



ISTITUTO COMPRENSIVO STATALE

“G. Garibaldi” ad indirizzo musicale

Via Portella delle Ginestre, 12 – 92010 – REALMONTE (AG)

(Realmonte- Siculiana- Montallegro- Cattolica Eraclea)

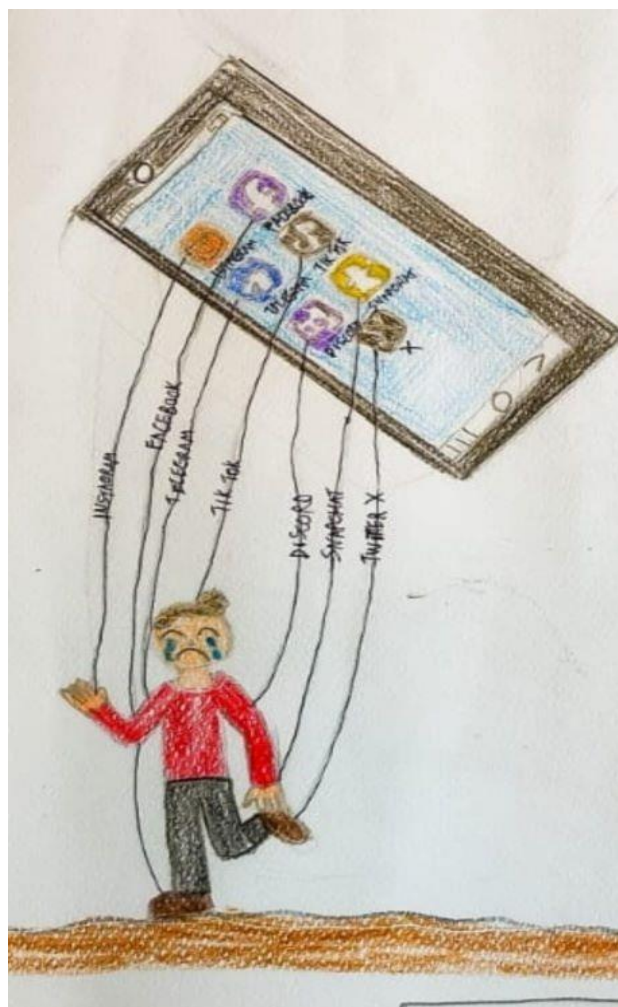
Tel e fax 0922/816434 - Cod. Fisc.: 80004670842

[e.mail: agic819001@istruzione.it](mailto:agic819001@istruzione.it) –

agic819001@pec.istruzione.it



E-SAFETY POLICY



1 PREMESSA

La scuola rappresenta il luogo in cui preadolescenti ed adolescenti sperimentano quotidianamente i processi di apprendimento vivendo straordinarie opportunità di crescita intellettuale, di maturazione, di acquisizione, di consapevolezza critica e responsabilità, ma allo stesso tempo si misurano con le difficoltà, la fatica, gli errori ed i momentanei insuccessi attraverso relazioni con i pari e con gli adulti. Questo è considerato ed identificato come il più critico dei periodi del ciclo della vita, in quanto momento di transizione, di cambiamenti fisici e psichici che spesso sono difficili da accettare e comprendere per i ragazzi che li affrontano. Non sono più bambini, ma neanche completamente adulti e spesso non sanno come muoversi in una realtà che non risparmia critiche e giudizi. È all'interno di questa difficoltà che, sempre più spesso, possono metter in atto condotte a rischio come bullismo e cyberbullismo, autolesionismo – cutting, disturbi dell'alimentazione, vandalismo di gruppo, dipendenza da internet, abuso di sostanze, giochi estremi online. Condotte molto diverse accomunate però dalla stessa importante funzione evolutiva: affermare la propria indipendenza, mettersi alla prova, entrare in relazione con le proprie emozioni. E' in questo senso che il ruolo della famiglia e della scuola risulta fondamentale; insieme devono ascoltare e comprendere disagio e disorientamento, ma anche contrastarne lo sviluppo verso comportamenti pericolosi; devono attivare quei fattori di protezione, ovvero risorse personali ed ambientali che consentono di affrontare situazioni complesse e devono altresì fare il possibile per disattivare quei fattori di rischio che facilitano l'attuazione da parte degli adolescenti di condotte pericolose.

IL BULLISMO è una forma di comportamento sociale di tipo violento ed intenzionale, oppressivo e vessatorio sia di natura fisica che psicologica, ripetuto nel tempo ed attuato nei confronti di persone considerate dal soggetto che perpetra l'atto come bersagli facili e/o impossibilitati a difendersi.

È tipico dell'età preadolescenziale ed adolescenziale e spesso viene messo in atto nella scuola. Si presenta in modi diversi e va distinto dal semplice scherzo e/o "ragazzata". È caratterizzato da:

- **PIANIFICAZIONE:** Il bullo sceglie attentamente la vittima tra i compagni più timidi ed isolati per ridurre il rischio di possibili ritorsioni, aspetta con pazienza un momento di ridotta vigilanza dell'adulto ed agisce con l'intenzione di nuocere;
- **POTERE:** il bullo è più forte della vittima, non tanto per forza fisica ma soprattutto dal

punto di vista sociale in quanto ha un gruppo di amici-complici con cui agisce, mentre la vittima è sola, vulnerabile ed incapace di difendersi;

- RIGIDITÀ DEI RUOLI: i ruoli di bullo e vittima sono rigidamente assegnati;
- GRUPPO: gli atti di bullismo vengono sempre compiuti in gruppi più o meno numerosi;
- PAURA: sia la vittima che gli spettatori passivi, ovvero i compagni che assistono agli episodi, hanno paura, temono che parlando la situazione possa solo peggiorare e portare a ritorsioni. Pensano che sia meglio subire in silenzio.

L'atto di bullismo può manifestarsi in forma:

- FISICA: atti aggressivi diretti (calci, pugni etc.), danneggiamento delle cose altrui, furto intenzionale;
- VERBALE: in maniera manifesta (deridere, umiliare, svalutare, criticare, accusare) o nascosta (diffondere voci false ed offensive, provocazioni);
- RELAZIONALE: sociale (esclusione di un compagno dalle attività di gruppo) o manipolativa (rompere i rapporti di amicizia di cui gode la vittima);

IL CYBERBULLISMO si manifesta come una forma di bullismo perpetrato attraverso la rete internet con la diffusione sui social network di messaggi offensivi, video e foto denigratori, tramite la creazione di gruppi contro.

Sono molto spesso messaggi di intolleranza e non accettazione verso chi è diverso per etnia, per religione, per genere e per identità di genere, per caratteristiche psico-fisiche, per particolari realtà familiari, verso chi non si allinea a stereotipi estetici, alimentando pregiudizi e disinformazione con la creazione di fake-news. Gli studenti attuali, se da una parte hanno una estrema competenza tecnica non hanno altrettanta consapevolezza delle conseguenze a cui porta un uso malevolo delle competenze digitali, anche se non sempre il confine tra premeditazione e incompetenza sia così facile da individuare. Il cyberbullo agisce nell'anonimato e lo sviluppo delle tecnologie gli permette di infiltrarsi nella vita della vittima con estrema facilità e rapidità. Spesso gli adulti di riferimento non sono all'altezza di verificare le attività in rete.

I TRATTI DISTINTIVI del Cyberbullismo sono:

- ANONIMATO: il bullo si nasconde dietro un nome falso, un nickname ritenendo ingenuamente di non poter essere scoperto;
- ASSENZA DI RELAZIONE: tra vittima e bullo, ma non si esclude che il bullo possa anche essere qualcuno di molto vicino alla vittima;

- MANCANZA DI FEEDBACK EMOTIVO: a volte non vedendo le reazioni della vittima il cyberbullo non è completamente consapevole del danno che arreca e questo fa abbassare i suoi livelli di autocontrollo;

Rientrano nel CYBERBULLISMO:

- FLAMING: messaggi online violenti e volgari mirati a suscitare battaglie verbali in un forum;
- HARASSMENT(molestie): spedizione ripetuta di messaggi insultanti mirati a ferire qualcuno tramite email, sms, mms, pubblicazioni su blog, forum;
- CYBERSTALKING: invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità;
- DENIGRATION: pubblicazione all'interno di comunità virtuali di pettegolezzi e commenti crudeli, calunniosi, denigratori, al fine di danneggiare la reputazione della vittima;
- EXCLUSION: escludere deliberatamente una persona da un gruppo on line per provocare in essa un sentimento di emarginazione;
- TRICKERY(inganno): ottenere la fiducia di qualcuno con l'inganno per poi pubblicare o condividere con altri le informazioni ottenute in via confidenziale, attraverso la pubblicazione di audio e video;
- IMPERSONATION: (furto di identità): violare un account e accedere in modo non autorizzato a programmi e contenuti appartenenti alla persona intestataria dello stesso.
- SEXTING: invio di messaggi corredati da immagini, audio o video a sfondo sessuale via smartphone ed internet.

1.1 Riferimenti normativi.

- Articoli 3, 33,34 della Costituzione Italiana;
- Direttiva MIUR n.16 del 5\2\2007 recante “Linee di indirizzo generali ed azioni a livello nazionale per la prevenzione e la lotta al bullismo”;
- Direttiva MPI n.30 del 15\3\2007 recante “Linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità dei genitori e dei docenti”;
- Direttiva MPI n.104 del 30\11\2007 recante “Linee di indirizzo e chiarimenti interpretativi ed applicativi in ordine alla normativa vigente posta a tutela della privacy con particolare riferimento all'utilizzo di telefoni cellulari o di altri dispositivi elettronici

nelle comunità scolastiche allo scopo di acquisire e/o divulgare immagini, filmati o registrazioni vocali”;

□ Direttiva MIUR n. 1455\06 □ DPR 249\98 e 235\2007 recante “Statuto delle studentesse e degli studenti”;

□ Delle linee di orientamento per azioni di prevenzione e di contrasto al bullismo ed al cyber bullismo. MIUR aprile 2015;

□ Artt.581,582,594,595,610,612,635 del CODICE PENALE □ Artt. 2043,2047,2048 del CODICE CIVILE □ Legge 29\5\2017 n. 71.

1.2 Integrazione della Policy con Regolamenti esistenti.

Il presente documento integra per obiettivi e contenuti i documenti che specificano le politiche dell’Istituto:

- PTOF, incluso il piano per l’attuazione del PNSD;
- Regolamento interno d’istituto;
- Regolamento per l’utilizzo dei laboratori di informatica;

2 RUOLI E RESPONSABILITÀ

Il nostro Istituto, nel suo fermo rifiuto di ogni forma di sopraffazione, prepotenza, esclusione coinvolge l’intera comunità educante nell’opera di riconoscimento, prevenzione, contrasto dei comportamenti a rischio, per il raggiungimento del benessere nella vita scolastica, per il supporto al superamento delle difficoltà in una condivisione di intenti e proposte.

Dirigente scolastico:

□ Adotta e sostiene una politica scolastica che faciliti il riconoscimento del bullismo, del cyberbullismo e delle condotte a rischio, attivando progetti di prevenzione e contrasto dei fenomeni;

□ Prevede azioni culturali ed educative rivolte agli studenti per acquisire le competenze necessarie all’esercizio di una cittadinanza digitale consapevole;

□ Favorisce la discussione all’interno dell’istituto, attraverso i vari organi collegiali, creando i presupposti di regole condivise di comportamento per il contrasto dei fenomeni sopraindicati;

- ☐ Individua un docente in qualità di referente d'Istituto e di un gruppo di lavoro per la prevenzione ed il contrasto al bullismo e al cyberbullismo e alle condotte a rischio;
- ☐ Promuove azioni di sensibilizzazione dei fenomeni nel territorio in rete con Enti, associazioni, istituzioni, coinvolgendo l'intera comunità scolastica;
- ☐ Si attiva per la predisposizione di uno sportello ascolto con la collaborazione di qualificato personale esterno;
- ☐ Prevede all'interno del PTOF triennale corsi di aggiornamento e formazione in materia di prevenzione dei fenomeni di bullismo, cyberbullismo rivolti al personale docente ed ATA;
- ☐ Predispone sul sito della scuola uno spazio dedicato al tema in cui raccogliere materiale informativo e di restituzione delle attività svolte dalla scuola nell'ambito della prevenzione;
- ☐ Qualora venga a conoscenza di atti di cyberbullismo (salvo il fatto che in esso si riscontrino reati) informa tempestivamente i soggetti che esercitano la responsabilità genitoriale o i tutori dei minori coinvolti ed attiva adeguate azioni di carattere educativo.

Referente cyberbullismo d'Istituto:

- ☐ Promuove la conoscenza e la consapevolezza del bullismo, del cyberbullismo e dei comportamenti a rischio attraverso progetti di istituto che coinvolgano genitori, studenti e tutto il personale;
- ☐ Coordina le attività di prevenzione ed informazione delle sanzioni previste e sulle responsabilità di natura civile e penale;
- ☐ Compila un registro per tenere traccia di tutte le segnalazioni e, se necessario, chiede supporto alle Associazioni territoriali o alla Polizia Postale;
- ☐ Si rivolge a partner esterni alla scuola, quali servizi sociali e sanitari, aziende del privato sociale, forze di polizia per realizzare un progetto di prevenzione;
- ☐ Cura i rapporti di rete fra scuole per eventuali convegni, seminari etc. e per la partecipazione alla giornata mondiale sulla Sicurezza in internet (Safer Internet Day);
- ☐ Si attiva per un monitoraggio finalizzato a fornire una fotografia della situazione presente nella scuola e consentire una valutazione oggettiva degli interventi attuati.

Animatore Digitale e Team dell'Innovazione:

- ☐ Pubblicano il documento di E-Safety Policy sul sito della scuola;
- ☐ Diffondono i contenuti del documento tra docenti e studenti.

L'Animatore digitale supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento:

- ai rischi online,
- alla protezione e gestione dei dati personali,
- all'organizzazione di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica);
- al monitoraggio e rilevamento di eventuali episodi o problematiche connesse all'uso delle TIC a scuola,
- al controllo che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

Collegio dei Docenti:

- ☐ Promuove scelte didattiche ed educative in continuità e congruenza tra i vari ordini ed in collaborazione con altre scuole in rete per la prevenzione.

Consiglio di Classe, Interclasse ed Intersezione

- ☐ Pianifica attività didattiche e/o integrative finalizzate al coinvolgimento attivo e collaborativo degli studenti ed all'approfondimento di tematiche che favoriscano la riflessione e la presa di coscienza della necessità dei valori della convivenza civile;
- ☐ Favorisce un clima collaborativo all'interno della classe e nelle relazioni con le famiglie e propone progetti di educazione alla legalità ed alla cittadinanza attiva
- ☐ Si riunisce per valutare l'applicazione di eventuali provvedimenti in base alla gravità delle infrazioni.

Docenti:

- ☐ Intraprendono azioni congruenti con l'utenza del proprio ordine di scuola sia nell'acquisizione e nel rispetto delle norme legate al vivere civile che nella trasmissione dei valori legati ad un uso responsabile della rete;
- ☐ Valorizzano nell'attività didattica metodologie di lavoro di tipo cooperativo, di peer education, mediazione, gruppi di discussione, role playing, con modalità adeguate all'età;

- ☐ Monitorano atteggiamenti preoccupanti dandone comunicazione al Dirigente Scolastico;
- ☐ Si impegnano a rimanere aggiornati sulle tematiche del bullismo, del cyberbullismo e dei comportamenti a rischio anche attraverso la frequenza a corsi di aggiornamento proposti dalla scuola o dall'ambito territoriale di appartenenza

Alunni:

- ☐ Imparano le regole basilari di comportamento (netiquette) quando sono collegati in rete facendo attenzione alle comunicazioni che inviano;
- ☐ Sono coinvolti nella progettazione e nella realizzazione di iniziative scolastiche al fine di favorire un migliorato benessere nello stare a scuola;
- ☐ Si impegnano a diffondere buone pratiche nel rispetto dei diritti di ogni membro della comunità scolastica ed extrascolastica;
- ☐ Sono consapevoli che il Regolamento di istituto limita l'utilizzo degli smartphone all'interno dell'istituto;
- ☐ Sono consapevoli che non è loro consentito, all'interno della scuola, acquisire e divulgare immagini, video e messaggi vocali relativi al personale docente e non docente e relativi ai compagni della propria o di altre classi, neanche negli spostamenti da o per i vari ambienti del plesso, inclusi gli spazi esterni all'edificio scolastico.
- ☐ Sono comprese in questo divieto anche le attività didattiche esterne alla scuola ed i viaggi di istruzione di uno o più giorni, nel rispetto del diritto alla riservatezza di tutti;
- ☐ Sono a conoscenza del diritto\dovere di segnalare al Dirigente Scolastico, al referente del Bullismo, allo psicologo dello sportello, ai docenti, eventuali atti di cui sono a conoscenza, consapevoli del fatto che verrà loro garantita completa riservatezza di quanto comunicato;
- ☐ Sono consapevoli dei reati che si configurano con atti di bullismo e cyberbullismo e delle conseguenze in materia legale.

Tecnico informatico:

- ☐ Può controllare ed accedere a tutti i files della intranet;
- ☐ Limita attraverso un proxy l'accesso ad alcuni siti;
- ☐ Consiglia modalità sull'utilizzo dei laboratori, come la prenotazione degli stessi che consentirà di tenere traccia di ora e giornata ed eventuali anomalie riscontrate da ciascuno.

Direttore dei Servizi Generali e Amministrativi:

- ☐ assicura, nei limiti delle risorse finanziarie disponibili, gli interventi di

manutenzione necessari ad evitare un cattivo funzionamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate.

Collaboratori Scolastici

☐ Garantiscono la vigilanza e la segnalazione ai docenti dell'eventuale uso improprio dei dispositivi personali degli alunni negli spazi comuni, negli spostamenti da o per i vari ambienti del plesso, inclusi gli spazi esterni all'edificio scolastico.

Genitori:

- ☐ Partecipano attivamente alle azioni di formazione \informazione istituite dalla scuola;
- ☐ Sono attenti ai comportamenti dei propri figli;
- ☐ Vigilano sull'uso delle tecnologie da parte dei ragazzi, stabilendo regole e direttive precise, con particolare attenzione alle modalità, agli atteggiamenti, ai tempi di uso;
- ☐ Conoscono le azioni messe in campo dalla scuola, ne condividono gli intenti e collaborano secondo le modalità previste dal patto di corresponsabilità:
- ☐ Conoscono il regolamento disciplinare d'istituto;
- ☐ Conoscono le sanzioni previste dal regolamento disciplinare d'istituto in caso di cyber bullismo e bullismo e uso del cellulare.

3 GESTIONE DELLE INFRAZIONI ALLA POLICY.

Nel caso si verificano azioni riscontrabili e riferibili a bullismo e cyberbullismo così come descritto nei capitoli dedicati, si dovrà immediatamente avviare una procedura al termine della quale verranno stabiliti degli interventi disciplinari. Tutti gli eventi configurabili in azioni di bullismo e cyberbullismo sono da considerare infrazione grave al Regolamento disciplinare d'Istituto. Nel caso del bullismo anche la condotta dei compagni sostenitori del bullo verrà considerata deplorable.

Gli episodi di bullismo e cyberbullismo saranno sanzionati, privilegiando sanzioni disciplinari di tipo riparativo e di service learning, convertibili in attività a favore della comunità scolastica.

GESTIONE DELLE INFRAZIONI ALLA E-POLICY

Infrazioni degli alunni

INFRAZIONI	FREQUENZA	PROVVEDIMENTO	ORGANO COMPETENTE
L'alunno non ha il cellulare/smartwatch spento (riceve chiamate o notifica di messaggi)	<u>Prima volta:</u>	Richiamo verbale (con annotazione sul registro di classe) e comunicazione alla famiglia sul diario personale.	Docente
	<u>Seconda volta:</u>	Nota sul registro di classe e sul registro elettronico per dare comunicazione alla famiglia ed intervento del DS/ Responsabile di plesso.	Docente + DS/Responsabile di plesso
	<u>Uso reiterato:</u>	Convocazione della famiglia e in seguito provvedimento disciplinare	Coordinatore del CdC + DS + CdC
L'alunno utilizza dispositivi elettronici per chiamate o messaggi o per altro uso non consentito (giochi, musica, chat, etc.)	<u>Prima volta:</u>	Nota sul registro di classe e sul registro elettronico (con comunicazione alla famiglia sul diario personale) ed eventuale intervento del Dirigente Scolastico/ Responsabile di plesso	Docente /DS / Responsabile di plesso
	<u>Uso reiterato:</u>	Nota sul registro di classe e sul registro elettronico (con comunicazione alla famiglia sul diario personale) ed eventuale intervento del Dirigente Scolastico/ Responsabile di plesso	Coordinatore del CdC + DS + CdC
L'alunno utilizza dispositivi elettronici		Ritiro della verifica; nota sul registro di classe e sul registro	Docente + CdC

durante una verifica scritta		elettronico (con comunicazione alla famiglia sul diario personale)	
L'alunno effettua riprese audio, foto o video senza informarne preventivamente il docente		Nota sul registro di classe e sul registro elettronico, eventuale intervento del Dirigente Scolastico/ Responsabile di plesso Convocazione della famiglia e in seguito provvedimento disciplinare.	Docente + Cdc+ Responsabile di plesso
L'alunno diffonde in modo non autorizzato e/o lesivo audio, foto, video, link, documenti		Nota sul registro di classe e sul registro elettronico, convocazione della famiglia intervento del Dirigente Scolastico e del Consiglio di Classe (provvedimento disciplinare in base alla gravità).	Docente +DS + CdC

Infrazioni dei docenti

La gestione delle infrazioni del personale scolastico ricade nella disciplina contrattuale. In particolare gli insegnanti potrebbero esporre gli alunni al rischio disattendendo le regole sulla gestione della strumentazione e causare danni per la mancanza di intervento tempestivo nel caso di infrazione da parte degli alunni.

4 Formazione e Curricolo

4.1. Curricolo sulle competenze digitali per gli studenti

Nell'ambito del PNSD l'Istituto può proporsi un programma di educazione alla sicurezza on-line da affiancarsi ad una didattica digitale:

- Promuovere una serie di comportamenti "adeguati";
- Appurare l'attendibilità delle informazioni trovate in rete;
- Riportare sempre la fonte delle informazioni pervenute;
- Conoscere e rispettare la netiquette (regole condivise che disciplinano il rapporto tra utenti della rete, i siti e qualsiasi altro tipo di comunicazione);
- Mantenere private le informazioni personali proprie e degli altri;
- Comprendere che le fotografie in rete possono essere manipolate o utilizzate per scopi diversi da quelli per cui sono state pubblicate;
- Comprendere che la rete traccia e tiene memoria di tutto ciò che viene pubblicato;
- Comprendere il motivo per cui non bisogna pubblicare foto o video di altre persone senza il loro consenso;
- Conoscere le conseguenze di azioni sbagliate in rete;
- Conoscere le diverse forme di cyberbullismo e le persone e/o associazioni a cui rivolgersi per chiedere consiglio;
- Rispettare i copyright.

4.2. Formazione dei docenti sull'utilizzo consapevole e l'integrazione delle TIC nella didattica

Le attività di formazione si possono svolgere su diversi livelli:

- ☐ formazione istituzionale, organizzata dal Miur secondo il PNSD, attraverso gli snodi formativi;
- ☐ formazione istituzionale in contrasto al bullismo, attraverso:
- ☐ interventi su classi individuate dalla scuola stessa,
- ☐ interventi che vedono la presenza dell'intera comunità educante, compresi i genitori;
- ☐ la formazione dei referenti di istituto;
- ☐ formazione specifica di Istituto, legata alle esigenze formative rilevate;
- ☐ partecipazione a progetti internazionali con la finalità di condividere materiale e tecniche di prevenzione e gestione di casi di bullismo per possibilità di costruire una conoscenza collaborativa con altri Paesi attraverso la piattaforma e-twinning .

4.3. Sensibilizzazione delle famiglie

Il presente documento verrà pubblicato sul sito ed affiancato da un vademecum per i genitori affinché comprendano i rischi della rete e collaborino proficuamente con il personale della scuola.

I progetti realizzati dagli studenti verranno pubblicati sul sito della scuola nella giornata mondiale della sicurezza in rete al fine di mettere in evidenza e valorizzare il contributo degli studenti.

4.4. Gestione accessi (password, backup, ecc.)

Nei computer presenti nei laboratori sono previsti diversi profili di accesso con password relative:

- amministratore;
- docente;
- classe;
- guest.

Disposizioni sull'uso del laboratorio

1. Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.
2. I laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività didattiche, funzionali all'insegnamento e alla formazione del personale docente e non docente.
3. L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.
4. E' vietato cancellare o alterare files/dati presenti sull'hard disk.
5. Il laboratorio non deve mai essere lasciato aperto o 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.
6. In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al Responsabile di plesso/DSGA

Disposizioni sull'uso dei software

1. I software installati sono ad esclusivo uso didattico.
2. E' fatto divieto di usare software non conformi alle leggi sul copyright.
3. E' cura dell'insegnante-utente di verificarne la conformità. Gli insegnanti possono

installare nuovo software sui PC del laboratorio.

4. E' responsabilità degli insegnanti di assicurarsi che la copia non infranga le leggi sul copyright in vigore.

Accesso a internet

1. L'Accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;
2. Internet non può essere usato per scopi vietati dalla legislazione vigente;
3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;
4. E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da Internet, scaricare ed installare software senza licenza;
5. E' opportuno sempre utilizzare l'account istituzionale durante la navigazione in internet per una maggiore sicurezza dei contenuti e protezione dei dati personali.

4.5. Sito web della scuola

La scuola ha un sito web nel quale sono pubblicati tutti i documenti relativi la sicurezza in rete e la prevenzione di rischi legati ad un uso inconsapevole o sbagliato della stessa.

5 Strumentazione personale

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

Gli alunni si impegnano ad utilizzare telefoni cellulari, smartphone, smartwatch, tablet, ecc. esclusivamente per scopi didattici e previa autorizzazione da parte dei docenti.

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

Durante le ore di lezione è consentito ai docenti l'uso di dispositivi elettronici personali unicamente a scopo didattico e ad integrazione dei dispositivi scolastici disponibili.

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

L'uso di dispositivi elettronici personali è permesso solo per attività funzionali al servizio

6. Azioni

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

- diffondere un'informazione adeguata al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono contrarre sul web;
- introdurre regole precise per l'uso di dispositivi digitali propri, quali cellulare e smartphone, agli studenti in orario scolastico, regolamentando l'uso del cellulare e 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).
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse 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)

6.1. Rilevazione e denunce

Che cosa segnalare

Andranno opportunamente segnalati:

- ☐ dati particolari o riservati pubblicati in chat o social network (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.

6.2 Come gestire le segnalazioni

Raccogliere la segnalazione dell'alunno/docente/personale scolastico corredata da prove che attestino l'azione avvenuta.

Dare tempestiva informazione alle famiglie in merito all'accaduto, raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico ed, eventualmente, alla Polizia Postale.

6.3 Gestione dei casi

presa in carico da parte dell'insegnante che può rivolgersi alle seguenti figure:

- Dirigente scolastico
- Referente d'Istituto
- Polizia di Stato/ Polizia postale
- Telefono Azzurro (800.280.000)
- Help line Telefono Azzurro per "Generazioni connesse" (1.96.96)
- Save the Children

N.B. Per i reati più gravi la scuola si rivolgerà direttamente agli organi di polizia competenti.

Referente Scolastico

Prof.ssa Maria Elena Cottone

Dirigente Scolastico

Prof.ssa Paola Catanzaro