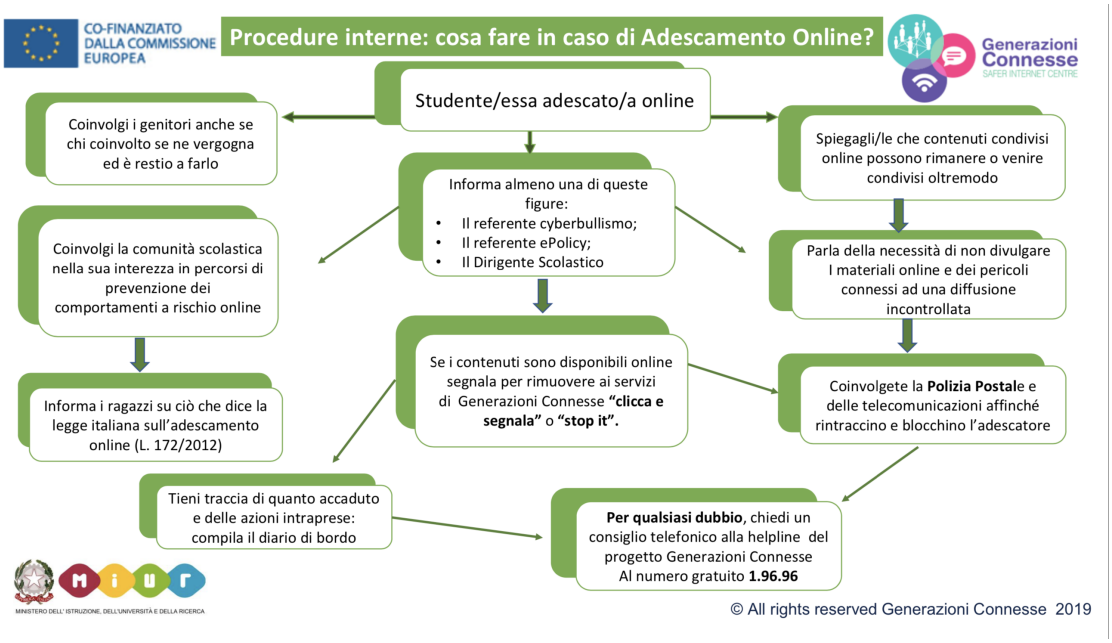




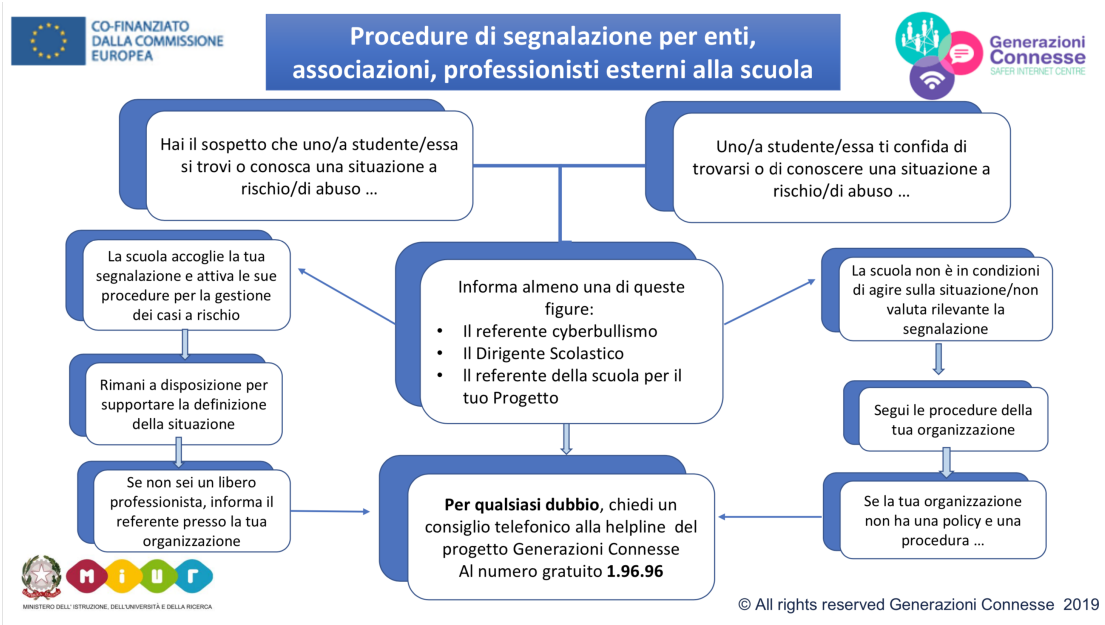
Procedure interne: cosa fare in caso di sexting?



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

https://www.generazioniconnesse.it/_file/documenti/E-LEARNING-LEZIONI/Corso-5/Scheda%20di%20segnalazione.docx

https://www.generazioniconnesse.it/_file/documenti/E-LEARNING-LEZIONI/Corso-5/Diario%20di%20bordo%20.docx

https://www.generazioniconnesse.it/_file/documenti/E-LEARNING-LEZIONI/Corso-5/iGloss%201.0%20l_ABC%20dei%20comportamenti%20devianti%20online.pdf

https://www.generazioniconnesse.it/_file/documenti/E-LEARNING-LEZIONI/Corso-5/Elenco%20reati%20procedibili%20Ufficio.pdf

Il nostro piano d'azioni

Non è prevista nessuna azione.

Ds Elena Osnaghi
10/04/2020 09:16:24