



UNIONE EUROPEA



REPUBBLICA ITALIANA



REGIONE SICILIANA

MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA' E DELLA RICERCA

ISTITUTO COMPRENSIVO STATALE "ANTONINO CAPONNETTO"

SCUOLA DELL'INFANZIA "SANTA PETRONILLA" – SCUOLA PRIMARIA "A.CAPONNETTO"

SCUOLA MEDIA STATALE "GIOVANNI VERGA"

Via Maria Montessori, 1 - 93100 **CALTANISSETTA** Tel. e Fax 0934/595552

e-mail clic821009@istruzione.it – clic821009@pec.istruzione.it

Codice Ministeriale. CLIC821009 - C.F.92058470854

E-SAFETY POLICY



INTRODUZIONE

- SCOPO DELLA POLICY

Lo scopo della E-Safety Policy è di stabilire i principi fondamentali tipici di tutti i membri della comunità scolastica per quanto riguarda l'utilizzo di tecnologie; salvaguardare e proteggere i bambini, i ragazzi e lo staff dell'Istituto; assistere il personale della scuola a lavorare in modo sicuro e responsabile con altre tecnologie di comunicazione di Internet e monitorare i propri standard e le prassi; impostare chiare aspettative di comportamento e/o codici di condotta rilevanti per un uso responsabile di Internet a scopo didattico, personale o ricreativo; affrontare gli abusi online come il cyberbullismo, che sono riferimenti incrociati con le altre politiche della scuola; garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito o pericoloso è inaccettabile e che saranno intraprese le opportune azioni disciplinari e giudiziarie.

- **RUOLI E RESPONSABILITÀ (CHE COSA CI SI ASPETTA DA TUTTI GLI ATTORI DELLA COMUNITÀ SCOLASTICA).**

✓ **Dirigente Scolastico:**

È responsabile della presentazione di questo documento all'attenzione del Consiglio di Istituto e al Collegio dei Docenti; deve anche valutare l'efficacia della politica e monitorarne/indirizzarne l'attuazione, anche in collaborazione con personale scolastico, enti locali e stakeholder territoriali. A tale scopo necessita di ricevere tempestive informazioni sulle violazioni al presente regolamento o eventuali problemi attualmente non noti dal corpo docente o dal personale ATA che ne vengano a conoscenza.

✓ **Animatore digitale e Team digitale:**

Curano la redazione e la revisione annuale della policy sulla base delle osservazioni ricevute da tutti i soggetti interessati; ne assicurano la massima diffusione dentro la comunità scolastica in tutte le sue componenti (docenti/ata, genitori e studenti), mediante pubblicazione sul sito della scuola. Riferiscono al Dirigente Scolastico situazioni o problemi di particolare rilevanza su cui intervenire.

✓ **Personale docente**

I docenti devono:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- aver preso visione della presente policy;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'Animatore digitale per le opportune indagini/azioni/sanzioni;
- mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici;
- integrare i problemi di sicurezza informatica in tutti gli aspetti del curriculum di studi e in altre attività extracurricolari;

- far comprendere e mettere in pratica alla componente studentesca le regole di comportamento relative alla sicurezza informatica;
- far nascere nella componente studentesca una buona cognizione della proprietà del software e delle normative sul diritto d'autore nonché di far comprendere la necessità di effettuare ricerche sul web e la relativa estrazione di documenti evitando il plagio o l'illecita diffusione di dati personali;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche ecc. nelle lezioni e nelle altre attività scolastiche che ne prevedono la necessità a scopi didattici;
- guidare la navigazione di studentesse e studenti, nelle lezioni in cui l'uso di Internet è pianificato, verso siti controllati come idonei per il loro uso, onde evitare di incontrare materiali inadatti.

✓ **Personale ATA**

Il personale ATA è tenuto:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- aver preso visione della presente policy;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'animatore digitale per le opportune indagini/azioni/sanzioni;
- mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici.

✓ **Studenti**

Tutti gli alunni sono responsabili per l'utilizzo corretto dei sistemi informatici e della tecnologia digitale in accordo con i termini previsti da questa policy.

In particolare sono tenuti a:

- non utilizzare dispositivi personali durante le attività didattiche se non espressamente consentito dal personale docente:

- avere una buona comprensione delle possibilità di ricerca sul web e della necessità di evitare il plagio, rispettare le normative sul diritto d'autore, non diffondere dati personali;
- comprendere l'importanza della segnalazione di ogni abuso, uso improprio o accesso a materiali inappropriati e conoscere il protocollo per tali segnalazioni;
- conoscere e comprendere le politiche sull'uso di dispositivi mobili e di macchine fotografiche digitali;
- capire le politiche di utilizzo delle immagini ed essere consapevoli del significato e della gravità del cyberbullismo.
- capire l'importanza di adottare buone pratiche di sicurezza informatica in tutti i momenti della vita, a tutela dell'incolumità propria e altrui e per evitare di perpetrare reati punibili sia a livello scolastico sia da parte della magistratura.

✓ **Genitori**

Genitori e tutori svolgono un ruolo cruciale nel garantire che i loro figli comprendano la necessità di utilizzare i dispositivi Internet e mobili in modo appropriato.

La scuola coglierà ogni occasione per sensibilizzare i genitori attraverso incontri con la Polizia postale ed altri esperti o educatori, circolari, sito web e altre comunicazioni telematiche, informazioni su campagne di sicurezza promosse da altre istituzioni o su convegni dedicati a questo tema. I genitori saranno incoraggiati a sostenere la scuola nel promuovere le buone pratiche di e-safety e a seguire le linee guida sull'uso appropriato di:

- immagini digitali e video registrati in occasione di eventi scolastici, anche al di fuori delle aule;
- accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico;
- dispositivi personali dei loro figli nella scuola.

- CONDIVISIONE E COMUNICAZIONE DELLA POLICY ALL'INTERA COMUNITÀ SCOLASTICA.

Questa policy si applica a tutti i membri della comunità scolastica che hanno accesso o che sono utenti dei sistemi informatici della scuola. In particolare essa viene redatta per regolare il comportamento della componente studentesca dentro le aule scolastiche e per sensibilizzarli all'adozione di buone pratiche quando sono fuori dalla scuola e autorizza i membri del personale docente a erogare sanzioni disciplinari per comportamenti inappropriati avvenuti all'interno dell'istituzione scolastica.

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

- condivisione in sede di Collegio dei docenti e inserimento nel PTOF;
- pubblicazione della E-Safety Policy sul sito della scuola;
- comunicazione a genitori e alunni all'inizio dell'anno scolastico e nelle attività di orientamento;
- fornire informazioni agli studenti sull'uso responsabile della rete in modo tale che possano sviluppare "comportamenti sicuri".
- fornire informazioni al personale, agli alunni ed ai genitori su come segnalare azioni di bullismo o cyber-bullismo

- GESTIONE DELLE INFRAZIONI ALLA POLICY.

Le infrazioni alla policy possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori a docenti/ATA. In particolare si attueranno le seguenti operazioni:

- Osservare in modo attento e partecipe quanto accade;
- Coinvolgere se possibile nel dialogo e confrontarsi con il referente e-safety della scuola;
- Confrontarsi con il Dirigente scolastico e valutare l'opportunità di informare la famiglia per creare una rete di supporto e un piano d'azione condiviso;

- Attivare le forze dell'ordine competenti o i servizi del territorio più adeguati.

- **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 e tutte le modifiche della Policy saranno discusse in dettaglio con tutto il personale docente e ATA.

- **INTEGRAZIONE DELLA POLICY CON REGOLAMENTI ESISTENTI.**

La presente policy è allegata in appendice al Regolamento di Istituto.

FORMAZIONE E CURRICOLO

- **CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI.**

L'uso delle TIC va inserito pertanto nel curriculum sia a livello disciplinare sia a livello interdisciplinare. In particolare il curriculum dovrà essere strutturato per prevedere di:

- insegnare ciò che è accettabile nell'utilizzo di Internet e ciò che è vietato, fornendo strumenti per l'utilizzo efficace di Internet e la conoscenza delle conseguenze delle violazioni;
- mostrare come produrre, pubblicare e presentare contenuti digitali in modo appropriato, sia in ambienti privati sia per un pubblico più vasto;
- insegnare la valutazione dei contenuti Internet;
- impiegare materiali prelevati da Internet a scopi didattici conformemente al diritto d'autore;
- rendere alunne e alunni criticamente consapevoli dei materiali che si leggono sul web allo scopo di vagliare le informazioni prima di accettarne la fondatezza, la coerenza, le origini;
- mostrare la segnalazione di contenuti Internet sgradevoli o illegali.

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

Nel PTOF si prevede che una parte della formazione in servizio obbligatoria ai sensi della L. 107/2015 sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica e ai temi informatici in generale. Inoltre si prevede:

- la somministrazione di un questionario rivolto ai docenti per la rivelazione dei bisogni "digitali";
- la formazione dei docenti all'utilizzo del registro elettronico e dello scrutinio elettronico;
- la ricognizione e messa a punto delle dotazioni digitali;
- l'attivazione e comunicazione di iniziative di formazione, in particolare rivolte allo sviluppo e alla diffusione del Coding e del pensiero computazionale;
- la formazione del personale in materia di sicurezza on-line attraverso corsi di formazione e/o aggiornamento;
- il monitoraggio del piano digitale di Istituto e dei risultati conseguiti;

- SENSIBILIZZAZIONE DELLE FAMIGLIE.

Si prevede l'attuazione di un programma continuativo di informazione, consulenza e orientamento per i genitori, attraverso:

- la presentazione ai genitori, i cui figli si scrivono nel nostro Istituto, del regolamento della Policy, al fine di garantire che i principi di comportamento sicuro on-line siano chiari;
- incontri con la Polizia Postale;
- Aggiornamento dei genitori sulle attività svolte dagli studenti in campo digitale in modo da coinvolgerli attivamente .
- incontri di consulenza con esperti;
- informazioni sui siti nazionali di sostegno per genitori, quali il sito www.generazioniconnesse.it.

GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA.

- ACCESSO AD INTERNET: FILTRI ANTIVIRUS E SULLA NAVIGAZIONE.

Si prevede di monitorare il traffico web ed eventualmente di bloccare l'accesso a siti inappropriati ad un contesto scolastico.

Occorre, inoltre, sensibilizzare tutta la comunità scolastica sull'opportunità di mantenere aggiornati gli antivirus installati sulle macchine personali e controllare i dispositivi di archiviazione esterna che vengano collegati al proprio pc.

Inoltre si prevedono i seguenti interventi per regolamentare l'accesso ad internet:

- Controllo della validità e dell'origine delle informazioni a cui si accede o che si ricevono;
- Utilizzo di fonti alternative di informazione per proposte comparate;
- Ricerca del nome dell'autore, dell'ultimo aggiornamento del materiale e di altri possibili link al sito;
- Rispetto dei diritti di autore e dei diritti di proprietà intellettuale.

Il potenziamento della rete permetterà la creazione di connessioni temporanee e gestite dal docente per attività laboratoriali anche del tipo "Bring your own device" (BYOD), in cui l'alunno potrà utilizzare il proprio tablet o notebook.

- GESTIONE ACCESSI (PASSWORD, BACKUP, ECC.).

Ai docenti è consentito accedere ad Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto.

Attualmente gli alunni accedono tramite password personale solo alla piattaforma Edmodo che viene utilizzata in alcune classi per la condivisione di materiale di supporto allo studio. La connessione Wi-Fi ad Internet dalla scuola è regolata da un meccanismo di autenticazione-autorizzazione:.

Gli alunni hanno accesso ai laboratori multimediali guidati da un docente che al termine della lezione verifica lo spegnimento delle postazioni.

- **E-MAIL.**

L'Istituto possiede una casella di posta elettronica istituzionale (@istruzione.it - @pec.istruzione.it) utilizzata per ricevere comunicazioni istituzionali ma anche per comunicare con tutto il personale docente e ATA.

Le comunicazioni tra personale scolastico, famiglie e allieve/allievi via e-mail devono avvenire preferibilmente tramite un indirizzo e-mail della scuola o all'interno del registro elettronico.

- **BLOG E SITO WEB DELLA SCUOLA**

La scuola è dotata di sito internet (www.icscaponnettocl.gov.it).

L'inserimento dei contenuti è possibile solo ai docenti incaricati della gestione del sito web (Funzione strumentale o Referente).

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.

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.

- **SOCIAL NETWORK**

In conformità con le indicazioni fornite annualmente alle scuole dal Garante della privacy si cercherà nella pratica didattica di educare la componente studentesca circa i rischi connessi con l'assunzione, l'uso, la condivisione, la pubblicazione e la distribuzione delle immagini sui social network.

Per esempio a ogni utente sarà consigliato di non fornire mai dati personali di alcun tipo che possano identificare con precisione le persone e la loro residenza o ubicazione.

Alunni, genitori e personale docente/ATA saranno informati sull'uso sicuro degli spazi di social network e sulle conseguenze legali di ogni uso improprio. Gli alunni saranno invitati a usare nickname e avatar non riconoscibili quando utilizzano siti di social networking.

- PROTEZIONE DEI DATI PERSONALI.

I dati personali degli alunni e del personale della scuola sono custoditi e trattati secondo le norme di legge.

Ogni famiglia riceve le credenziali per l'accesso riservato al registro elettronico, in cui il corpo docente è tenuto a registrare assenze, valutazioni, note e osservazioni. La pubblicazione delle informazioni attraverso tale strumento assolve l'obbligo di comunicare prontamente ed efficacemente ogni evento riguardante l'alunno/a.

All'atto dell'iscrizione è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video dei minori.

STRUMENTAZIONE PERSONALE

- PER GLI STUDENTI: GESTIONE DEGLI STRUMENTI PERSONALI: CELLULARI, TABLET ECC..

I telefoni cellulari, i tablet e le relative fotocamere e registratori vocali non verranno utilizzati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate dal corpo docente.

Per gli alunni con bisogni educativi speciali (DSA - BES) si adotteranno le modalità di impiego di strumenti compensativi quali tablet e computer portatili previsti all'interno del PDP.

- PER I DOCENTI E IL PERSONALE DELLA SCUOLA: GESTIONE DEGLI STRUMENTI PERSONALI: CELLULARI, TABLET ECC..

Ogni docente può utilizzare la connessione tramite il pc di classe per la gestione del registro elettronico e per l'attività didattica; alcuni docenti utilizzano propri dispositivi, ma solo a fini didattici.

Telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate.

La password di accesso alla rete wireless va custodita con cura e per nessuna ragione deve essere divulgata a chi non ha titolo per utilizzarla.

Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.

PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

- PREVENZIONE (RISCHI – AZIONI)

Le misure di prevenzione comprendono l'integrazione nel curricolo dei temi legati al corretto utilizzo delle TIC e di Internet. La progettazione di incontri didattici specifici deve essere pianificata, garantendo un intervento su ogni classe, con la presenza del Team digitale o di personale esperto.

La scuola si avvale della collaborazione di enti e associazioni per realizzare incontri rivolti alla componente studentesca e alle famiglie con l'intento di fornire ogni elemento utile alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica.

- RILEVAZIONE

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

La scuola prevede l'attivazione di uno sportello di ascolto al quale la componente studentesca si può rivolgere per avere consigli e sostegno psicologico anche relativamente alle tematiche del cyber-bullismo.

Tra gli strumenti di rilevazione si utilizzeranno il diario di bordo e i questionari, i modelli e gli schemi proposti all'interno del progetto Generazioni Connesse:

Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi Scuola _____ Anno Scolastico _____							
N°	Data	ora	Episodio (riassunto)	Azioni intraprese		Insegnante concui l'alunno/asièconfidato	Firma
				Cosa?	Da chi?		

- **GESTIONE DEI CASI** (definizione delle azioni da intraprendere a seconda della specifica del caso).

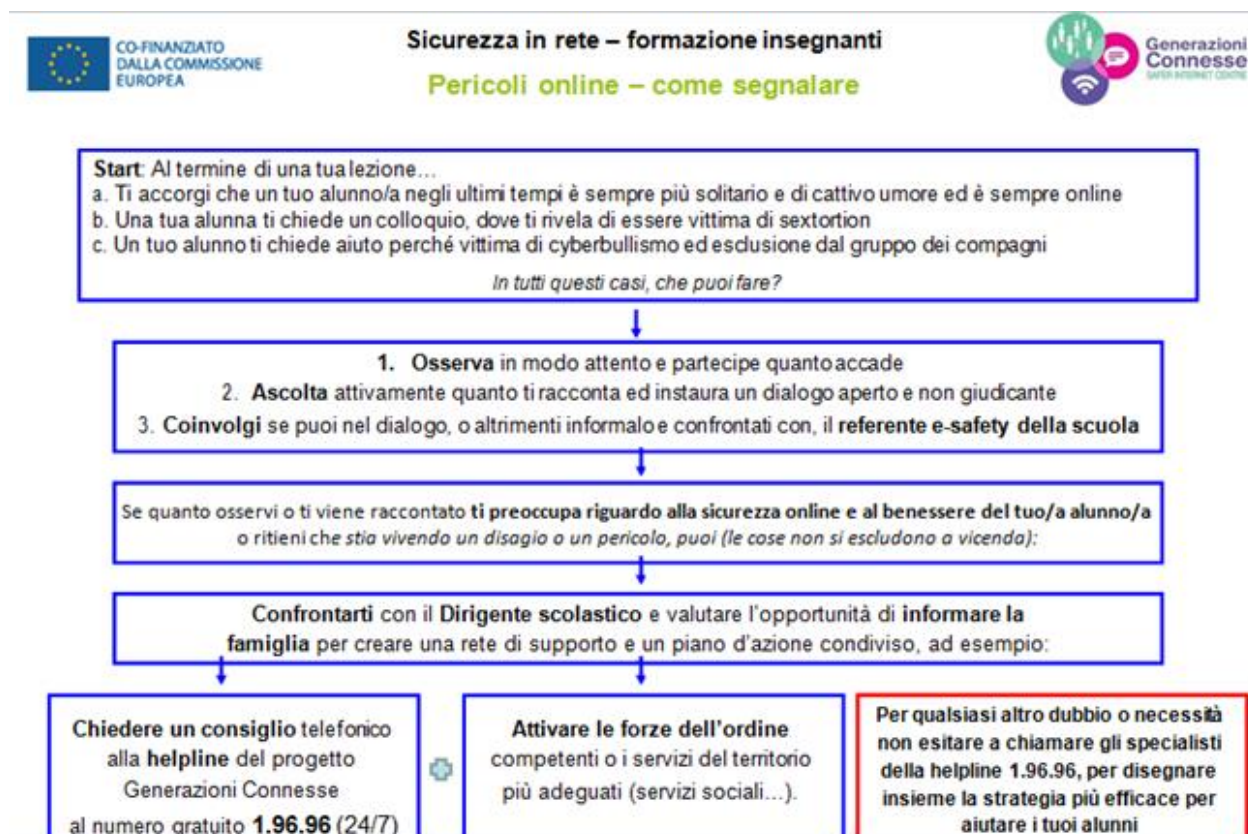
La gestione dei casi rilevati va differenziata a seconda della loro gravità; fermo restando che è opportuna la condivisione a livello di Consiglio di Classe di ogni episodio rilevato, anche minimo, alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe.

Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e come rimediare.

Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire.

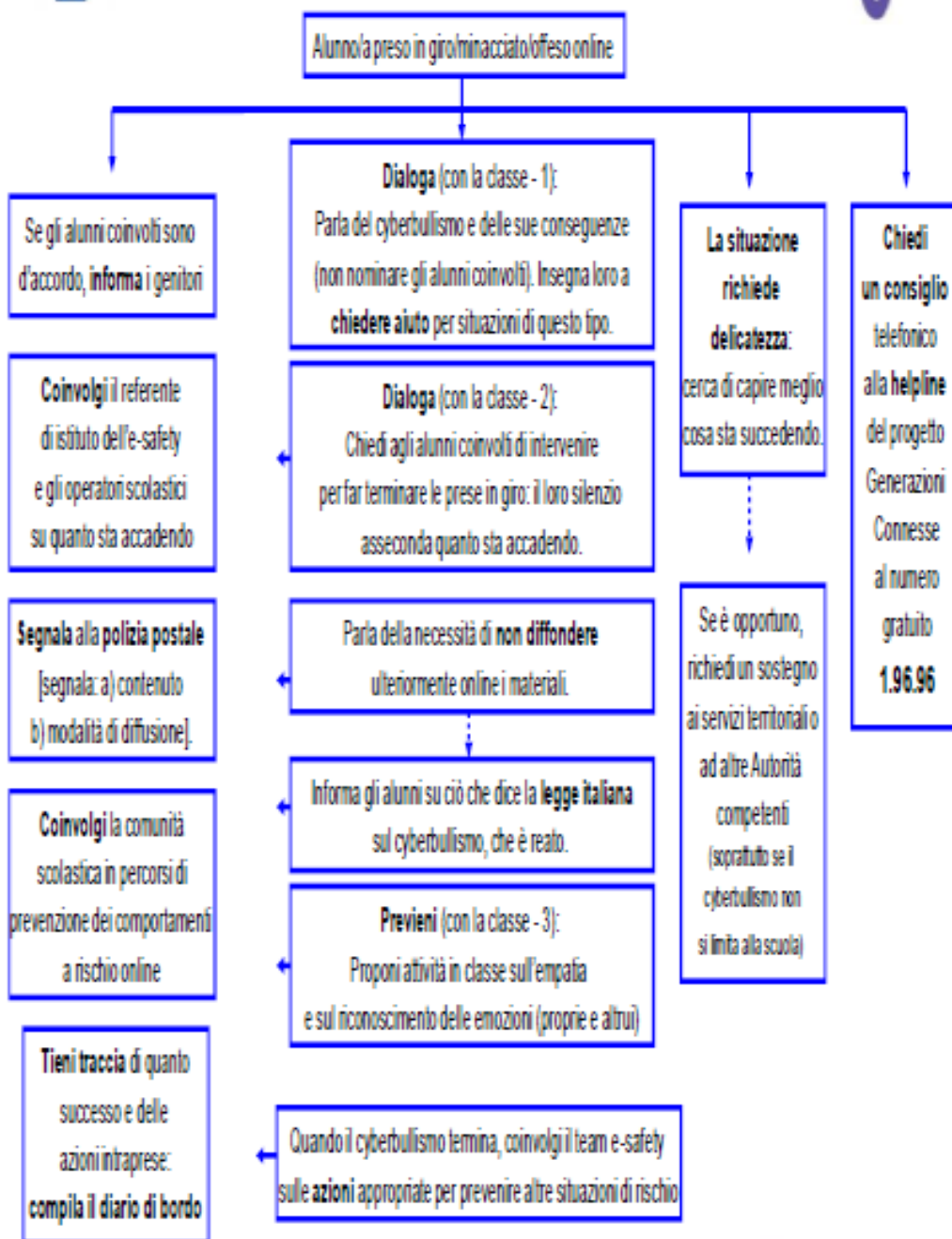
Ogni volta che un membro del personale o studente viola la E-Safety Policy, la decisione finale sul livello di sanzioni sarà a discrezione del Dirigente Scolastico e rifletterà le procedure comportamentali e disciplinari della scuola.

Tra gli strumenti per la segnalazione e gestione dei casi si utilizzeranno i modelli e gli schemi proposti all'interno del progetto Generazioni Connesse:





Sicurezza in rete - Schema per la scuola Cosa fare in caso di... cyberbullismo?



Si prevede inoltre l'applicazione di procedure operative per la gestione delle infrazioni alla E-Safety Policy, seguendo il modello fornito dal progetto Generazioni connesse.

Esempi di possibili infrazioni ed interventi:

STUDENTI:

INFRAZIONI	POSSIBILI SANZIONI
<ul style="list-style-type: none">• L'uso di siti non-educativi durante le lezioni.• L'utilizzo non autorizzato di e-mail.• L'uso non autorizzato del telefono cellulare (o altre nuove tecnologie) durante le lezioni.• Uso di instant messaging / siti di social networking.	Fare riferimento all'insegnante della classe/ E- Safety Coordinator/Dirigente Scolastico
<ul style="list-style-type: none">• L'uso continuato di siti non-educativi durante le lezioni dopo essere stato avvertito.• L'uso non autorizzato di e-mail dopo essere stato avvertito.• L'uso non autorizzato del telefono cellulare (o altre nuove tecnologie) dopo essere stato avvertito.• L'uso continuato messaggistica / chat room istantanea, siti di social networking, newsgroup.• L'uso di materiale offensivo.	Fare riferimento all'insegnante della classe/ E- Safety Coordinator/Dirigente Scolastico Escalation a: <ol style="list-style-type: none">1. rimozione dei diritti di accesso a Internet per un periodo;2. rimozione di telefono fino a fine giornata;3. contatto con i genitori.
<ul style="list-style-type: none">• Rovinare o distruggere deliberatamente i dati di qualcuno, violare la privacy altrui o messaggi inappropriati , video o immagini su un sito di social networking.• Invio di un messaggio e-mail o MSN che è considerato molestia o azione di bullismo.• Cercare di accedere a materiale offensivo o pornografico.	Fare riferimento all'insegnante della classe/ E- Safety Coordinator/Dirigente Scolastico Escalation a: <ol style="list-style-type: none">1. rimozione dei diritti di accesso a Internet per un periodo;2. rimozione del telefono fino a fine giornata;3. contatto con i genitori;4. contattare le autorità competenti.
<ul style="list-style-type: none">• Invio di e-mail o messaggi di MSN considerati molestia o bullismo dopo essere stato avvertito.• Accedere deliberatamente allo scaricamento o alla diffusione di qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofobico o violento.• Trasmissione di materiale che viola i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati.• Portare il nome della scuola in discredito	Fare riferimento all'insegnante della classe / contatto con i genitori Altre possibili azioni di salvaguardia: <ol style="list-style-type: none">1. conservare le prove;2. informare i provider di servizi di posta elettronica del mittente;3. fare rapporto alle autorità competenti dove si sospetti la pedofilia o altre attività illegali.

PERSONALE SCOLASTICO:

INFRAZIONI	POSSIBILI SANZIONI
<ul style="list-style-type: none">• L'uso di Internet per attività personali non legate allo sviluppo professionale (shopping online, e-mail personali, instant messaging ecc.).• L'utilizzo di supporti di memorizzazione dei dati personali (ad esempio, chiavette USB) senza considerare l'accesso e l'adeguatezza di qualsiasi file memorizzato.• Non implementare adeguate procedure di salvaguardia.• Qualsiasi comportamento sul World Wide Web che compromette la professionalità del personale nella scuola e nella comunità.• L'uso improprio di primo livello di sicurezza dei dati, ad esempio uso illecito di password.• Violazione del copyright o della licenza per l'installazione di software .	<p>Fare riferimento all' E-Safety Coordinator/DSGA /Dirigente Scolastico</p> <p>Escalation a:</p> <ol style="list-style-type: none">1. avvertimento
<ul style="list-style-type: none">• Gravi danni intenzionali all'hardware o software del computer.• Qualsiasi tentativo deliberato di violare la protezione dei dati o di sicurezza informatica.• Creare, accedere, scaricare e diffondere deliberatamente qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofobico o violento.• Ricevere o trasmettere materiale che viola i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati.• Portare il nome della scuola in discredito	<p>Fare riferimento all'E-Safety Coordinator/ DSGA /Dirigente Scolastico</p> <p>Altre azioni di salvaguardia:</p> <ol style="list-style-type: none">1. rimuovere il PC in un luogo sicuro per garantire che non vi è alcun ulteriore accesso al PC o laptop;2. far verificare tutte le attrezzature per garantire che non vi è alcun rischio di alunni che accedono a materiali inappropriati nella scuola. <p>Escalation a: Contattare e fare rapporto alle autorità competenti</p>