

ISTITUTO COMPRENSIVO BRA 1

Via Vittorio Emanuele, n. 200 - c.a.p 12042 BRA (Cuneo) Tel./Fax 0172/412438
Sito: www.istitutocomprensivobral.gov.it E-mail: cnic86400t@istruzione.it

E-SAFETY POLICY

1. INTRODUZIONE

SCOPO DELLA E-POLICY

Il documento vuole presentare in maniera chiara ed esaustiva le linee guida dell'Istituto Comprensivo Bra 1 in materia di:

- utilizzo consapevole delle TIC nella didattica e negli ambienti scolastici;
- prevenzione/gestione di situazioni problematiche relative all'uso delle tecnologie digitali.

In seguito all'emanazione della Legge n.71 del 29 maggio 2017 la nostra scuola ha aderito al progetto **Generazioni Connesse**, promosso dal MIUR in collaborazione con la Comunità Europea, ed ha elaborato il presente documento in conformità con le **LINEE DI ORIENTAMENTO** per azioni di prevenzione e di contrasto al bullismo e cyberbullismo emanate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con il Safer Internet Center per l'Italia.

Le nuove tecnologie sono parte integrante dell'attività didattica, sono utilizzate nella comunicazione scuola/famiglia e rivestono un ruolo importante nella vita sociale degli alunni, soprattutto nella scuola secondaria di primo grado.

Occorre premettere che:

- Le attività di promozione all'utilizzo delle tecnologie digitali nella didattica costituiscono un tema centrale per l'attuazione del Piano Nazionale Scuola Digitale e sono già previste nel Piano Triennale dell'Offerta Formativa, in particolare nel progetto predisposto dall'Animatore Digitale.
- La presente bozza di Policy è stata redatta da un gruppo di lavoro, sarà presentata al Collegio dei Docenti e al Consiglio di Istituto per condivisione e approvazione. Inoltre, data la velocità di evoluzione delle tecnologie, sarà passibile di eventuali cambiamenti.
- Il progetto "Generazioni connesse" sarà inserito nel nostro Piano Triennale dell'Offerta Formativa e le azioni preventivate nel Piano d'Azione della nostra scuola, visto il loro elevato numero e la complessità di alcune di esse, verranno portate avanti progressivamente nei prossimi anni.

RUOLI E RESPONSABILITA'

- **Il Dirigente Scolastico:**
 - è responsabile per la sicurezza dei dati;
 - è informato sulle linee guida contenute nella e-policy ed è garante della sua applicazione.

- **Il DSGA:**
 - assicura, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione richiesti da cattivo funzionamento e/o danneggiamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate;
 - cura la registrazione dei disservizi e delle problematiche relative alla rete e all'uso del digitale segnalate, provvedendo all'intervento del personale tecnico di assistenza.

- **L'Animatore Digitale (in collaborazione con il suo team):**
 - pubblica la Policy sul sito della scuola e promuove la diffusione dei suoi contenuti;
 - stimola la formazione interna alla scuola negli ambiti del PNSD, attraverso l'organizzazione di laboratori formativi, favorendo l'animazione e la partecipazione di tutta la comunità scolastica alle attività formative;
 - individua soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno degli ambienti della scuola (es. uso di particolari strumenti per la didattica di cui la scuola si è dotata; adozione di metodologie comuni; informazione su innovazioni esistenti in altre scuole; laboratorio di coding per tutti gli studenti), in sinergia con attività di assistenza tecnica condotta da altre figure;
 - Coordina e gestisce l'atelier digitale (in via di allestimento).

- **I Docenti:**
 - supervisionano e guidano gli alunni nelle attività che prevedono l'accesso alla rete, inseriscono tematiche legate alla sicurezza online nella didattica;
 - sviluppano le competenze digitali degli alunni e fanno in modo che conoscano e seguano le norme di sicurezza nell'utilizzo del web e utilizzino correttamente le tecnologie digitali sia a scuola sia nelle attività didattiche extracurricolari (vedi regolamento d'Istituto sull'uso delle TIC);
 - segnalano al Dirigente scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazioni;
 - durante le assemblee di inizio anno informano i genitori della necessità di visionare la Policy sul sito istituzionale.
 - Informare le famiglie tramite circolare di inizio d'anno con ricevuta del genitore di presa visione o al momento di iscrizione.

- **I Genitori:**

- Sostengono la scuola nel promuovere la sicurezza online, leggendo la policy e partecipando agli incontri organizzati dalla scuola, o a livello cittadino, sui temi della sicurezza online.

- **Gli alunni:**

- Conoscono e rispettano i regolamenti (generali e specifici delle aule di informatica) e segnalano al docente di classe eventuali usi impropri della rete e dei dispositivi;
- ascoltano e seguono le indicazioni fornite dai docenti e dai genitori per un uso corretto e responsabile delle tecnologie digitali;
- partecipano attivamente ai progetti e alle attività sul corretto utilizzo della tecnologia promosse dalla scuola;
- si impegnano a considerare l'utilizzo delle rete internet non solo come aspetto ludico, piuttosto come opportunità di conoscenza, di approfondimento, di crescita, di condivisione delle idee.

CONDIVISIONE E COMUNICAZIONE ALL'INTERA COMUNITA' SCOLASTICA

La E-Policy sarà pubblicata sul sito della scuola, dopo essere stata approvata dal Collegio dei Docenti e dal Consiglio di Istituto. Sarà presentata, in particolar modo, ai genitori e agli studenti della scuola secondaria di primo grado e delle classi quinte della scuola primaria.

GESTIONE DELLE INFRAZIONI ALLA POLICY

In relazione a quanto specificato in questa policy le infrazioni saranno gestite in modo graduale rispetto alla gravità dell'infrazione e, nel caso degli alunni, anche rispetto alla loro età.

Nel caso in cui un docente rilevi un'infrazione alle indicazioni della Policy è necessario che informi i colleghi del team o il coordinatore di classe; contestualmente sarà informato il vicario di plesso. L'infrazione sarà riportata al Dirigente Scolastico e alla famiglia. Nel caso in cui l'infrazione si configuri come atto di cyberbullismo, il docente informa il referente per il bullismo/cyberbullismo il quale agirà secondo le disposizioni della L.71/2017. Nel caso si tratti di un reato è necessario che il Dirigente Scolastico informi tempestivamente le autorità competenti (polizia postale o questore).

MONITORAGGIO DELL'IMPLEMENTAZIONE DELLA POLICY E SUO AGGIORNAMENTO

Il Dirigente Scolastico è responsabile dell'implementazione della Policy all'interno dell'Istituto. L'Animatore Digitale (insieme al Team dell'innovazione digitale), il gruppo GLI (con sottogruppo preposto) e il Referente per il Cyberbullismo, in accordo con il Dirigente Scolastico, partecipano alla revisione e all'aggiornamento del documento.

L'aggiornamento del documento è sottoposto all'approvazione del Collegio dei Docenti e del Consiglio di Istituto.

INTEGRAZIONE DELLA POLICY CON I REGOLAMENTI ESISTENTI

La Policy è coerente con quanto stabilito dalla Legge (Statuto delle studentesse e degli studenti della scuola secondaria DPR 24 giugno 1998 n. 249 modificato dal DPR 21 Novembre 2007 n. 235; Legge 29 maggio 2017 n. 71 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo"; Legge 31 dicembre 1996 n. 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali"), dai Regolamenti vigenti (di Istituto e Regolamento sull'utilizzo delle TIC) e dal Patto di Corresponsabilità.

2. FORMAZIONE E CURRICOLO

CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI

Le competenze digitali sono promosse in maniera trasversale dai docenti, sulla base delle loro pratiche di insegnamento.

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

- **primaria:** Usa con responsabilità le tecnologie in contesti comunicativi concreti per ricercare informazioni e per interagire con altre persone, come supporto alla creatività e alla soluzione di problemi semplici.
- **secondaria di primo grado:** Utilizza con consapevolezza e responsabilità le tecnologie per ricercare, produrre ed elaborare dati e informazioni, per interagire con altre persone, come supporto alla creatività e alla soluzione di problemi.

FORMAZIONE DEI DOCENTI SULL'UTILIZZO E L'INTEGRAZIONE DELLE TIC NELLA DIDATTICA

L'Animatore digitale ed il suo team predispongono un piano di formazione triennale progettato a partire dai bisogni formativi dei docenti.

I corsi attivati riguardano l'utilizzo di metodologie multimediali nella didattica quotidiana.

Si considera altresì necessaria un'opportuna autoformazione da parte dei docenti.

FORMAZIONE DEI DOCENTI SULL'UTILIZZO CONSAPEVOLE E SICURO DI INTERNET E DELLE TECNOLOGIE DIGITALI

L'ASL CN2 mette a disposizione del territorio il Progetto "Display" gestito dal gruppo Steadycam (per la prevenzione e per l'educazione ad un uso corretto dei nuovi media), organizzando corsi di formazione per docenti di ogni ordine di scuola, ai quali prendono parte docenti del nostro Istituto.

SENSIBILIZZAZIONE DELLE FAMIGLIE

A partire dalla scuola primaria (secondo necessità) la scuola invita i genitori ad assumersi l'incarico di accompagnare e supervisionare i figli durante la navigazione in rete, aiutandoli a riconoscere ed evitare i rischi.

Durante le prime riunioni di classe, i docenti suggeriscono la consultazione del portale Generazioni Connesse, dotato di una specifica Area Genitori, dove è possibile reperire informazioni e consigli pratici per una equilibrata e consapevole gestione del rapporto tra bambini, ragazzi e media. Si segnalano inoltre le attività promosse da Steadycam sul territorio rivolte alle famiglie "Safe Internet Day".

3. GESTIONE DELL'INFRASTRUTTURE E DELLE STRUMENTAZIONI TIC DELLA SCUOLA

ACCESSO AD INTERNET: FILTRI, ANTIVIRUS E NAVIGAZIONE

Data la giovane età degli studenti del nostro istituto è fondamentale fare tutto il possibile per evitare l'esposizione a contenuti inappropriati. Gli alunni non sono mai lasciati soli nelle aule in cui sono presenti dei computer collegati ad internet. L'accesso a internet è possibile nella scuola primaria e nella scuola secondaria in tutte le aule, molte dotate di Lavagna Interattiva Multimediale con relativo computer portatile e nei laboratori d'informatica.

Le impostazioni sono definite e mantenute dal responsabile dei laboratori e dall'Animatore digitale ed è in carico a ciascun docente la segnalazione di malfunzionamenti e disservizi.

I docenti hanno piena autonomia nel collegamento ai siti web nelle postazioni a loro riservate.

Relativamente agli alunni che accedono a Internet durante l'attività didattica sono consentiti la navigazione guidata da parte dell'insegnante e la stesura di documenti collaborativi purché sotto il controllo dell'insegnante e nel caso in cui tale attività faccia parte di un progetto di lavoro precedentemente autorizzato.

Le scuole dell'Istituto sono dotate di antivirus, monitorati e tenuti aggiornati dai responsabili dei laboratori informatici.

Qualora l'attività didattica preveda una modalità BYOD (Bring Your Own Device, in italiano "porta il tuo dispositivo") di utilizzo dei dispositivi personali degli allievi, questi devono connettersi esclusivamente tramite wi-fi protetto da appositi filtri della scuola, non possono per alcun motivo utilizzare la propria connessione dati e le applicazioni di messaging e social network.

GESTIONE ACCESSI

L'accesso alla rete wi-fi è dotata di password che viene comunicata esclusivamente dall'Animatore Digitale o, in sua assenza, dal Responsabile del Laboratorio.

I computer portatili presenti nelle aule non richiedono una password di accesso per l'accensione. Ogni docente è quindi tenuto ad un controllo della strumentazione in aula poiché l'uso del dispositivo è permesso agli alunni solo su autorizzazione dell'insegnante. Ogni docente accede al registro elettronico attraverso una password personale che non può essere comunicata a terzi, né agli alunni.

Nel laboratorio di informatica è possibile effettuare installazioni e aggiornamenti di software solo tramite l'autorizzazione del Responsabile di Laboratorio e dell'Animatore Digitale.

Per la Scuola Secondaria di primo grado si specifica che i computer in aula professori hanno un unico nome utente e password. Tutte le aule sono dotate di pc portatili a disposizione dei docenti per la compilazione del registro elettronico e come supporto alla didattica.

La connessione alla rete wi-fi è accessibile ed è disponibile per i docenti (la rete è accessibile a tutti i docenti tramite password che viene loro comunicata all'inizio dell'anno). Inoltre la rete wi-fi è disponibile anche per la fruizione da parte degli alunni solo ed esclusivamente per attività didattiche, con la possibilità di comunicare una password di rete temporanea che viene accesa e poi spenta dal responsabile digitale di plesso su richiesta dei docenti conduttori dell'attività.

SITO WEB DELLA SCUOLA

Il sito dell'Istituto Comprensivo è raggiungibile all'indirizzo
<http://www.istitutocomprensivobra1.gov.it>

Il sito prevede un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali, avvisi di carattere generale e comunicazioni interne o dal territorio.

Il Dirigente e il suo Staff verificano i contenuti destinati alla pubblicazione. Responsabile della gestione del sito è l'Animatore Digitale congiuntamente alla Commissione "Redazione Sito" che visiona i materiali didattici prima della pubblicazione con l'obiettivo di verificarne l'idoneità in base ai requisiti stabiliti.

SOCIAL NETWORK

Per la Legge l'utilizzo dei Social Network con la pubblicazione di nomi e giudizi sulle persone o sulle istituzioni e la diffusione di foto/filmati senza il consenso e, comunque,

all'insaputa delle persone coinvolte, può determinare ricadute di carattere anche penale, come ad esempio la diffamazione.

Si invitano pertanto tutti i fruitori a non prelevare o diffondere immagini, video o registrazioni – anche solo audio – non autorizzate, ad eliminare da internet eventuali riferimenti offensivi o comunque illeciti (ed inopportuni) nei confronti dell'Istituto e dei suoi docenti e studenti.

Allo stesso tempo, si invitano gli allievi e i genitori a fare un uso prudente dei Social Network, in particolare Facebook, Whatsapp e Instagram, limitandone l'uso alle sole comunicazioni funzionali, evitando ad ogni modo di esprimere giudizi sull'operato degli altri studenti o del personale della scuola, giudizi che una volta pubblicati comportano sempre una assunzione di responsabilità da parte di chi li ha scritti o anche semplicemente diffusi.

La Scuola Secondaria è presente su Facebook con una propria pagina su cui vengono esclusivamente pubblicate foto e comunicazioni relative alla didattica.

Al momento non vengono utilizzate piattaforme didattiche (Edmodo, Weschool, google classroom, ...) Dal prossimo anno scolastico, i docenti interessati, potranno utilizzare google classroom o altre piattaforme gratuite conosciute, purché sicure.

PROTEZIONE DEI DATI PERSONALI

In fase di iscrizione degli alunni alla scuola i genitori sottoscrivono un'informativa sul trattamento dei dati personali, in ottemperanza all'art. 13 D.Lgs 30 giugno 2003 , n. 196 (Codice in materia di protezione dei dati personali).

All'inizio del ciclo di istruzione i genitori rilasciano il consenso all'utilizzo di materiale fotografico e audiovisivo riservato ed elaborati degli alunni per esporli anche in sedi diverse da quelle dell'Istituto quali pubblicazioni in formato digitale e siti web.

In caso di utilizzo di piattaforme digitali condivise o di strumenti per la creazione e la gestione di classi virtuali viene acquisito preventivamente il consenso informato dei genitori.

In caso di attività di ampliamento dell'offerta formativa, organizzate in collaborazione con Enti esterni, viene richiesto preventivamente ai genitori il consenso informato alle riprese audio/ video e al loro eventuale utilizzo per scopi didattici, informativi e divulgativi anche tramite pubblicazione su siti web.

L'accesso ai dati riportati nel registro elettronico (schede di valutazione) è riservato ai genitori della scuola tramite l'invio di una password di accesso strettamente personale.

4. STRUMENTAZIONE PERSONALE

PER GLI STUDENTI DELLE SCUOLE PRIMARIE: è vietato l'utilizzo di cellulari per l'intera durata delle attività scolastiche. E' consentito agli alunni con Bisogni Educativi Speciali utilizzare il proprio notebook o tablet, senza connessione internet.

PER GLI STUDENTI DELLA SCUOLA SECONDARIA DI PRIMO GRADO: è vietato l'utilizzo, a livello personale, di cellulari per l'intera durata delle attività scolastiche. E' consentito agli alunni con Bisogni Educativi Speciali utilizzare il proprio dispositivo elettronico, senza connessione internet. L'utilizzo dei device, senza connessione internet, è consentito anche agli altri alunni in casi specifici concordati con il docente, previa richiesta della famiglia e sottoscrizione di un Regolamento interno.

PER I DOCENTI: durante il loro orario di servizio è consentito l'utilizzo di dispositivi elettronici personali solo ed esclusivamente per fini didattici.

PER IL PERSONALE DELLA SCUOLA: è vietato l'utilizzo di dispositivi elettronici durante l'orario di servizio per uso personale.

PER LE CLASSI CHE RICHIEDONO I DISPOSITIVI PERSONALI:

Al momento solo pochi docenti della Scuola secondaria utilizzano saltuariamente la modalità Byod, una pratica veloce e flessibile che rende possibile la partecipazione digitale degli alunni, con il loro dispositivo, nel corso della didattica "tradizionale" in aula. Nel futuro, sulla base delle esigenze didattiche e della nuova formazione digitale, è possibile che questa pratica venga implementata, oppure resti una opzione secondaria rispetto all'uso del nuovo laboratorio di informatica.

Le iniziative significative dei docenti che coinvolgano l'ambito digitale dovranno essere comunicate al Referente informatico di plesso che provvederà ad informare l'Animatore digitale ed eventualmente a sostenere il collega sull'uso delle TIC nella didattica.

Al momento non sono definite linee specifiche riguardo la sicurezza, per cui la responsabilità è demandata al docente richiedente.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

PREVENZIONE

In linea con il nostro PTOF la didattica inclusiva è lo strumento più efficace per la prevenzione di comportamenti scorretti e per favorire il rispetto dell'altro.

La scuola si impegna ad attrezzare le aule con dispositivi elettronici sicuri e protetti.

I docenti si impegnano ad organizzare per gli alunni momenti di riflessione sui temi dell'utilizzo consapevole di internet e a formarsi su queste tematiche.

I genitori si impegnano a prendere visione della E-safety Policy e a seguire le azioni promosse dalla scuola e dal territorio per l'utilizzo consapevole della rete.

Gli alunni si impegnano a rispettare i regolamenti e a partecipare attivamente alle occasioni di confronto su queste tematiche organizzate dalla scuola e dal territorio.

Per i rischi connessi all'utilizzo delle nuove tecnologie (grooming, cyberbullismo, furto di identità, sexting), la scuola si affida a consulenti esterni per organizzare incontri informativi rivolti agli alunni (Steadycam).

Il Referente per il Cyberbullismo, terminata la sua personale formazione, si impegna a diffondere tra i colleghi interessati i principali rischi connessi ad internet.

RILEVAZIONE

Premesso che la tutela dei minori è l'unico diritto superiore a quelli di cronaca, satira e libera espressione, si considerano da segnalare tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o un piccolo gruppo) tramite un utilizzo irresponsabile dei social network.

In particolare si segnaleranno:

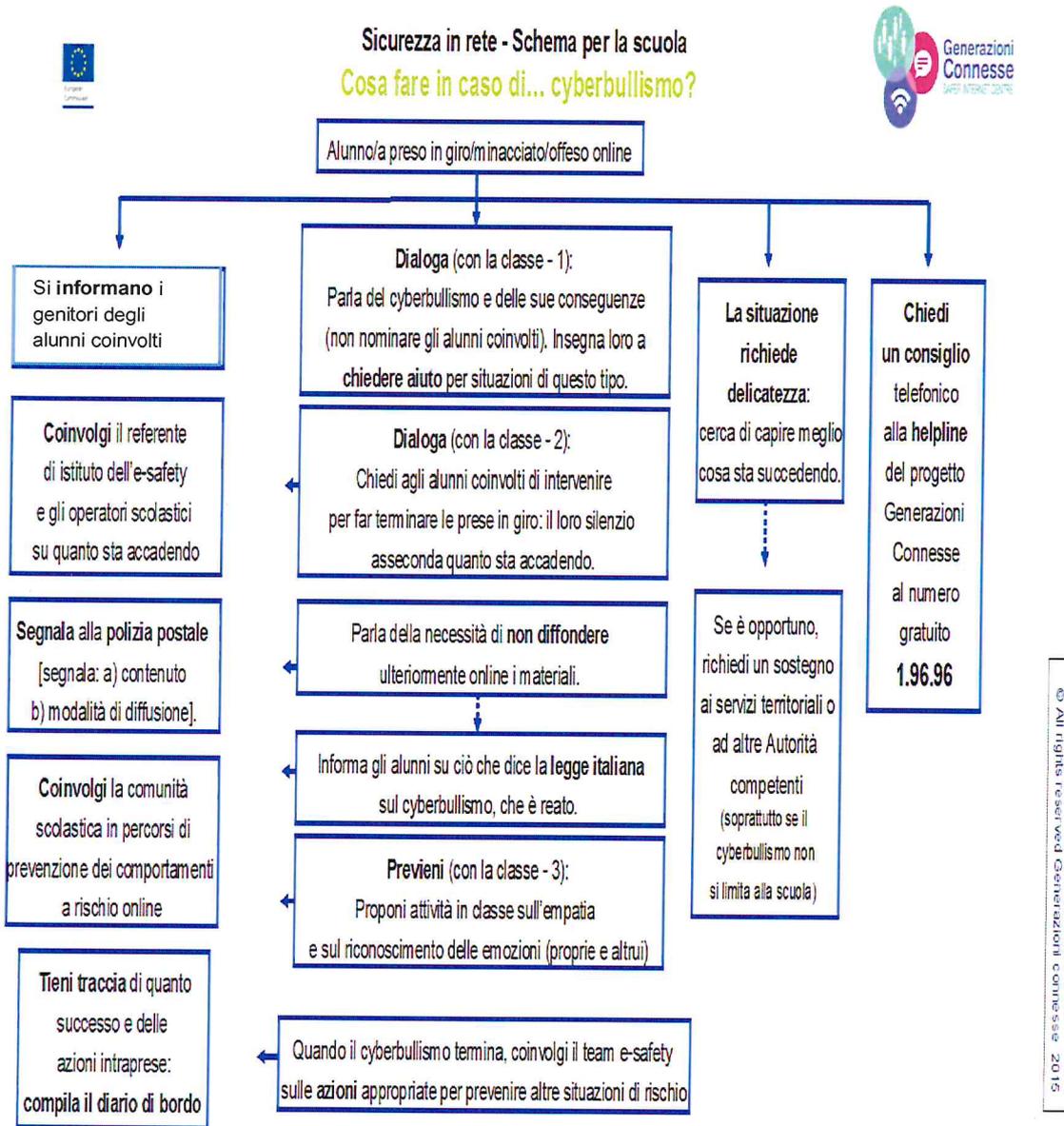
- contenuti afferenti la violazione della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video di eventi privati), pubblicati contro la propria volontà o senza le autorizzazioni previste;
- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

Tutte le segnalazioni riportate dai docenti saranno registrate su apposita scheda (Modulo segnalazione – Allegato 1)

I docenti di classe informano i colleghi o il coordinatore di classe e il referente per il bullismo/cyberbullismo. Contestualmente saranno informati anche i vicari di plesso. Il referente informa il Dirigente Scolastico, il quale procede ad informare le famiglie. Tutte le segnalazioni riportate dai docenti saranno registrate su apposita scheda (Diario di bordo – Allegato 2).

GESTIONE DEI CASI

Nel caso in cui un docente sia informato di azioni di cyberbullismo o altre infrazioni informatiche deve attenersi alle modalità riportate nello schema seguente:



I passaggi principali sono:

- coinvolgere i colleghi di classe o il coordinatore di classe
- coinvolgere le parti e cercare di creare un dialogo
- compilare il modulo per la segnalazione
- informare il referente del cyberbullismo
- informare la vicaria di plesso
- informare il Dirigente Scolastico
- se il caso lo richiede si informeranno le forze dell'ordine Polizia Postale per un loro intervento
- segnalazione al Questore o alla Procura della Repubblica dei minorenni per un ammonimento nel caso in cui si configuri un possibile reato o una grave infrazione.

Bra, 22 giugno 2018

Il Dirigente scolastico

Dott. Giuseppe Giacone



L'Animatore Digitale

Franca Dominici



La referente per il progetto

Maura Brero



Allegato 1

PROGETTO GENERAZIONI CONNESSE

MODULO PER LA SEGNALAZIONE DI CASI

Nome di chi compila la segnalazione:

Ruolo:

Data:

Scuola:

Descrizione dell'episodio o del problema	
Soggetti coinvolti	<p>Vittima/e: Classe:</p> <p>1. 2. 3.</p> <p>Bullo/i: Classe:</p> <p>1. 2. 3.</p>
Chi ha riferito dell'episodio?	<p>- La vittima</p> <p>- Un compagno della vittima, nome:</p> <p>- Genitore, nome:</p> <p>- Insegnante, nome:</p> <p>- Altri, specificare:</p>
Atteggiamento del gruppo	<p>Da quanti compagni è sostenuto il bullo?</p> <p>Quanti compagni supportano la vittima o potrebbero farlo?</p>
Gli insegnanti sono intervenuti in qualche modo ?	
La famiglia o altri adulti hanno cercato di intervenire ?	
Chi è stato informato della situazione?	<p><input type="checkbox"/> coordinatore di classe data:</p> <p><input type="checkbox"/> consiglio di classe data:</p> <p><input type="checkbox"/> dirigente scolastico data:</p> <p><input type="checkbox"/> la famiglia della vittima/e data:</p> <p><input type="checkbox"/> la famiglia del bullo/i data:</p> <p><input type="checkbox"/> le forze dell'ordine data:</p> <p><input type="checkbox"/> altro, specificare:</p>

MODULO PER IL FOLLOW-UP DEI CASI

AZIONI INTRAPRESE

La situazione è

Aggiornamento 1

migliorata invariata peggiorata

Come:

Aggiornamento 2

migliorata invariata peggiorata

Come:

Aggiornamento 3

migliorata invariata peggiorata

Come:

Allegato 2



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 (narrato)	Azioni intraprese		Insegnante con cui l'alunno si è conitato	Firma
				Cosa?	Da chi?		

