E-Safety Policy

IC Via Volsinio
Roma

INDICE

- *Azioni*
- *Rilevazione*
- *Come segnalare: quali strumenti e a chi*
- *Sportello d'ascolto*
- *Legge 71/2017*

1. Introduzione

1.1 Scopo della Policy

Con l'obiettivo di educare gli studenti ad un uso critico e consapevole della rete e sensibilizzare gli adulti di riferimento - docenti, personale della scuola e genitori - sull'importanza di una navigazione sicura e protetta, l'I.C. Via Volsinio ha avviato negli anni una proficua collaborazione con la Polizia Postale, realizzando incontri periodici con gli studenti e con le famiglie e nel biennio 2015-2017 ha partecipato al progetto "Generazioni Connesse", iniziativa co-finanziata dalla Commissione Europea e coordinata dal MIUR-Direzione Generale per lo studente, in partenariato col Ministero dell'Interno - Polizia Postale e delle Comunicazioni, l'Autorità Garante per l'Infanzia e l'Adolescenza, Save the Children Italia, Telefono Azzurro e le principali realtà italiane che si occupano di sicurezza nella rete.

L'adesione al progetto prevede la stesura da parte della scuola di un documento volto a descrivere la percezione della sicurezza in rete all'interno dell'Istituto, le norme comportamentali che possano limitarne i rischi, le procedure per l'utilizzo delle TIC in ambiente scolastico, le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali. Le linee di azione indicate recepiscono e realizzano le indicazioni della legge n.71 del 21 maggio 2017.

Negli ultimi anni la scuola ha investito notevoli risorse progettuali per incrementare l'uso delle tecnologie informatiche nella didattica, per svolgere esperienze formative innovative e per rendere più efficienti le funzioni amministrative nell'organizzazione generale della scuola.

Con il documento, denominato ***E-Safety Policy***, ci si prefigge di:

- stabilire i principi fondamentali cui tutta la comunità scolastica dovrà attenersi nell'utilizzo delle tecnologie, perché esse possano divenire strumento per una didattica integrata;

- fissare chiari codici di condotta che possano salvaguardare gli alunni dalle conseguenze disciplinari e/o giudiziarie delle loro azioni;
- fornire strumenti di tutela contro gli atteggiamenti di cyberbullismo per la tutela del benessere psico-fisico di tutti gli studenti.

1.2 Ruoli e Responsabilità

La E-Safety Policy è un documento condiviso da tutte le componenti educative che operano nella scuola e approvato dal Collegio dei Docenti e dal Consiglio d'Istituto. Sottoposto a periodico aggiornamento, esso declina i compiti, i ruoli e le responsabilità di ciascuna componente della comunità scolastica, così come di seguito specificato.

Ruoli e responsabilità della Scuola

La Scuola si impegna a:

1. promuovere un'educazione finalizzata ad un uso sicuro e consapevole dei nuovi media;
2. fornire agli studenti gli strumenti per conoscere e utilizzare le potenzialità formative delle tecnologie digitali;
3. rendere consapevoli gli alunni circa i rischi a cui sono esposti con un uso non corretto delle tecnologie digitali;
4. intervenire con gli strumenti a disposizione in tutti quei casi che minacciano la sicurezza dei ragazzi in rete;
5. promuovere e favorire iniziative volte alla formazione del personale docente e non sulle tematiche relative alla sicurezza in rete e all'uso consapevole e responsabile delle strumentazioni;
6. promuovere azioni di conoscenza e diffusione del regolamento interno per quanto riguarda nello specifico l'uso delle TIC e dei dispositivi personali;
7. diffondere la peer education, come strategia efficace per contrastare i rischi legati alle tecnologie digitali, agli ambienti virtuali, ai social network, ecc.;
8. adottare misure atte a prevenire e contrastare ogni forma di violenza e di prevaricazione;
9. garantire, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per il buon funzionamento delle dotazioni in uso e favorire l'acquisizione di sistemi per il monitoraggio e l'accesso sicuro.

Ruoli e responsabilità delle Famiglie

Le Famiglie si impegnano a:

1. informarsi sulle linee adottate dalla scuola circa l'utilizzo delle tecnologie;
2. vigilare i comportamenti dei ragazzi nella rete;
3. proseguire anche nei contesti extrascolastici l'azione di sensibilizzazione avviata dalla scuola;
4. collaborare con la scuola, quando necessario, per attuare interventi educativi a seguito di comportamenti impropri messi in atto dai figli;
5. partecipare alle iniziative formative promosse dalla scuola e a loro riservate.

Ruoli e responsabilità degli Studenti

Gli Studenti si impegnano a:

1. partecipare con interesse a tutte le iniziative che li informino circa le procedure di autotutela;
2. segnalare i casi che necessitano dell'aiuto dell'adulto per una corretta gestione;
3. conoscere e rispettare il regolamento sull'uso delle dotazioni tecnologiche della scuola e dei dispositivi personali;
4. adottare comportamenti a tutela della propria e altrui privacy e sicurezza;
5. assumere atteggiamenti rispettosi degli altri nella comunicazione in rete.

1.3 Condivisione e comunicazione della Policy all'interno dell'intera comunità scolastica

Applicandosi a tutti membri della scuola, la E-Safety Policy di Istituto viene comunicata al personale, agli alunni, alla comunità scolastica attraverso:

1. la pubblicazione sul sito della scuola;
2. la diffusione presso gli studenti mediante la lettura e la discussione all'interno delle classi;
3. la sottoscrizione da parte dei genitori all'inizio del primo anno di scuola secondaria del Patto di Corresponsabilità, aggiornato secondo le linee guida contenute nella Policy

1.4 Gestione dell'infrazione alla Policy

All'interno della scuola opera un docente Referente con il compito di coordinare le iniziative di prevenzione e di contrasto ai fenomeni di bullismo e cyberbullismo, anche avvalendosi della collaborazione delle Forze di Polizia, delle associazioni e dei centri di aggregazione giovanile presenti sul territorio.

La gestione delle infrazioni, rilevate dalle figure preposte e dal personale della scuola, è responsabilità del Dirigente Scolastico, il quale esamina i singoli casi e avvia le opportune procedure in conformità alla presente Policy, anche avvalendosi della collaborazione dei suoi Collaboratori e del Referente bullismo e cyberbullismo per la comunicazione con i Consigli di Classe e con i genitori degli studenti responsabili dell'infrazione.
Qualora essa richieda l'intervento della Polizia Postale si procederà come da protocollo.

1.5 Integrazione della Policy con Regolamenti esistenti

La presente Policy viene integrata nel Regolamento d'Istituto e nel Patto di Corresponsabilità e pubblicata sul sito della scuola all'indirizzo http://www.istitutoviavolsinio.it.

2. Formazione e Curricolo

2.1 Curricolo sulle competenze digitali degli studenti

Nell'ambito del PNSD, all'interno del curricolo sulle competenze digitali in via di definizione, l'Istituto si propone un programma di progressiva educazione alla sicurezza on line come parte del curricolo scolastico. Si impegna a sviluppare comportamenti adeguati all'età degli alunni e a promuovere attività mirate a:

1. sviluppare strategie per valutare le informazioni trovate in rete e affinare una ricerca;
2. creare una figura di alunno cyber-esperto per facilitare e diffondere le buone pratiche di utilizzo della rete attraverso la metodologia peer to peer;
3. educare a segnalare eventuali abusi on line e a richiedere aiuto quando si incorre in problemi nella navigazione;

4. far conoscere le conseguenze (penali e civili) che possano derivare dalla pubblicazione impropria di foto o video altrui e dalla diffusione in rete di dati sensibili;
5. far riconoscere il rischio insito nella comunicazione on line con identità sconosciute;
6. far identificare un comportamento non corretto in un ambiente on line;

Nell'ottica della condivisione delle buone pratiche educative, l'Istituto promuove la partecipazione ad iniziative ed eventi dedicati al tema della sicurezza in rete, quali la giornata dell'Internet Safety Day.

2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica

La Scuola ha partecipato con successo a progetti, anche di livello europeo, che hanno consentito di avviare un adeguamento dell'infrastruttura e di dotare le aule di strumenti utili a una didattica integrata sia nella sede di Via Volsinio che in quella di Via S. Maria Goretti. All'interno della scuola operano un Animatore Digitale e un Team per l'Innovazione con il compito di creare i contesti più favorevoli per l'attuazione del PNSD; i docenti della scuola sono stati destinatari di iniziative di aggiornamento e di formazione sul tema delle nuove tecnologie, sia gestite a livello centrale dal Miur, che organizzate a livello locale con l'impiego delle figure dedicate all'interno della scuola. Interventi sull'uso del Registro elettronico sono reiterati ogni anno, anche in funzione delle implementazioni che l'azienda distributrice del prodotto apporta al sistema, come la possibilità di inserire in piattaforma materiali didattici disciplinari da condividere con gli studenti.

La Scuola ha inoltre partecipato con una progettualità specifica al bando per i progetti PON sul tema "Cittadinanza e creatività digitale" e "Inclusione sociale e lotta al disagio", ricevendo finanziamenti utili a realizzare moduli formativi sui temi legati alla E-Policy di Istituto.

2.3 Formazione dei docenti sull'uso consapevole e sicuro di internet e delle tecnologie digitali

La Scuola diffonde e pone in evidenza ai docenti mediante l'invio agli indirizzi email personali le iniziative di formazione che pervengono alla casella istituzionale dell'Istituto e ne favorisce la partecipazione. La E-Policy di Istituto è presentata agli Organi Collegiali e da essi adottata, nella condivisione totale delle linee guida e di azione. Il Referente del bullismo e cyberbullismo lavora in sinergia con i team di classe ogni qualvolta essi ne ravvisino la necessità, come

supporto alla gestione dei casi e/o con interventi specifici con i ragazzi. Anche i moduli formativi previsti dai progetti PON offrono un'importante possibilità di formazione a medio e lungo termine sul tema.

2.4 Sensibilizzazione delle famiglie

Incontri rivolti alle famiglie sono stati effettuati nel corso degli aa.ss. 2015/16 e 2016/17 con la partecipazione degli operatori del progetto "Generazioni Connesse". Nell'incontro di inizio anno scolastico con le famiglie delle classi in entrata nella scuola secondaria, la Scuola responsabilizza i genitori sull'uso del Registro Elettronico e presenta la E-Safety Policy, che sarà poi sottoposta agli studenti nel corso del triennio perché ne conoscano le linee guida e di azione.

3. Gestione dell'infrastruttura e della strumentazione ICT della scuola

La Scuola mette in atto le azioni necessarie per garantire agli studenti l'accesso alla documentazione in rete, adottando cautele che possano diminuire le possibilità di rischio durante la navigazione (Art.1, commi 7, 57,58 della Legge n.107del 15 luglio 2015, Legge n. 71 del 29 maggio 2017, Art. 4, comma 1 della Legge 71 del 29 maggio 2017).
Resta fermo che, per la presenza di un gran numero di dispositivi personali all'interno della struttura scolastica, la Scuola non può assumersi responsabilità conseguenti all'uso improprio delle tecnologie informatiche e della rete.

3.1 Comportamenti da mettere in atto nell'uso dei dispositivi elettronici e della rete

<u>Buone pratiche da mettere in atto nell'uso della rete:</u>

• Controllare la validità e l'origine delle informazioni a disposizione;

• Utilizzare fonti alternative di informazione per proposte comparate;

• Ricercare il nome dell'autore, i riferimenti circa l'ultimo aggiornamento del materiale, l'indirizzo di altri possibili link al sito;

• Rispettare i diritti di autore e i diritti di proprietà intellettuale, nonché le linee guida di buona condotta dell'utente;

• Rispettare nella navigazione la legislazione vigente;

• Non divulgare notizie private contenute nelle documentazioni elettroniche cui si è avuto o si ha accesso;

• Tutelare la propria privacy e quella degli altri al fine di non diffondere dati sensibili (indirizzo, recapito, altro) nel web;

• Rispettare la netiquette (regole condivise che disciplinano il rapporto fra utenti della rete, siti, forum, mail e qualsiasi altro tipo di comunicazione);

• Richiedere l'autorizzazione ad un adulto prima di iscriversi a mailing-list o registrarsi a siti web;

• Non prendere appuntamenti con le persone conosciute tramite web;

• Comunicare con gli adulti di riferimento (docenti, genitori) nel caso in cui si incontrino in Internet immagini o scritti che infastidiscono e/o se si è oggetto di richieste di contatto da parte di sconosciuti.

<u>Regole di comportamento da rispettare:</u>

- Accedere ai dispositivi elettronici e al web solo su autorizzazione del docente e unicamente a fini didattici;
- Non modificare le impostazioni del corredo informatico della scuola;
- Utilizzare correttamente il parco tecnologico dell'Istituto, considerandolo un bene comune da mantenere in piena funzionalità ed efficienza;
- Rispettare nella navigazione e nell'uso degli applicativi le persone di ogni nazionalità, cultura, religione, sesso;
- Non utilizzare i dispositivi elettronici per fotografare e/o riprendere luoghi, ambienti, persone della scuola e/o comunicare senza previa autorizzazione;
- Non diffondere nella rete informazioni personali o di altre persone (indirizzi, numeri di telefono, foto, altro);
- Non scaricare materiali dal web senza autorizzazione del docente.

L'inosservanza di tali regole avvierà le opportune procedure a termini di Regolamento d'Istituto.

3.2 *Sito web della scuola*

L'Istituto dispone di un proprio spazio web e di un proprio dominio: www.istitutoviavolsinio.it

Il Dirigente Scolastico e il personale incaricato di gestire il sito garantiscono la rispondenza del contenuto pubblicato alle norme di legge.
All'interno del sito una specifica sezione consente la pubblicazione di materiali didattici ai fini della loro divulgazione nella comunità scolastica e nel territorio.

I contenuti sono pubblicati previa autorizzazione del Dirigente Scolastico, Responsabile della Trasparenza.

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

3.3 Social network

A norma di legge la diffusione in rete di nomi, dati, giudizi, foto, filmati, audio, sui singoli o sulle istituzioni e senza il consenso delle persone coinvolte può determinare conseguenze di carattere anche penale.

Si invitano pertanto gli studenti a non diffondere sul web immagini, video o registrazioni – anche solo audio – non autorizzati, nel pieno rispetto della privacy di tutti. Chiunque venga a conoscenza di presenza nella rete di offese, ingiurie o commenti impropri che possano ledere l'immagine dell'Istituto e/o dei suoi docenti e studenti è tenuto a darne segnalazione alle persone preposte nella scuola.

Allo stesso tempo, si invitano le famiglie a vigilare affinché l'uso dei Social Network, in particolare Facebook, Whatsapp e Instagram, avvenga nel pieno rispetto delle norme.

La comunicazione attraverso la rete tra famiglie, docenti e alunni dovrà avvenire tramite il Registro elettronico, la mail della scuola, la mail dedicata al profilo professionale di cui è opportuno si doti ciascun insegnante .

3.4 Posta elettronica

Le caselle di posta elettronica dell'Istituto devono essere utilizzate solo per attività inerenti la comunicazione e gestione scolastica.

3.5 Privacy

1. La pubblicazione sul sito della scuola di fotografie e video che ritraggano lo studente potrà avvenire solo in presenza di esplicita autorizzazione firmata

dagli esercenti la patria potestà sul minore. In assenza di questa non sarà diffuso alcun materiale.

2. Per motivi di sicurezza, è opportuno che le password per l'accesso al Registro elettronico fornite dalla scuola a ciascun genitore siano conservate con cura e aggiornate con regolarità.
   Il dovere della custodia e della riservatezza delle password resta a carico dei genitori, soprattutto per quanto riguarda il codice Pin, che consente azioni nel Registro elettronico di esclusiva pertinenza delle figure esercenti la patria potestà sul minore.

3.6 Registro elettronico

Ogni famiglia riceve le credenziali per l'accesso al registro elettronico, in cui il personale docente è tenuto a registrare assenze, valutazioni, note e osservazioni. L'uso del registro elettronico è illustrato alle famiglie attraverso brevi e chiare istruzioni disponibili sul sito.

La compilazione del registro elettronico da parte dei docenti assolve l'obbligo di comunicare prontamente ed efficacemente ogni evento riguardante gli studenti.
Sul registro elettronico vengono rese disponibili anche le circolari del Dirigente Scolastico pubblicate contestualmente sul sito della scuola, la cui firma per presa visione deve essere presentata al docente di classe.

Coloro che non possono accedere a Internet e di conseguenza non possono consultare il registro elettronico sono pregati di darne segnalazione tempestiva in segreteria. E' opportuno informarne anche gli insegnanti di classe perché le comunicazioni possano avvenire attraverso il quaderno disposto a questo scopo. Lo studente potrà utilizzare il diario personale per la corretta trascrizione dei compiti.

4. Strumentazione personale

4.1 Per gli studenti: gestione degli strumenti personali (cellulari, tablet, altro)

Come da Regolamento scolastico agli studenti è vietato l'utilizzo del cellulare all'interno della scuola.
I telefoni cellulari, i tablet e le relative fotocamere e registratori vocali potranno essere utilizzati durante le lezioni solo all'interno di attività didattiche programmate e gestite dal docente.
Non sono consentiti giochi e consolle che possono avere accesso a Internet,

nemmeno se custoditi dai docenti.
Se non giustificati dall'attività didattica in corso e autorizzati dal docente, i dispositivi saranno requisiti dall'insegnante e restituiti al termine delle lezioni giornaliere.
Sarà cura del docente provvedere ad avviare la sanzione disciplinare contemplata nel Regolamento, dandone comunicazione direttamente alla famiglia nel caso di infrazione lieve, al Dirigente Scolastico e al Referente Cyberbullismo nel caso di episodi di maggiore gravità.
Per specifiche urgenze, è consentito agli studenti utilizzare l'apparecchio telefonico della scuola, previa autorizzazione degli insegnanti e presa in carico di un operatore; allo stesso modo le famiglie possono rivolgersi al numero della scuola per casi di urgente necessità.

4.2 Per i docenti e per il personale della scuola: gestione degli strumenti personali (cellulari, tablet, altro)

Per la realizzazione delle attività didattiche a carattere multimediale è disponibile il parco tecnologico della scuola, da implementare con i dispositivi personali (computer portatili, tablet, fotocamere, smartphone, altro) di concerto con le famiglie, soprattutto nel caso di necessità di collegamento a internet.

Dispositivi di archiviazione esterna di proprietà personale (cd, chiavette usb, dischi fissi portatili) devono essere controllati preventivamente perché la presenza di eventuali virus non danneggino il corredo tecnologico dell'Istituto.

5. Prevenzione, rilevazione e gestione dei casi

La Scuola è una comunità di dialogo, di ricerca, di esperienza sociale, informata ai valori democratici e volta alla crescita della persona in tutte le sue dimensioni. In essa ognuno, con pari dignità e nella diversità dei ruoli, opera per garantire la formazione alla cittadinanza, la realizzazione del diritto allo studio, lo sviluppo delle potenzialità di ciascuno e il recupero delle situazioni di svantaggio, in armonia con i principi sanciti dalla Costituzione e dalla Convenzione internazionale sui diritti dell'infanzia di New York del 20 novembre 1989 e con i principi generali dell'ordinamento italiano di cui al DPR 24 giugno 1998, n. 249.

5.1 Prevenzione

La Scuola realizza una politica interna pro-attiva tesa a creare un ambiente di apprendimento sereno e sicuro in cui sia chiaro sin dal primo giorno di scuola

che (cyber)bullismo, prepotenza, aggressione e violenza non sono permessi e tollerati; un luogo in cui sia possibile parlare di sé e dei propri problemi alla ricerca di soluzioni; un contesto che stimoli ognuno a partecipare attivamente alle azioni finalizzate al contrasto del (cyber)bullismo.

Contrastare il (cyber)bullismo implica la creazione di una comunità solidale, in cui ogni allievo assuma con consapevolezza il diritto di vivere una scuola senza violenza, ma anche la responsabilità di difendere e sostenere i compagni più vulnerabili. Il coinvolgimento dei coetanei è indispensabile per creare un clima di solidarietà, combattere l'omertà e l'indifferenza, incoraggiare le vittime a chiedere aiuto, sottrarre al bullo i potenziali proseliti.

5.2 Rischi

Cyberbullismo: detto anche "bullismo elettronico", è una forma di prepotenza virtuale attuata attraverso l'uso di internet e delle tecnologie digitali. Come il bullismo tradizionale, esso è una forma di prevaricazione e di oppressione reiterata nel tempo, perpetrata da una persona o da un gruppo di persone "più potenti" nei confronti di un'altra percepita come più debole.

A differenza del bullo tradizionale, il cyber-bullo può colpire la vittima in qualsiasi momento e ovunque essa si trovi, rimanendo nell'ombra e contando su un pubblico potenzialmente enorme, quello della rete. L'anonimità della persona e dei gesti che compie può spingerlo a colpire in modo ancora più duro. E le conseguenze possono essere gravi e persistenti come nel bullismo tradizionale, anche se non avviene alcun contatto fisico.

Adescamento on line: la Rete non è una "giungla" abitata da criminali che adescano i ragazzi, ma possono accadere episodi spiacevoli. Certi "amici" potrebbero essere tutt'altro che quello che dicono di essere. E bisogna insegnare ai ragazzi come tenerli bene alla larga.
L'adescamento online o anche "**grooming**", si verifica quando un adulto manifesta un interesse sessuale inadeguato nei confronti di un minore e lo approccia online con l'intenzione di iniziare una relazione o avere incontri di persona. A volte i minori non sono vittime passive. Può accadere che loro stessi facciano un uso di Internet inadeguato, cercando stimoli di natura sessuale e andando incontro a situazioni di rischio. Questo può succedere molto più spesso se i ragazzi non hanno ricevuto un'adeguata educazione all'affettività e alla sessualità.

Sexting: parola sincretica che unisce i termini inglesi sex e texting, rappresenta la pratica di inviare o postare messaggi di testo (SMS, ma anche messaggi

tramite whatsapp e chat) e immagini a sfondo sessuale, come foto di nudo o semi-nudo, via cellulare o tramite Internet. Tutte le immagini spedite via telefono cellulare o postate online, sono praticamente impossibili da eliminare in forma definitiva e restano nella rete anche dopo la loro cancellazione. Chiunque potrebbe averle scaricate o anche condivise con altre persone, creando pregiudizio grave all'immagine del proprietario di tali documenti.

Pornografia infantile: si intende con questo termine ogni tipo di materiale che rappresenti visivamente un bambino in atteggiamenti sessualmente espliciti, reali o simulati. Ma anche qualsiasi rappresentazione degli organi sessuali di un bambino per scopi essenzialmente sessuali. Produrre questo materiale, e soprattutto diffonderlo, è reato penale. Ed espone la persona ritratta al rischio di un utilizzo improprio delle immagini da parte di altri.

Gioco d'azzardo: è raro, ma la rete può portare a una vera e propria dipendenza chiamata "Internet addiction". I ragazzi che ne soffrono sono spesso inconsapevoli ma, lontani dalla rete, manifestano presto insofferenza, irascibilità e altri sintomi di disagio. Rispetto alle dipendenze legate a Internet, quella da giochi d'azzardo online presenta una serie di problematiche peculiari.

Dipendenza da Internet: può essere una vera e propria sindrome, riguarda ragazzi e ragazze che non riescono a fare a meno della rete e, una volta privati di essa, provano un forte disagio che non attenuano in alcun altro modo. Al di là della patologia, piuttosto rara o molto estrema, un abuso di Internet e delle tecnologie è sempre negativo.
Non è solo un discorso di ore passate davanti al computer. Internet dovrebbe avere un utilizzo "integrativo", che incentivi e accompagni le attività dei ragazzi nel mondo reale: divertirsi con gli amici, coltivare hobby, innamorarsi, fare sport… Se la rete ha invece un ruolo "sostitutivo", è un problema e bisognerebbe intervenire.

Esposizione a contenuti dannosi: navigando i ragazzi possono imbattersi in contenuti non adatti al loro livello di maturità. Immagini violente, pornografiche, a sfondo razzista, ma anche informazioni non corrette che essi potrebbero non essere in grado di leggere in chiave critica. Questo evento potrebbe turbarli o, in alcuni casi, trascinarli in una situazione di pericolo.

5.3 Azioni

La Scuola si propone di aiutare gli studenti a prevenire e riconoscere alcuni tra i più comuni pericoli che si possono incontrare nel web, offrendo strumenti di

supporto all'azione di contrasto. Per prevenire i rischi connessi alla navigazione in rete sia a casa che nell'ambiente scolastico, essa propone le seguenti azioni:

- Informare i minori circa le opportunità e i rischi dei nuovi media;
- Aiutarli a entrare in contatto con i loro sentimenti e ad esprimerli;
- Riaffermare sistematicamente l'importanza della riservatezza dei propri dati personali;
- Rendere i ragazzi consapevoli delle impostazioni sui livelli di privacy dei profili social e dell'importanza di non inserire mai dati identificabili e rintracciabili;
- Sollecitare a non inviare fotografie proprie e di altre persone;
- Rispettare in internet le persone diverse per nazionalità, cultura, religione, sesso: il razzismo e ogni tipo di discriminazione sociale non sono ammessi;
- Ricordare ai ragazzi l'importanza di aggiornare costantemente le password e di condividerle con i genitori;
- Ricordare ai minori che se dovessero verificarsi situazioni che li mettano a disagio, è importante che ne parlino con un adulto o un amico;
- Mostrare le possibilità didattiche e formative delle TIC, perché esse divengano strumento efficace di studio e di lavoro;
- Proporre agli alunni attività di ricerca di informazioni in rete e guidarli opportunamente nella scelta dei siti e nell'utilizzo delle parole chiave.

5.4 Rilevazione e gestione

In caso di episodi di bullismo, cyberbullismo, sexting, utilizzo improprio di foto o dati personali, ecc, il coordinatore di classe prenderà in esame la situazione, ascolterà gli interessati e cercherà di comprendere la diversa gravità dei fatti.

Segnalerà quindi gli eventi al Dirigente Scolastico e al Referente Cyberbullismo, i quali valuteranno la situazione e successivamente convocheranno i genitori.
Nei casi meno gravi i ragazzi saranno guidati in una riflessione personale e/o collettiva per aiutarli a prendere coscienza dell'errore.
Nei casi più gravi si procederà a termini di Regolamento per l'individuazione e l'applicazione delle sanzioni disciplinari.
Di fronte a situazioni che prefigurino reati civili e penali l'Istituto informerà gli Organi di competenza e procederà come previsto dalla legge 71/2017.

Nelle procedure descritte ci si potrà avvalere dei protocolli suggeriti dalla piattaforma messa a disposizione da Generazioni Connesse, come da schema allegato:

Sicurezza in rete - Schema per la scuola

Cosa fare in caso di... cyberbullismo?

Alunno/a preso in giro/minacciato/offeso online

- Se gli alunni coinvolti sono d'accordo, **informa** i genitori
- **Coinvolgi** il referente di istituto dell'e-safety e gli operatori scolastici su quanto sta accadendo
- **Segnala** alla **polizia postale** [segnala: a) contenuto b) modalità di diffusione].
- **Coinvolgi** la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online
- **Tieni traccia** di quanto successo e delle azioni intraprese: **compila il diario di bordo**

- **Dialoga** (con la classe - 1): Parla del cyberbullismo e delle sue conseguenze (non nominare gli alunni coinvolti). Insegna loro a **chiedere aiuto** per situazioni di questo tipo.
- **Dialoga** (con la classe - 2): Chiedi agli alunni coinvolti di intervenire per far terminare le prese in giro: il loro silenzio asseconda quanto sta accadendo.
- Parla della necessità di **non diffondere** ulteriormente online i materiali.
- Informa gli alunni su ciò che dice la **legge italiana** sul cyberbullismo, che è reato.
- **Previeni** (con la classe - 3): Proponi attività in classe sull'empatia e sul riconoscimento delle emozioni (proprie e altrui)
- Quando il cyberbullismo termina, coinvolgi il team e-safety sulle **azioni** appropriate per prevenire altre situazioni di rischio

- **La situazione richiede delicatezza**: cerca di capire meglio cosa sta succedendo.
- Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola)

- **Chiedi un consiglio** telefonico alla **helpline** del progetto Generazioni Connesse al numero gratuito **1.96.96**

Sicurezza in rete - Schema per la scuola

Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi

Scuola_____ Anno Scolastico_____

N°	Data	ora	Episodio (riassunto)	Azioni intraprese		Insegnante con cui l'alunno/a si è confidato	Firma
				Cosa?	Da chi?		

5.5 Come segnalare: quali strumenti e a chi

La Scuola provvederà:

- ad attivare una *mail dedicata* alla segnalazione di casi di rischio;
- ad allestire una *Cassetta della Posta* per chi volesse segnalare casi in forma anonima o non disponga di una mail personale;
- a diffondere i servizi di consulenza offerti da *Save the Children e Telefono azzurro*, a disposizione di genitori e alunni.

5.6 Lo Sportello di ascolto

Nell'Istituto è attivo uno sportello di ascolto, gestito da un docente iscritto all'Albo degli Psicologi, che offre l'opportunità ai ragazzi di parlare delle proprie problematiche e di avere un confronto e dei consigli su come affrontare situazioni di disagio e di inadeguatezza.

5.7 La legge 71/2017

Sono state approvate in via definitiva il 17 maggio 2017, le "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo". Pubblicata in Gazzetta Ufficiale il 3 giugno 2017, la legge n. 71/2017 è entrata in vigore il 18 giugno dello stesso anno.

La norma fornisce una **definizione dettagliata del cyber bullismo** come "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" e indica misure di carattere preventivo ed educativo nei confronti dei minori (vittime e autori del bullismo sul web) da attuare in ambito scolastico.

Chi compie atti di bullismo e cyberbullismo è responsabile di reati penali e danni civili

Secondo il codice penale italiano i comportamenti penalmente rilevanti in questi casi sono:

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

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

Vengono riportati di seguito i punti chiave della norma:

- SEGNALAZIONE e RIMOZIONE

Ciascun minore con più di 14 anni, il genitore o chi esercita la responsabilità sul minore, 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 di qualsiasi dato del minore vittima di cyberbullismo. Qualora entro le ventiquattro ore successive la SEGNALAZIONE non vi sia stata alcuna comunicazione da parte del responsabile ed entro le quarantotto ore non abbia provveduto oppure non sia possibile individuare il gestore del sito internet o del social, l'interessato può fare istanza al Garante per la protezione dei dati personali, il quale provvede entro quarantotto ore alla rimozione.

- PREVENZIONE ed EDUCAZIONE NELLE SCUOLE

L'uso consapevole della rete entra a far parte dell'offerta formativa in ogni ordine di scuola. Il Ministero dell'Istruzione adotta delle linee d'orientamento per la prevenzione e il contrasto del fenomeno. Gli uffici scolastici regionali sono chiamati a promuovere progetti elaborati nelle scuole, nonché azioni integrate sul territorio di contrasto del cyberbullismo e di educazione alla legalità. E'

disposto, inoltre, che le istituzioni scolastiche promuovano, nell'ambito della propria autonomia, l'educazione all'uso consapevole della rete internet e ai diritti e doveri ad esso connessi.

- REFERENTE PER OGNI SCUOLA

Ogni istituto deve individuare tra i propri docenti un referente con il compito di coordinare le iniziative di prevenzione e contrasto. In quest'ottica si programmano corsi di formazione per personale scolastico per garantire l'acquisizione di idonee competenze nell'ambito di azioni preventive a sostegno del minore.

- RISORSE POLIZIA POSTALE

Nell'ambito di ciascun programma operativo nazionale sono stanziate ~~idonee~~ risorse alla formazione del personale specializzato nella tutela dei minori sul web. I fondi certi per la Polizia Postale sono destinati all'aggiornamento dei docenti, nell'ottica di individuare un referente cyberbullismo per ogni autonomia scolastica e dare luogo alla formazione continua dedicata agli studenti.

- AMMONIMENTO

Un provvedimento studiato nella logica di educare e responsabilizzare i giovani che, anche solo inconsapevolmente, si rendono attori di comportamenti penalmente perseguibili.

La procedura dell'ammonimento prevede che fino a quando non sia stata proposta denuncia per diffamazione, minaccia o trattamento illecito di dati, il Questore è chiamato a convocare il minore, colpevole verso altri minori, unitamente a un genitore, ammonendo il medesimo.

Il Garante per la protezione dei dati personali ha pubblicato nel sito http://gpdp.it il MODELLO per la segnalazione/reclamo in materia di cyberbullismo da inviare a: cyberbullismo@gpdp.it.

Il modello è riportato a pagina successiva:

Modello semplificato

Modello per segnalare episodi di bullismo sul web o sui social network e chiedere l'intervento del Garante per la protezione dei dati personali

Con questo modello si può richiedere al Garante per la protezione dei dati personali di disporre **il blocco/divieto della diffusione online di contenuti ritenuti atti di cyberbullismo** ai sensi dell'art. 2, comma 2, della legge 71/2017 e degli artt. 143 e 144 del d.lgs. 196/2003

INVIARE A
Garante per la protezione dei dati personali
indirizzo e-mail: cyberbullismo@gpdp.it

IMPORTANTE - La segnalazione può essere presentata direttamente da chi ha un'età maggiore di 14 anni o da chi esercita la responsabilità genitoriale su un minore.

CHI EFFETTUA LA SEGNALAZIONE?

(Scegliere una delle due opzioni e compilare TUTTI i campi)

☐ Mi ritengo vittima di cyberbullismo e **SONO UN MINORE CHE HA COMPIUTO 14 ANNI**	Nome e cognome Luogo e data di nascita Residente a Via/piazza Telefono E-mail/PEC

☐ Ho responsabilità genitoriale su un minore che si ritiene vittima di cyberbullismo	Nome e cognome Luogo e data di nascita Residente a Via/piazza Telefono E-mail/PEC **Chi è il minore vittima di cyberbullismo?** Nome e cognome Luogo e data di nascita Residente a Via/piazza

IN COSA CONSISTE L'AZIONE DI CYBERBULLISMO DI CUI TI RTIENI VITTIMA?

(indicare una o più opzioni nella lista che segue)

☐ pressioni
☐ aggressione
☐ molestia
☐ ricatto
☐ ingiuria
☐ denigrazione
☐ diffamazione
☐ furto d'identità (es: qualcuno finge di essere me sui social network, hanno rubato le mie password e utilizzato il mio account sui social network, ecc.)
☐ alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali (es: qualcuno ha ottenuto e diffuso immagini, video o informazioni che mi riguardano senza che io volessi, ecc.)
☐ qualcuno ha diffuso online dati e informazioni (video, foto, post, ecc.) per attaccare o ridicolizzare me, e/o la mia famiglia e/o il mio gruppo di amici

QUALI SONO I CONTENUTI CHE VORRESTI FAR RIMUOVERE O OSCURARE SUL WEB O SU UN SOCIAL NETWORK? PERCHE' LI CONSIDERI ATTI DI CYBERBULISMO?

(Inserire una sintetica descrizione – **IMPORTANTE SPIEGARE DI COSA SI TRATTA**)

_____

_____

_____

_____

_____

DOVE SONO STATI DIFFUSI I CONTENUTI OFFENSIVI?

☐ sul sito internet [è necessario indicare l'indirizzo del sito o meglio la URL specifica]
_____

☐ su uno o più social network [specificare su quale/i social network e su quale/i profilo/i o pagina/e in particolare] _____

☐ altro [specificare] _____

Se possibile, allegare all'e-mail immagini, video, screenshot e/o altri elementi informativi utili relativi all'atto di cyberbullismo e specificare qui sotto di cosa si tratta.

1) _____
2) _____
3) _____

HAI SEGNALATO AL TITOLARE DEL TRATTAMENTO O AL GESTORE DEL SITO WEB O DEL SOCIAL NETWORK CHE TI RITIENI VITTIMA DI CYBERBULLISMO RICHIEDENDO LA RIMOZIONE O L'OSCURAMENTO DEI CONTENUTI MOLESTI?

☐ Si, ma il titolare/gestore non ha provveduto entro i tempi previsti dalla Legge 71/20017 sul cyberbulllismo [allego copia della richiesta inviata e altri documenti utili];

☐ No, perché non ho saputo/potuto identificare chi fosse il titolare/gestore

HAI PRESENTATO DENUNCIA/QUERELA PER I FATTI CHE HAI DESCRITTO?

☐ Si, presso _____;

☐ No

Luogo, data Nome e cognome

Informativa ai sensi dell'art. 13 del Codice in materia di protezione dei dati personali

Il Garante per la protezione dei dati personali tratterà i dati personali trasmessi, con modalità elettroniche e su supporti cartacei, per lo svolgimento dei compiti istituzionali nell'ambito del contrasto del fenomeno del cyberbullismo. Il loro conferimento è obbligatorio ed in assenza degli stessi la segnalazione/reclamo potrebbe non poter essere istruita. I dati personali potrebbero formare oggetto di comunicazione ai soggetti coinvolti nella trattamento dei dati personali oggetto di segnalazione/reclamo (con particolare riferimento a gestori di siti internet e social media), all'Autorità giudiziaria o alle Forze di polizia ovvero ad altri soggetti cui debbano essere comunicati per dare adempimento ad obblighi di legge. Ciascun interessato ha diritto di accedere ai dati personali a sé riferiti e di esercitare gli altri diritti previsti dall'art. 7 del Codice.