Costruiamo Futuro

Ministero dell'Istruzione
Università e Ricerca

ISTITUTO COMPRENSIVO
"MARTIN LUTHER KING"

VIA LEONE XIII - CALTANISSETTA

DOCUMENTO
E-SAFETY POLICY

Generazioni Connesse
SAFER INTERNET CENTRE

Indice

Capitolo 1

INTRODUZIONE

La Policy di e-safety è un documento autoprodotto dalla scuola, sulla base dell'indice ragionato messo a disposizione da Generazioni Connesse, sito del progetto Safer Internet Center per l'Italia, volto a descrivere una nuova visione del fenomeno della rete, le norme comportamentali e 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 responsabile delle tecnologie digitali.
La policy di e-safety dell'Istituto Comprensivo Martin Luther King è un lavoro destinato ad un maggiore approfondimento, per questo potrà essere revisionato annualmente da un gruppo di docenti formato sulle tematiche presenti nella policy.

1.1 SCOPO DELLA POLICY

L'intento del nostro Istituto è quello di promuovere liuso da parte degli alunni delle tecnologie digitali e di internet in modo responsabile, di far acquisire competenze e corrette norme comportamentali, di prevenire e gestire problematiche che derivano da un utilizzo pericoloso o dannoso delle tecnologie digitali.
I nostri allievi dimostrano un'innata predisposizione all'uso delle tecnologie, tuttavia, troppo spesso,a questa abilità si oppone una incapacità, dovuta alla giovane età, di non interpretare bene tutte le informazioni a cui, incessantemente, sono sottoposti, soprattutto attraverso l'uso dei social network. Pertanto la scuola attua parallelamente attività di prevenzione, controllo e formazione di docenti, allievi e famiglie.
L'uso delle nuove tecnologie, se non adeguatamente usati, può trasformarsi in una trappola attraverso cui i giovani possono diventare vittime o carnefici di cyberbullismo.
Dunque, la policy di e-safety nasce dalla rilevazione di questo bisogno ed è volto a definire:

- norme comportamentali e procedure per l'utilizzo delle tecnologie nell'ambito dell'Istituto;
- misure per la prevenzione e per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

Il Dirigente Scolastico, i docenti e l'Animatore Digitale hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di internet anche a casa, per prevenire il verificarsi di situazioni pericolose.
Per l'elaborazione del presente documento ci si è avvalsi del materiale bibliografico, reperibile in rete e messo a disposizione da Generazioni Connesse.

1.2 RUOLI E RESPONSABILITÀ

Nell'ambito di questa policy sono individuati i seguenti ruoli e le principali responsabilità correlate:
Genitori: devono contribuire, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete; incoraggiare l'impiego delle TIC da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza; agire in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite;
Dirigente scolastico: deve garantire la sicurezza (tra cui la sicurezza online) dei membri della comunità scolastica, offrire a tutti gli insegnanti una formazione adeguata in merito a un utilizzo positivo e responsabile delle TIC, seguire le procedure previste dalle norme in caso di reclami o

attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola;
Animatore digitale, collaboratore del dirigente e responsabile del laboratorio di informatica: cercano di stimolare la formazione interna all'istituto negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi online e alle misure di prevenzione e gestione degli stessi, monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola,nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola, assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);
Direttore dei servizi generali e amministrativi: deve assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni; prevedere interventi di personale tecnico di assistenza per la soluzione di problematiche relative alla rete e all'uso del digitale segnalate dai docenti; garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet;
Docenti: devono informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento; garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi; garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet; garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali; assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente; controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito); nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei.
Infine non va sottovalutato il ruolo degli **studenti** come primi attori del percorso di acquisizione della capacità di positiva gestione delle proprie competenze digitali: in tale ottica si rende indispensabile coinvolgere anche i più giovani, non solo quali destinatari, ma anche interlocutori attivi e propositivi di tutte le azioni e gli interventi volti alla piena attuazione della Policy.
In particolare, il ruolo degli alunni include i seguenti compiti:

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

1.3 CONDIVISIONE E COMUNICAZIONE DELLA POLICY ALL'INTERA COMUNITÀ SCOLASTICA

1. Condivisione e comunicazione della Policy agli alunni:

- all'inizio dell'anno, in occasione dell'illustrazione del regolamento d'istituto agli alunni da parte dei docenti, verrà presentata la policy, insieme ai regolamenti correlati;
- nel corso dell'anno saranno dedicate da ciascun docente alcune lezioni sulle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al cyberbullismo.

2. Condivisione e comunicazione della Policy al personale:

Le norme adottate dalla scuola in materia di sicurezza nell'utilizzo del digitale saranno discusse negli organi collegiali (collegio docenti, riunioni di dipartimento, consigli di classe) e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito web della scuola;
Il personale della scuola riceverà un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso materiali resi disponibili anche sul sito web della scuola.

3. Condivisione e comunicazione della Policy ai genitori:

- Le famiglie saranno informate in merito alla linea di condotta adottata dalla scuola per un uso sicuro e responsabile delle tecnologie digitali e di internet attraverso la condivisione del presente documento e di materiali informativi specifici sul sito web della scuola;
- al fine di sensibilizzare le famiglie sui temi dell'uso delle TIC saranno organizzati dalla scuola incontri informativi, durante i quali si farà riferimento alla presente policy.

1.4 GESTIONE DELLE INFRAZIONI ALLA POLICY

Tutte le infrazioni alla presente Policy andranno tempestivamente segnalate al Dirigente Scolastico, che avrà cura di convocare le parti interessate onde valutare le possibili azioni da intraprendere.

1. Infrazioni degli alunni

È bene che i docenti introducano attività laboratori ali miranti a sviluppare nei loro alunni una sempre maggiore consapevolezza dei rischi legati a un uso imprudente e improprio del web e che forniscano loro, ogni qualvolta avvenga un'infrazione alle regole stabilite, gli strumenti per affrontare le conseguenze dei loro errori.
I provvedimenti disciplinari da adottare da parte del consiglio di classe nei confronti dell'alunno che ha commesso un'infrazione alla policy (in proporzione sia all'età dello studente sia alla gravità dell'infrazione commessa) saranno i seguenti:
- richiamo verbale;
- sanzioni estemporanee commisurate alla gravità della violazione commessa (assegnazione di attività aggiuntive da svolgere a casa su temi di Cittadinanza e Costituzione; divieto temporaneo di prendere parte alla ricreazione e simili);
- nota informative sul diario ai genitori;
- convocazione dei genitori per un colloquio con l'insegnante;
- convocazione dei genitori per un colloquio con il Dirigente scolastico.

2. Infrazioni del personale scolastico

Le infrazioni alla policy da parte del personale scolastico possono riguardare sia la mancata osservanza delle regole qui descritte sulla gestione della strumentazione, sia la mancata sorveglianza e pronto intervento nel caso di infrazione da parte degli alunni.

3. Infrazioni dei genitori

Compito precipuo dei genitori è supportare gli insegnanti e il personale scolastico nel riconoscimento e nella costruzione di azioni di contrasto efficacia i principali rischi rappresentati dalla navigazione in internet di utenti molto giovani e spesso poco accorti.
Nel caso di infrazione si prevedono interventi, rapportati alla sua gravità, che vanno dalla semplice comunicazione del problema, alla convocazione da parte dell'insegnante di classe o del Dirigente Scolastico.

Capitolo 2

FORMAZIONE E CURRICULO

Per competenze digitali si intendono competenze che abilitano allo studio, e , in prospettiva futura, al lavoro, in maniera aumentata, potenziata, sfruttando le tecnologie per i propri obiettivi, le proprie aspirazioni, i propri interessi personali.
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, al progetto "Generazioni Connesse", coordinato dal MIUR, in partenariato col Ministero dell'Interno-Polizia Postale e delle Comunicazioni e ha già stilato un Piano d'Azione.

2.1 CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI

La Raccomandazione del Parlamento Europeo e del Consiglio del 18 dicembre 2006 relativa alle competenze chiave per l'apprendimento permanente (2006/962/CE), individua la competenza digitale, ovvero il "saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione."
Su queste indicazioni l'Istituto ha già attivati percorsi rivolti ad alunni sull'uso consapevole delle tecnologie con i seguenti obiettivi:

- promuovere un uso consapevole delle nuove tecnologie;
- sensibilizzare e attivare gli studenti sui rischi e i pericoli derivanti da un uso non corretto dei social network;
- favorire lo sviluppo di una cittadinanza attiva e responsabile;
- educare e sensibilizzare i minori ai rischi associati all'utilizzo di piattaforme di condivisione.
- conoscere e acquisire consapevolezza su natura, ruolo e opportunità delle TSI nel quotidiano;
- distinguere il reale dal virtuale, pur riconoscendone le correlazioni;
- sviluppare le abilità di base nelle TSI (uso del computer per reperire, valutare, conservare,
- produrre, presentare e scambiare informazioni;
- acquisire consapevolezza su come le TSI possono coadiuvare la creatività e l'innovazione;
- riflettere sulle problematiche legate alla validità e all'affidabilità delle informazioni disponibili.

In virtù della valenza trasversale delle competenze digitali, la loro acquisizione verrà promossa attraverso percorsi didattici disciplinari e/o interdisciplinari inerenti diverse aree, coerentemente con gli obiettivi individuati nel curricolo di Istituto.

2.2 FORMAZIONE DOCENTI SULL'UTILIZZO CONSAPEVOLE E SICURO DI INTERNET E DELLE TECNOLOGIE DIGITALI NELLA DIDATTICA

Al fine di promuovere la condivisione di buone pratiche per un uso consapevole e sicuro delle TIC nella didattica, e di prevenire e contrastare "ogni forma di discriminazione e del bullismo, anche informatico" [Legge 170/2015, art. 1, c. 7, l], il nostro Istituto ha aderito, quest'anno, al progetto "Generazioni Connesse" (SIC ITALY II), coordinato dal MIUR, in partenariato col Ministero dell'Interno-Polizia Postale e delle Comunicazioni e stilato un Piano d'azione con le seguenti priorità:

- analizzare il fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica;
- promuovere la partecipazione del corpo docente ai corsi di formazione sull'utilizzo e l'integrazione delle TIC nella didattica;
- organizzare incontri con esperti;

- organizzare dei laboratori/eventi destinati a docenti, studenti e genitori per sensibilizzare l'intera comunità scolastica sui rischi della navigazione non controllata e su un corretto uso delle tecnologie digitali.

2.3 SENSIBILIZZAZIONE DELLE FAMIGLIE

La scuola darà ampia diffusione, tramite pubblicazione sul sito, del presente documento di policy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso non consapevole e critico del digitale.
Allo scopo di mantenere viva l'attenzione delle famiglie sull'uso responsabile e sicuro delle nuove tecnologie, l'Istituto promuove opportunità di incontro e formazione per le famiglie sui temi oggetto della Policy, offerte dal territorio, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità.

Capitolo 3

GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE TIC DELLA SCUOLA

Accesso a Internet

L'accesso a Internet è possibile nei plessi della scuola secondaria di I grado e nei plessi della scuola primaria sia nei laboratori informatici, presenti in tutti i plessi dell'Istituto, sia nelle aule, dotate di LIM con relativo computer portatile custodito in un cassetto chiuso a chiave. Inoltre, la sede centrale della scuola secondaria è dotata di un'aula attrezzata per cl@ssi 2.0.
Nei laboratori di informatica e nelle aule sono attivi filtri per la navigazione sicura;.
Le impostazioni sono definite e manutenute dall'Animatore digitale e dal responsabile di plesso della sede centrale ed è in carico a ciascun docente la segnalazione di disservizi.

Gestione accessi (password, backup, ecc.)

Nei computer presenti nelle aule e nei laboratori sono previsti tre profili di accesso con relative password:
- amministratore;
- docente;
- alunno.

È possibile effettuare installazioni e aggiornamenti di software solo tramite la password amministratore, fornita al personale di assistenza tecnica e all'Animatore Digitale. E' previsto un backup automatico su server.

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.
I docenti utilizzano per scopi didattici il proprio account su dominio istruzione.it. La posta elettronica è protetta da antivirus e da antispam.

Blog e sito web della scuola

La scuola ha un sito web. Tutti i contenuti del settore didattico sono pubblicati direttamente sotto la supervisione dei responsabili del sito web (Animatore Digitale e responsabile di plesso della sede centrale) che ne valutano con il Dirigente scolastico la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc..

Social network

Attualmente i docenti utilizzano Youtube, social network da cui è possibile reperire videolezioni, film e documentari di interesse esclusivamente didattico e per approfondire alcuni argomenti di particolare importanza. Tutti i contenuti utilizzati su Youtube vengono preventivamente visionati e selezionati dai docenti in termini di sicurezza e di adattabilità alla programmazione scolastica.
In alcuni casi, l'istituzione scolastica, per nome e per conto della stessa, è autorizzata a utilizzare il canale Youtube e la pagina di Facebook per la diffusione e/o pubblicazione di un evento, previa richiesta di autorizzazione e supervisione del Dirigente Scolastico.

Protezione dei dati personali

Il personale scolastico è incaricato del trattamento dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi.
Viene inoltre fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni.

Capitolo 4

STRUMENTAZIONE PERSONALE

Per gli studenti: gestione degli strumenti personali - cellulari, tablets, ecc..

Gli alunni della scuola secondaria di primo grado si impegnano a tenere spenti e custoditi in cartella i telefoni cellulari. Nella scuola primaria si chiede alle famiglie di non lasciare i dispositivi ai propri figli. In caso di urgenza per comunicazioni tra gli alunni e le famiglie, su autorizzazione dei docenti e sotto il diretto controllo dei collaboratori scolastici, gli alunni potranno comunicare con le famiglie tramite gli apparecchi telefonici della scuola.
L'uso di dispositivi personali è consentito per lo svolgimento di attività didattiche programmate dai docenti. Gli alunni con certificazione DSA utilizzeranno gli strumenti compensativi quali tablet e computer portatili sotto stretto controllo dei docenti.

Per i docenti: gestione degli strumenti personali - cellulari, tablets, ecc..

Durante le ore di lezione è consentito ai docenti l'uso di dispositivi elettronici personali, come il tablet, unicamente a scopo didattico e a integrazione dei dispositivi scolastici disponibili (il computer di classe), in special modo per l'utilizzo del registro elettronico.
E' opportuno che ogni insegnante dia chiare informazioni sul corretto utilizzo della rete; segnali eventuali malfunzionamenti o danneggiamenti al tecnico informatico; non salvi dati personali e sensibili.
Durante il restante orario di servizio l'uso del cellulare è consentito solo per comunicazioni personali che rivestano carattere di urgenza, mentre l'uso di altri dispositivi elettronici personali è permesso per attività funzionali all'insegnamento.

Per il personale della scuola: gestione degli strumenti personali - cellulari, tablets, ecc..

Durante l'orario di servizio al restante personale scolastico l'uso del cellulare è consentito per comunicazioni personali urgenti. L'uso di altri dispositivi elettronici personali è permesso solo per attività funzionali al servizio, e preventivamente autorizzato.
Il personale ATA vigila sull'utilizzo non autorizzato delle TIC.

Capitolo 5

PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

Gli operatori scolastici ed in modo particolare gli insegnanti, sono promotori e garanti della costruzione dialogica di un percorso formativo partecipato, e nel loro ruolo diventano confidenti degli alunni e delle loro esperienze. Proprio per questo, gli insegnanti sono spesso i primi a rilevare le problematiche e i rischi che bambini e gli adolescenti possono trovarsi ad affrontare ogni giorno. Si pensi ai numerosi casi di bullismo e di cyberbullismo di cui gli insegnanti vengono a conoscenza e che si trovano ad affrontare durante l'anno scolastico.
E' compito degli insegnanti imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente.
Tra questi, un'attenzione specifica andrà prestata ai fenomeni di bullismo/cyber bullismo quest'ultimo una forma di prepotenza virtuale attuata attraverso l'uso di internet e delle tecnologie digitali), di sexting (pratica di inviare o postare messaggi di testo e immagini a sfondo sessuale, come foto di nudo o semi-nudo, via cellulare o tramite Internet e adescamento o grooming (una tecnica di manipolazione psicologica, che gli adulti potenziali abusanti utilizzano online, per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata) (Glossario di "Generazioni connesse"). Tuttavia in orario scolastico, alcuni studenti, eludono la sorveglianza del personale della scuola, usano il cellulare, non solo per comunicare con i propri genitori, ma anche per navigare su internet, andando su siti non adatti e inviando materiali riservati (foto, video e altro). Così facendo, gli studenti possono incorrere anche a scuola nei 17 rischi sopra descritti.

Rilevazione
La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti.

<u>Che cosa segnalare</u>

Qualora si riscontri la pubblicazione di:
- dati sensibili o riservati (foto, immagini, video personali, informazioni private proprie o di amici; l'indirizzo di casa o il telefono, ecc.);
- contenuti che possano considerarsi in qualche modo lesivi dell'immagine altrui (commenti
- offensivi, minacce, osservazioni diffamatorie o discriminatorie, foto o video denigratori,
- videogiochi che contengano un'istigazione alla violenza, ecc.);
- contenuti riconducibili alla sfera sessuale: messaggi, immagini o video a sfondo sessuale,
- come foto di nudo o semi-nudo, ecc.
- andranno opportunamente segnalati per gli interventi opportuni.

<u>Come segnalare: quali strumenti e a chi</u>

Il personale della scuola, anche con il supporto tecnico dell'Animatore Digitale, provvederà a conservare le eventuali tracce di una navigazione non consentita su internet o del passaggio di materiali inidonei sui pc della scuola nonché la data e l'ora. Nel caso di messaggi, si cercherà di risalire al mittente attraverso i dati del suo profilo. L'insegnante dovrà copiare e stampare i messaggi per fornire le eventuali prove all'indagine sugli abusi commessi e raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico, alla famiglia ed, eventualmente, alla Polizia Postale. Qualora siano coinvolti più alunni, in qualità di vittime o di responsabili della condotta scorretta, le famiglie degli alunni in questione saranno convocate e informate tempestivamente per un confronto.

In base alla gravità dei fatti si provvederà:
- a una comunicazione scritta tramite diario alle famiglie;
- a una nota disciplinare sul registro on-line;
- a una convocazione formale dei genitori degli alunni, tramite segreteria;
- a una convocazione delle famiglie da parte del Dirigente scolastico;
- per i reati più gravi la scuola si rivolgerà direttamente agli organi di polizia competenti.

Gestione dei casi - Definizione delle azioni da intraprendere a seconda della specifica del caso

La gestione dei casi rilevati va differenziata a seconda della loro gravità; è opportuno condividere ogni episodio con il team docenti. Alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe. In altri è opportuno convocare genitori e alunni per cercare di rimediare all'accaduto. Nei casi più gravi occorre sottoporre all'attenzione del Dirigente Scolastico l'accaduto perché predisponga le azioni da intraprendere.
E' opportuno:
- Promuovere campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni.
- Portare a conoscenza degli alunni che per la legge italiana il cyber-bullismo , la diffusione e il possesso di materiale pornografico è reato e che una foto o un video diffuso in rete potrebbero non essere tolti mai più.
- Sensibilizzare la popolazione studentesca sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione.
- Coinvolgere i genitori per attivare forme di controllo della navigazione e monitorare l'esperienza online dei propri figli.
- Tutelare la privacy e informare sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farli rispettare.
- I docenti, in classe, parlano di bullismo, adescamento, uso sicuro di internet e dei social network, sexting, cyberbullismo e delle conseguenze. Propongono riflessioni sulle menzogne dette per stringere relazioni online.
- Promuovere la consapevolezza e le conoscenze sul cyberbullismo, attraverso corsi di formazione, seminari, dibattiti. E' infatti importante che docenti, personale ATA, genitori e studenti abbiano una chiara e condivisa definizione di cyberbullismo.
- Informare i docenti, il personale ATA ed i genitori sui comportamenti non verbali correlati al cyberbullismo. Gli adulti dovrebbero allertarsi se uno studente, dopo l'uso di internet o del proprio telefonino, mostra stati depressivi, ansiosi o paura.
- Aggiornare il Regolamento di Istituto prevedendo apposite norme in tema di cyberbullismo e navigazione on line sicura. Specificare quando e come si possono utilizzare all'interno della scuola, i computers ed i videotelefonini.
- Segnalare agli alunni l'esistenza di una linea di ascolto attiva tutto l'anno 24 ore su 24 di telefono azzurro che raccoglie richieste di ascolto e di aiuto. Al servizio HOTLINE si possono segnalare, in forma anonima, contenuti pedopornografici e altri contenuti dannosi diffusi dalla rete.

Per tutti i casi che costituiscono reato occorre informare il Dirigente Scolastico per confrontarsi sulle azioni da intraprendere ed eventualmente attivare l' intervento delle forze dell'ordine. Non esistono protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi, tuttavia si praticano forme di collaborazione informale nella prevenzione e contrasto del bullismo e del cyber bullismo con la polizia di stato.

Capitolo 6

AZIONI

L'obiettivo che l'insegnante deve proporsi dopo avere riconosciuto il pericolo è agire di conseguenza, con azioni di contrasto efficaci e mirate, rispetto ai rischi sopra elencati. 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 di volta in volta 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. Le dovute eccezioni (uso del cellulare per comunicazioni alunno-famiglia in occasione di uscite didattiche) andranno espressamente regolamentate e dovranno comunque avvenire sotto la supervisione diretta di un docente responsabile;
- dotare i dispositivi della scuola di filtri che impediscano l'accesso a siti web non adatti ai minori (black list).

Azioni utili a impedire un utilizzo incauto, scorretto o criminoso degli strumenti digitali:
materiali inviati, scaricati, ricevuti o condivisi - su dispositivi digitali in uso a scuola (principalmente pc) sono:

- bloccare l'accesso a un sito o a un insieme di pagine impedendone la consultazione;
- controllare periodicamente i siti visitati dagli alunni;
- utilizzare un software in grado di intercettare le richieste di collegamento e di respingere quelle non conformi alle regole stabilite dall'amministratore;
- affidare a un gruppo di docenti con il supporto dell'animatore, le regole di filtraggio.

Annessi in via di definizione:le procedure operative sono state espresse nel documento, ma saranno oggetto di ulteriore approfondimento e periodica rimodulazione

1. Procedure operative per la gestione delle infrazioni alla Policy
2. Procedure operative per la protezione dei dati personali.
3. Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni.
4. Procedure operative per la gestione dei casi.
5. Protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi

Il referente
Salvatore Falegname

Il Dirigente Scolastico
Rosa Cartella