



ISTITUTO COMPRESIVO SANFRONT - PAESANA

Corso Marconi 22 – Tel e fax. 0175/948172 12030 SANFRONT

e-mail: cnic83500t@istruzione.it pec: cnic83500t@pec.istruzione.it

www.istitutocomprensivodisanfrontpaesana.gov.it

C.M. CNIC83500T C.F. 94033130041

E-SAFETY POLICY

1. INTRODUZIONE

Il nostro Istituto intende incrementare l'uso delle tecnologie informatiche nella didattica e nell'organizzazione generale della scuola. Tuttavia, l'uso sempre più pervasivo di piattaforme in rete e dispositivi portatili ha esposto gli utenti, e in particolare i minori, a rischi tanto più rilevanti quanto meno è diffusa una cultura relativa ai modi legittimi di usare la rete e alla consapevolezza delle funzioni rese possibili.

Il nostro Istituto ha deciso così di sviluppare e attuare il progetto “Generazioni Connesse” (www.generazioniconnesse.it) attraverso la realizzazione di tre linee di intervento:

1. l'elaborazione di linee guida per una eSafety Policy d'Istituto, cioè di un proprio codice di condotta nella prevenzione e gestione dei casi di (cyber)bullismo e di un regolamento di sicurezza informatica;
2. la promozione nei confronti degli alunni della competenza digitale e della cultura del rispetto di regole comuni nell'uso dei servizi telematici;
3. la procedura per la gestione delle problematiche e un insieme di attività per la prevenzione dei rischi.

Le **linee guida** per la eSafety Policy sono parte integrante del Regolamento di Istituto e fanno riferimento ad un uso generale delle infrastrutture di rete.

PRINCIPI GENERALI

- a. Principi generali: Internet bene comune e strumento cruciale per lo sviluppo e l'esercizio dei diritti umani.
- b. Cittadinanza in rete: accesso all'infrastruttura indipendentemente dal luogo di residenza; accessibilità come strumento di inclusione.
- c. Consumatori e utenti della rete: competenze digitali, riservatezza, archiviazione e cancellazione dei dati personali.
- d. Produzione e circolazione dei contenuti: condivisione dei contenuti e della conoscenza in rete.
- e. Sicurezza in rete: protezione dei soggetti deboli.

2. FORMAZIONE E CURRICOLO

CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI

Il nostro Istituto ha elaborato il Curricolo per le competenze digitali chiave che è parte integrante del PTOF.

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

Il nostro Istituto ha partecipato con successo ai Fondi Strutturali Europei - Programma Operativo Nazionale “Per la scuola – Competenze e ambienti per l’apprendimento”, migliorando la propria connessione Wi-Fi.

La Scuola sta ampliando la sua dotazione di LIM e di tablet. È auspicabile che le azioni realizzate inneschino un circolo virtuoso che stimoli sempre più docenti a utilizzare e integrare le TIC nella didattica.

Sicuramente saranno pianificate occasioni di formazione per docenti sulle nuove metodologie innovative e sull’integrazione delle TIC nella didattica.

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

Oltre alla partecipazione di alcuni insegnanti al corso on line del progetto “Generazioni connesse”, è stato organizzato un corso di aggiornamento interno sui rischi della Rete per docenti e due serate informative per i genitori sulle stesse tematiche.

Viste le positive reazioni di docenti e genitori, la Scuola prevede di organizzare per l’anno prossimo iniziative di prevenzione primaria al (cyber)bullismo.

3. GESTIONE DELL’INFRASTRUTTURA, DELLA STRUMENTAZIONE ICT DELLA SCUOLA E DELLA STRUMENTAZIONE PERSONALE

La Scuola metterà in atto tutte le azioni necessarie per garantire agli studenti l’accesso alla documentazione cercata, adottando misure per diminuire le possibilità di rischio durante la navigazione, fermo restando che non è possibile garantire una navigazione totalmente priva di rischi e che la Scuola e gli insegnanti non possono assumersi le responsabilità conseguenti all’accesso accidentale e/o improprio a siti illeciti.

ACCESSO AD INTERNET: ANTIVIRUS E FILTRI SULLA NAVIGAZIONE

Buone pratiche nell’uso della rete

- Controllo della validità e dell’origine delle informazioni.
- Confronto con fonti alternative di informazione.
- Rispetto dei diritti di autore.

Linee guida di buona condotta dell’utente

- Rispettare la legislazione vigente.
- Non divulgare notizie private contenute nelle documentazioni elettroniche cui si ha accesso.
- Rispettare le regole condivise che disciplinano il rapportarsi fra utenti della rete.

Le regole

- Rispettare le persone diverse per nazionalità, cultura, religione, sesso.
- Non rivelare dettagli o informazioni personali o di altre persone.
- Non dare indirizzo e numero di telefono a persone incontrate sul web.

- Non prendere appuntamenti con le persone conosciute tramite web.
- Non inviare fotografie proprie o di altre persone.
- Riferire sempre a insegnanti e genitori se si incontrano in Internet immagini o scritti che infastidiscono.
- In casi di violazione di queste regole parlarne con genitori ed insegnanti.
- Chiedere il permesso prima di scaricare dal web materiale di vario tipo.

GESTIONE ACCESSI

Accesso docenti

- Ai docenti è consentito accedere ad Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto.
- Il proprietario del dispositivo è l'unico responsabile di tutte le operazioni svolte con esso.
- In caso di furto o smarrimento del dispositivo identificato, si deve immediatamente informare il personale tecnico incaricato che ne revocherà l'accesso alla Rete.
- Il docente verificherà lo spegnimento della postazione al termine della sua ora di lezione.

Accesso studenti

Il Regolamento di Istituto **vieta** l'uso del cellulare. In particolare, agli studenti **non** è consentito accedere ad Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto.

E-MAIL

- Solo i docenti possono utilizzare i servizi mail accedendo alla rete della scuola a fini esclusivamente didattici.

SITO WEB DELLA SCUOLA

Il Dirigente Scolastico e il personale incaricato di gestire le pagine del sito della Scuola hanno la responsabilità di garantire che il contenuto pubblicato sia accurato e appropriato.

La scuola offre all'interno del proprio sito una serie di servizi alle famiglie e ai fruitori esterni, come modulistica, GOL (Giornalino On Line), news dell'istituto.

I docenti possono pubblicare attività didattiche, di laboratorio o di progetto svolte durante l'anno con gli allievi, previo consenso scritto delle famiglie, ma con divieto di divulgazione sui social o mezzi di comunicazione quali Whatsapp di classe o di gruppo classe.

SOCIAL NETWORK

Si invitano gli studenti a non prelevare o diffondere immagini, video o registrazioni audio non autorizzate, e 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 e Whatsapp, 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.

4. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

PREVENZIONE

Il nostro Istituto ha scelto una politica interna tesa a creare un ambiente di apprendimento sereno e sicuro:

- in cui sia chiaro sin dal primo giorno di scuola che (cyber)bullismo, prepotenza e violenza non sono permessi,
- in cui sia stimolata la partecipazione diffusa di tutta la comunità scolastica nelle azioni finalizzate al contrasto del (cyber)bullismo.

Contrastare il bullismo implica la creazione di una comunità solidale, in cui ogni allievo accetta sia il diritto di vivere una scuola senza violenza, sia la responsabilità di difendere i compagni più vulnerabili.

Rischi

I rischi a cui sono esposti gli allievi sono numerosi: comportamenti aggressivi, molestie sessuali, intolleranza ed esclusione tra pari e contro il corpo docente ed ausiliario, autolesionismo, violazione della privacy, gioco d'azzardo on line...

Il nostro Istituto deve pertanto prenderli in considerazione tutti e pianificare azioni sia di prevenzione sia di gestione al verificarsi di possibili casi, attraverso un protocollo di azioni.

Azioni

Il nostro Istituto ha scelto di impegnarsi su più fronti per essere zona libera da (cyber)bullismo:

1. Collaborare con le forze dell'ordine (Carabinieri/Vigili/Polizia Postale) con lezioni informative nelle classi;
2. analizzare la possibilità di attivare programmi di intervento per la prevenzione del bullismo nella scuola primaria;
3. elaborare una proposta di approccio curricolare, inserendo attività di sensibilizzazione nell'azione didattica da svolgere in classe, a cura dei docenti, utilizzando filmati;
4. promuovere la diffusione della conoscenza delle "Linee di orientamento" del MIUR, per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo;
5. presentare la eSafety Policy così redatta agli Organi Collegiali e quindi inserirla nel sistema di Regolamenti della Scuola e renderla pubblica sul sito della Scuola.

RILEVAZIONE

Che cosa segnalare

Le tipologie di comportamenti online da segnalare sono:

- Offese e insulti tramite messaggi di testo, e-mail, pubblicati su social network.
- Diffusione di foto o video che ritraggono situazioni intime, violente o spiacevoli tramite il cellulare, siti web o social network.
- Diffusione di foto o video che ritraggono studenti della scuola o del personale scolastico in situazioni scolastiche imbarazzanti.
- Esclusione dalla comunicazione on-line, dai gruppi.
- Furto, appropriazione di identità, uso e rivelazione ad altri di informazioni personali.

Come accorgersi se un alunno è coinvolto in casi di cyberbullismo

È opportuno tenere presenti alcuni indicatori che ci possono aiutare per verificare se nella classe sono presenti episodi di prevaricazione. Esempi di domande stimolo utili per arrivare all'identificazione del problema sono presenti nei materiali di supporto dell'area scuole del sito ministeriale

Generazioni Connesse.

Come segnalare: con quali strumenti e a chi

La Scuola propone i seguenti strumenti per far uscire allo scoperto il problema:

- **Bully boxes:** cassette situate in alcuni punti della scuola, in cui gli studenti anonimamente potranno segnalare le proprie preoccupazioni o esperienze.
- **Counseling:** un insegnante da individuare in CD (es. referente bullismo o psicologo esperto...) che metta la propria competenza al servizio dei ragazzi (sportello di ascolto).

Dopo la rilevazione del fatto: come gestire le segnalazioni

Le tappe da seguire sono:

- fermare immediatamente l'abuso;
- dare sostegno alla vittima;
- lavorare sul gruppo classe affinché riconosca la gravità dell'accaduto e/o la propria partecipazione, espressa anche attraverso forme passive di coinvolgimento.

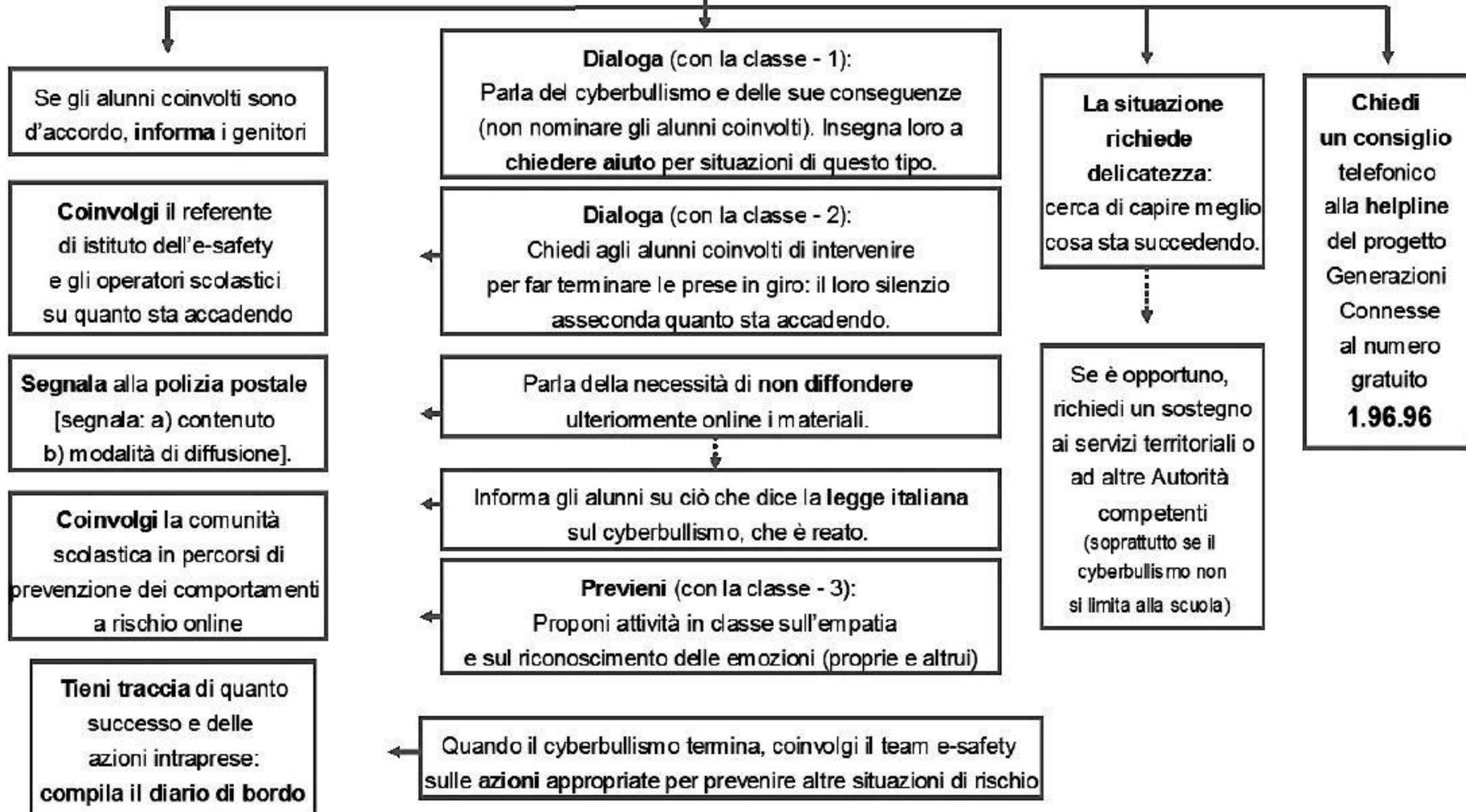
Il coinvolgimento dei coetanei è indispensabile per:

- creare un clima di solidarietà
- incoraggiare le vittime a chiedere aiuto
- sottrarre al (cyber)bullo potenziali proseliti.

La Scuola, in quanto comunità scolastica solidale, si dichiara contraria ad ogni forma di (cyber)bullismo. Perciò verrà proposta e condivisa la procedura descritta nel seguente schema (dal sito **Generazioni Connesse**):

Cosa fare in caso di... cyberbullismo?

Alunno/a preso in giro/minacciato/offeso online



E' previsto anche un monitoraggio costante dei casi segnalati, da realizzare attraverso un diario di bordo da compilare con regolarità.

Schema riepilogativo delle situazioni gestite legate a rischi online

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

© All rights reserved Generazioni connesse 2017

5. LINEE GUIDA PER UNA SCUOLA LIBERA DA CYBERBULLISMO:

Consigli per difendersi dai rischi legati all'uso delle nuove tecnologie

La forma online del bullismo (il cyberbullismo) ha alcune caratteristiche che la rendono particolarmente pericolosa perché:

- il cyberbullismo è pervasivo: la vittima è raggiungibile in qualsiasi luogo e in qualsiasi momento;
- è un fenomeno persistente: il materiale diffamatorio può rimanere disponibile per molto tempo;
- gli “spettatori” del cyberbullismo sono potenzialmente infiniti;
- chi pratica il cyberbullismo può essere anche una persona estranea, può anche agire in gruppo e può rimanere anonimo e protetto da nickname.
- tutti quelli che osservano senza far nulla (o mettono un “like” su un social o condividono o commentano foto o video) diventano corresponsabili del cyberbullismo.

LINEE GUIDA PER GLI STUDENTI

1 Tenere il pc protetto da virus e aggiornato.
2 Non dare informazioni personali senza il permesso dei genitori.
3 Utilizzare password adeguate e non usare la stessa password per più account.
4 Non accettare appuntamenti con persone conosciute solo sulla Rete.
5 Non rispondere a e-mail sospette e non aprire allegati potenzialmente dannosi. Non entrare in siti “a pagamento”.
6 Se un messaggio mette a disagio, non fare ricerche autonome sulla Rete, ma informare subito i genitori.
7 Se su un social o una chat qualcuno disturba o mette a disagio, interrompere ogni contatto.
8 Non pubblicare contenuti imbarazzanti (ottenuti con la webcam) o dannosi o inappropriati.
9 Verificare che ogni indirizzo web inizi con https:// (la s dopo http significa: connessione sicura).
10 Bloccare lo schermo quando non si usa il pc o il telefono, per evitare di essere ripresi in modo involontario.
11 Non inviare messaggi volgari o offensivi.
12 Riflettere bene prima di cliccare, specialmente se si naviga su siti sospetti.
13 Non dimenticare che anche sul web vigono il diritto alla privacy, il diritto ad essere rispettati dagli altri navigatori e la libertà di parola.

LINEE GUIDA PER I GENITORI

Consigli per difendere i propri figli dai pericoli legati all'uso delle nuove tecnologie

- È fondamentale l'accompagnamento all'utilizzo di Internet da parte di un adulto in relazione all'età del bambino.
- I bambini al di sotto dei 10 anni, in genere, non sono in grado di esplorare il web da soli.
- Con la preadolescenza e l'adolescenza si intensifica l'uso di Internet: la supervisione degli adulti è fondamentale anche in questa fase, poiché una maggior conoscenza e consapevolezza legate alla crescita non mettono comunque al riparo dai rischi della Rete.

Ricordare che...

- La protezione non è data solo da filtri da applicare al computer: è fondamentale, invece, il dialogo costante e continuo.
- È anche importante che gli adulti imparino a navigare in Internet e acquisiscano una cultura informatica di base.

LINEE GUIDA PER LA SCUOLA

Suggerimenti per prevenire il cyberbullismo e promuovere un uso critico della rete tra gli studenti

- È proprio nel mondo della scuola che il bullismo, il più delle volte, si genera e si manifesta.
- I giovani difficilmente parlano o si sfogano con gli adulti di quello che succede loro, per non essere scoperti o per paura di peggiorare la loro situazione.
- Ecco perché la scuola è il luogo migliore in cui iniziare a fare prevenzione e in cui promuovere una cultura che veda, nell'altro diverso da sé, solo un altro modo di essere, né migliore né peggiore.

1 Conoscere Internet significa dimostrare agli studenti di essere vicini al loro mondo.

2 È importante conoscere il livello delle conoscenze informatiche degli studenti.

3 È opportuno informare gli alunni sui rischi della Rete senza demonizzarla.

4 È necessario educare gli alunni alla prudenza quando si naviga in Rete.

5 Bisogna educare gli alunni a riconoscere le informazioni non affidabili.

6 I comportamenti illeciti nel mondo reale lo sono anche in Rete.

7 È buona cosa incoraggiare gli alunni a raccontare e discutere in classe le loro esperienze sulla Rete.

8 È necessaria una attenzione continua per impedire che gli alunni accedano, anche involontariamente, a materiali non idonei.

9 Occorre controllare periodicamente gli hard disk della scuola. Il materiale non idoneo trovato deve essere rimosso dall'hard disk ma conservato in una memoria riservata.