



ISTITUTO COMPRENSIVO N.9

Via Luigi Longo, 4 – 40139 Bologna Tel. 051-460205/460007

C.F. 91201100376 – C.M. BOIC85200B Codice Univoco di Fatturazione UFVT55

Sito:<http://www.ic9bo.gov.it>-mail:boic85200b@istruzione.it-mail pec:boic85200b@pec.istruzione.it

E-SAFETY POLICY

(APPROVATA DAL COLLEGIO DOCENTI DEL 18/05/2018)

INDICE

1. Introduzione

- Scopo della Policy.
- Ruoli e Responsabilità (*che cosa ci si aspetta da tutti gli attori della Comunità Scolastica*).
- Condivisione e comunicazione della Policy all'intera comunità scolastica.
- Gestione delle infrazioni alla Policy.
- Monitoraggio dell'implementazione della Policy e suo aggiornamento.
- Integrazione della Policy con Regolamenti esistenti.

2. Formazione e Curricolo

- Curricolo sulle competenze digitali per gli studenti.
- Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica.
- Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
- Incontri formativi con le famiglie

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

- Accesso ad Internet: filtri antivirus e sulla navigazione.
- Gestione accessi (password, backup, ecc.).
- E-mail.
- Blog e sito web della scuola.
- Protezione dei dati personali.

4. Strumentazione personale

- Per gli studenti: gestione degli strumenti personali - cellulari, tablet, ecc.
- Per i docenti: gestione degli strumenti personali - cellulari, tablet, ecc.
- Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet, ecc.

5. Prevenzione, rilevazione e gestione dei casi

Prevenzione

- Rischi.
- Azioni.

Rilevazione

- Che cosa segnalare.
- Come segnalare: quali strumenti e a chi.
- Come gestire le segnalazioni.

Gestione dei casi

- Definizione delle azioni da intraprendere a seconda della specifica del caso.

1. INTRODUZIONE

-Scopo della Policy.

La E-Safety Policy stabilisce i principi fondamentali per l'utilizzo delle tecnologie e per l'uso responsabile di Internet per tutta la comunità scolastica.

- Ruoli e Responsabilità (che cosa ci si aspetta da tutti gli attori della Comunità Scolastica).

1) Dirigente scolastico:

- garantire la sicurezza (tra cui la sicurezza on-line) dei membri della comunità scolastica;
- garantire agli insegnanti una formazione adeguata per un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC).

2) Animatore digitale, Team dell'innovazione e Figure strumentali su Innovazione, ricerca didattica, Nuove Tecnologie e Sostegno al lavoro docenti, in particolare all'uso delle TIC nella didattica:

- stimolare la formazione interna riguardo ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche relative all'utilizzo sicuro delle tecnologie digitali e di Internet a scuola;
- assicurare l'accesso alla rete della scuola solo tramite password;
- curare la manutenzione e lo sviluppo del sito web della scuola;
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".

3) Docenti:

- informarsi/aggiornarsi sull'uso sicuro delle tecnologie digitali e di Internet;
- integrare l'utilizzo corretto e sicuro delle TIC e di Internet nel curriculum di studio e nelle attività didattiche ed educative;
- presentare le potenzialità delle TIC per la ricerca di contenuti e materiali, evitando il plagio e rispettando i diritti d'autore;
- 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;
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare al Dirigente Scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di Internet, per l'adozione delle procedure previste dalle norme.

5) Alunni

- usare le tecnologie secondo le indicazioni dei docenti e mai con iniziative personali;
- comprendere l'importanza di adottare buone pratiche di sicurezza on-line;
- rispettare gli altri anche quando si comunica in rete.

6) Genitori

- sostenere la linea di condotta della scuola nei confronti dell'utilizzo delle tecnologie;
- seguire gli alunni nello studio a casa, adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllando l'utilizzo del pc e di Internet;

- concordare con i docenti linee di intervento coerenti e di carattere educativo in caso di un uso non responsabile o pericoloso delle tecnologie digitali o di Internet.

- Condivisione e comunicazione della Policy all'intera comunità scolastica.

La E-Safety Policy d'Istituto si applica a tutti i membri della scuola, compreso il personale, gli studenti e i genitori.

La Policy viene comunicata al personale, agli alunni, alla comunità nei seguenti modi:

- pubblicazione della E-Safety Policy sul sito della scuola;
- utilizzo consapevole, discusso con gli studenti e i genitori, all'inizio del primo anno, tramite il Patto di Corresponsabilità;
- utilizzo consapevole rilasciato al personale scolastico.

- Gestione delle infrazioni alla Policy:

- La scuola prenderà tutte le precauzioni necessarie per garantire la sicurezza on-line.
- Al personale e agli alunni saranno date informazioni sulle infrazioni e sulle eventuali sanzioni.
- Denunce di bullismo online saranno trattate in conformità con la legge attuale.

- Monitoraggio dell'implementazione della Policy e suo aggiornamento

La E-Safety Policy sarà riesaminata annualmente o quando si verificano cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola da una Commissione preposta e tutte le modifiche della Policy saranno approvate in sede di Collegio Docenti.

2 FORMAZIONE E CURRICOLO

Curricolo sulle competenze digitali per gli studenti

Competenza digitale significa utilizzare le nuove tecnologie in autonomia e con responsabilità nel rispetto degli altri e sapendone prevenire ed evitare i pericoli.

La scuola si propone di favorire lo sviluppo di competenze tra cui:

- saper valutare e verificare le informazioni on line;
- conoscere i rischi relativi all'uso delle tecnologie e di Internet;
- saper mantenere le informazioni personali private;
- saper segnalare eventuali abusi, tra cui il bullismo on-line, e chiedere aiuto ai docenti e ai genitori.

- Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

La scuola ha previsto:

- individuazione e formazione di un Animatore Digitale e di un Team dell'Innovazione;
- formazione dei docenti in materia di digitale e di didattica attiva con le TIC;
- ricognizione e messa a punto delle dotazioni digitali;
- monitoraggio della didattica attiva con le TIC come si evince dal PTOF e dei risultati conseguiti.

Sono previsti inoltre:

- incontri con esperti vari (Polizia di Stato, Arma dei Carabinieri, Associazioni, psicologi);
- materiali informativi tratti dal sito ministeriale Generazioni Connesse¹ per l'approfondimento personale e per le attività con gli studenti.

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

La scuola organizza incontri di formazione su:

- utilizzo della LIM;
- utilizzo dell'aula 3.0;
- Flipped classroom, Didattica per scenari, Debate, PBL, spazi flessibili;
- Piattaforma Moodle e Registro online e Google Suites .

- Sensibilizzazione delle famiglie

Infine la scuola promuove il coinvolgimento delle famiglie attraverso:

- incontri con personale esperto interno ed esterno alla scuola e diffusione del materiale informativo sulle tematiche trattate;
- materiali di approfondimento per le famiglie (pdf e video) tratti dal sito ministeriale Generazioni Connesse (1).

3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA.

- Accesso a Internet: filtri, antivirus e sulla navigazione.

L'accesso a Internet è possibile e consentito per la didattica in tutta la scuola. L'accesso è per tutti schermato da filtri che consentono il collegamento solo a siti idonei alla didattica, secondo le impostazioni date dall'Animatore digitale e dalle FS preposte.

- Gestione accessi (password, backup, ecc.)

L'accesso ad Internet è consentito attraverso l'assegnazione di uno username e di una password da parte del gestore dei servizi di Internet. Viene effettuato regolarmente il backup di tutti i dati (segreteria, sito, moodle, registro).

-E-Mail

I docenti e gli studenti possono avere su richiesta di un docente del Consiglio di classe un account *google apps for education*. L'account è strettamente personale, per cui ogni utente dovrà avere cura di disconnettere il proprio accesso al termine del suo utilizzo. Lo spazio è destinato alla ricezione di comunicazioni, all'invio di documentazione e alla condivisione di materiali con i docenti e gli altri studenti dell'IC.

- Blog e sito web della scuola

La scuola ha un sito web. Tutti i contenuti del settore didattico sono pubblicati direttamente e sotto supervisione del responsabile del sito individuato in un docente interno alla scuola.

- 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 allo svolgimento della propria funzione.

¹ (1) <http://www.generazioniconnesse.it/site/it/home-page/>. Il progetto è coordinato dal MIUR, 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, Università degli Studi di Firenze, Università degli studi di Roma "La Sapienza", Skuola.net, Cooperativa E.D.I. e Movimento Difesa del Cittadino, Agenzia Dire con lo scopo di dare continuità all'esperienza sviluppata negli anni, migliorando e rafforzando il ruolo del Safer Internet Centre Italiano, quale punto di riferimento a livello nazionale per quanto riguarda le tematiche relative alla sicurezza in Rete e al rapporto tra giovani e nuovi media.

4. STRUMENTAZIONE PERSONALE

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

Come da regolamento d'istituto non è consentito l'uso del cellulare; l'uso del tablet o pc personale può essere autorizzato dal docente solo per attività didattiche previa informazione e consenso da parte di un genitore.

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

È consentito l'uso di cellulari, tablet e altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili.

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

Durante l'orario di servizio al restante personale scolastico è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente.

5.PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

- Prevenzione

La scuola mira a promuovere un ambiente di apprendimento sereno, sicuro e accogliente, che insegni ad interagire in maniera responsabile e mette in atto tutte le azioni possibili per contrastare comportamenti di bullismo, cyberbullismo, violenza e prepotenza.

Rischi

La scuola avrà cura di porre attenzione alla rilevazione di rischi connessi alla navigazione sul web. In modo particolare riguardo a:

- ·Cyberbullismo;
- · Adescamento online;
- · Sexting;
- · Pornografia;
- · Pedopornografia;
- · Gioco d'azzardo;
- · Dipendenza da Internet;
- · Esposizione a contenuti dannosi o inadeguati.

Azioni

La scuola si impegna a:

1. promuovere la diffusione della conoscenza delle Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo del MIUR.
2. implementare la e-Safety Policy con il contributo di tutte le componenti (docenti, studenti, famiglie, personale A.T.A.).

- Rilevazione

Che cosa segnalare

Le tipologie di comportamenti da segnalare sono:

1. Uso di dispositivi elettronici per chiamate o messaggi o per altro uso non consentito (giochi, musica, chat, etc.);
2. Uso del cellulare per effettuare riprese audio, foto, video;
3. Uso del cellulare per diffondere a terzi, in modo non autorizzato, audio, foto o video in violazione delle norme sulla privacy.

Come segnalare: con quali strumenti e a chi

Per segnalare i casi e tenere traccia di ciò che è avvenuto la scuola utilizza le linee guida di Generazioni Connesse.

Come gestire le segnalazioni

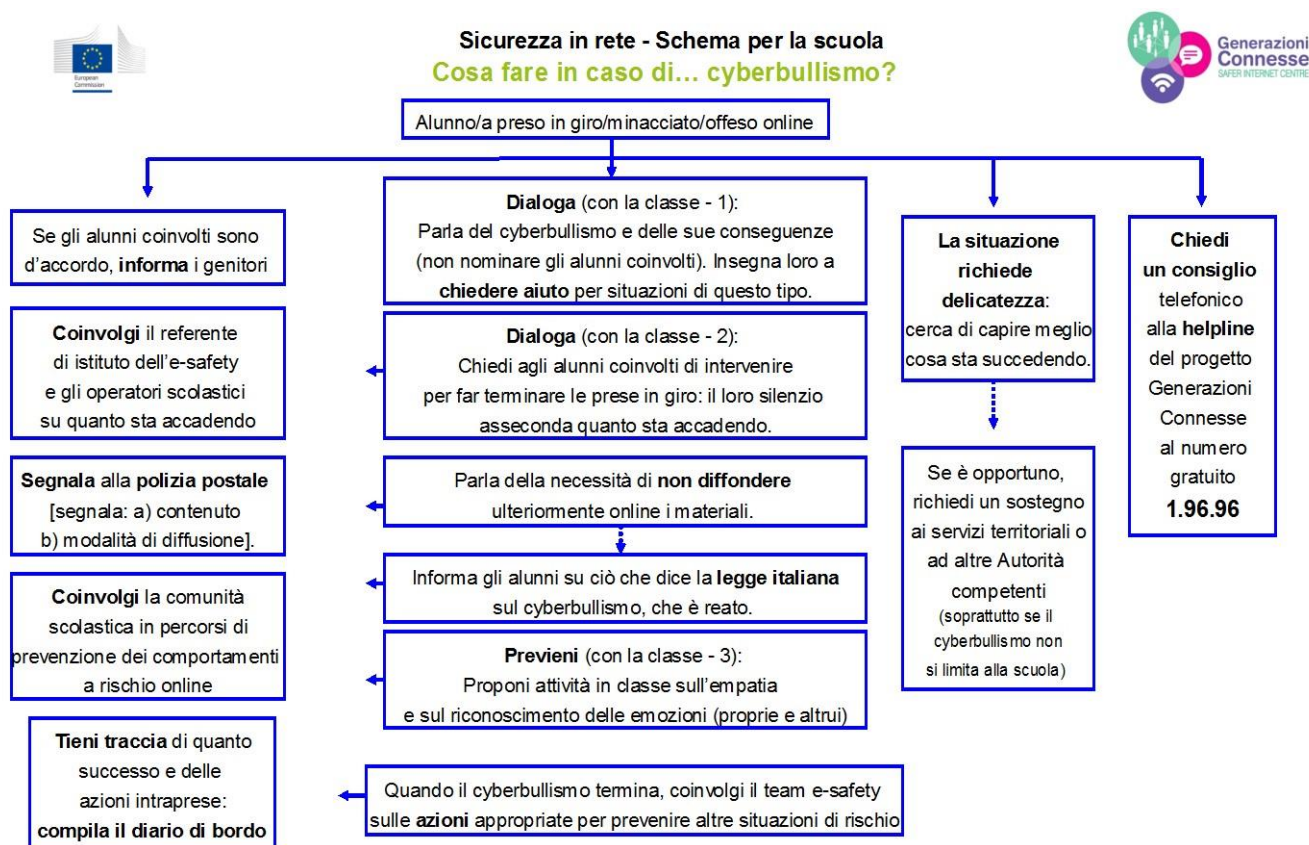
Le tappe da seguire quando si presenta un caso di (cyber)bullismo sono:

- fermare immediatamente l'abuso;
- dare sostegno alla vittima;
- lavorare sul gruppo classe affinché riconosca la gravità dell'accaduto e la propria partecipazione attraverso il silenzio o forme blande di coinvolgimento;
- dare supporto al bullo con un programma educativo che si focalizzi su due fronti: il coinvolgimento attivo del gruppo dei pari per sviluppare l'empatia e l'intervento dei docenti per gestire l'aggressività e la rabbia.

Il coinvolgimento dei coetanei è indispensabile per garantire l'efficacia dell'intervento ed è finalizzato a:

- creare un clima di solidarietà
- combattere l'indifferenza e la deresponsabilizzazione morale
- incoraggiare le vittime a chiedere aiuto
- sottrarre al (cyber)bullo potenziali proseliti.

In caso di cyberbullismo la scuola propone la procedura descritta nel seguente schema messo a disposizione sul sito www.generazioniconnesse.it :



- Gestione dei casi

Definizione delle azioni da intraprendere a seconda della specifica del caso.

Il **“Regolamento per la prevenzione e il contrasto al bullismo e al cyberbullismo”** della scuola stabilisce i seguenti provvedimenti:

CONTRAVVENZIONI	FREQUENZA	PROVVEDIMENTO	ORGANO COMPETENTE
L'alunno ha il cellulare acceso (riceve chiamate o notifica di messaggi)	Prima volta	Ritiro del cellulare	Docente
	Seconda volta	Nota sul registro di classe (con comunicazione alla famiglia sul diario personale)	Docente
	Uso reiterato	Ritiro temporaneo del cellulare e nota sul registro di classe; convocazione della famiglia ed in seguito provvedimento disciplinare del CdC	Coordinatore+ DS/delegato + CdC + Rappresentanti dei genitori
L'alunno utilizza dispositivi elettronici per chiamate o messaggi o per altro uso non consentito (giochi, musica, chat, etc.)	Prima volta	Ritiro temporaneo del cellulare e nota sul registro di classe; il docente valuta, a seconda dell'entità dell'infrazione, se restituire il dispositivo a fine lezione o consegnarlo ai genitori.	Docente
	Uso reiterato	Ritiro temporaneo del cellulare e nota sul registro di classe; convocazione della famiglia ed in seguito provvedimento disciplinare del CdC	Coordinatore + DS/delegato + CdC + Rappresentanti dei genitori
L'alunno utilizza dispositivi elettronici durante una verifica scritta		Ritiro della verifica e valutazione gravemente insufficiente della stessa; nota sul registro di classe (con comunicazione alla famiglia sul diario personale) e ritiro del cellulare	Docente + CdC
L'alunno effettua riprese audio, foto o video		Ritiro temporaneo del cellulare e nota sul registro di classe (con comunicazione alla famiglia sul diario personale) ed eventuale intervento del DS/delegato Provvedimento disciplinare	Docente + DS/delegato + CdC + Rappresentanti dei genitori
L'alunno diffonde a terzi, in modo non autorizzato, audio, foto o video in violazione delle norme sulla privacy		Ritiro temporaneo del cellulare e nota sul registro di classe (con comunicazione alla famiglia sul diario personale) Intervento del DS/delegato e convocazione delle parti coinvolte; Provvedimento disciplinare fino a 15 giorni	CdC + DS/delegato + Referente cyberbullismo + Rappresentante dei genitori + Polizia di Stato + Procura

La Referente
Prof.ssa Maddalena Francavilla

La Dirigente
Prof.ssa Giovanna Cantile