ISTITUTO COMPRENSIVO "GIOVANNI XXIII"
SCUOLA - INFANZIA – PRIMARIA - SECONDARIA di 1 grado
sede -Via Leonardo da Vinci, 5 - 20842 Besana in Brianza (MB) cod. fiscale 83009720158
tel.+39 0362 995 498 – +39 0362 996 011 fax +39 0362 915 268- cod. Mecc. MIIC83900N
sito internet: www.icbesanainbrianza.gov.it email: miic83900n@istruzione.it

E-Safety Policy
Istituto Comprensivo Giovanni XXIII- Besana in Brianza (MB).

1. Introduzione

- **Scopo della Policy**

Questa policy si applica a tutti i membri della comunità scolastica che hanno accesso o che sono utenti dei sistemi informatici della scuola.
Essa viene redatta per regolare il comportamento della comunità scolastica per quanto riguarda l'uso delle tecnologie e autorizza i membri del personale docente a erogare sanzioni disciplinari per comportamenti inappropriati avvenuti all'interno dell'Istituzione.
La scuola attua parallelamente attività di prevenzione, controllo e formazione di allievi e famiglie allo scopo di ridurre al minimo l'occorrenza di atti che non solo creano disagio nella comunità, ma possono configurarsi come reati, con particolare riferimento alla legge n. 71/2017 sulla tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo.

- **Ruoli e Responsabilità**

Qualsiasi membro della comunità scolastica abbia, in qualsiasi forma, notizia di un episodio ascrivibile alle categorie del bullismo e del cyberbullismo e di uno scorretto uso delle tecnologie è tenuto a darne tempestiva comunicazione al Dirigente Scolastico, al Referente di plesso, al Coordinatore di Classe e al Referente del bullismo e cyberbullismo.

Dirigente Scolastico
-individua attraverso il Collegio dei Docenti un referente del bullismo e del cyberbullismo
-coinvolge, nella prevenzione e contrasto al fenomeno del bullismo e cyberbullismo, tutte le componenti della comunità scolastica, partendo dall'utilizzo sicuro di Internet a scuola
-è responsabile della presentazione entro la fine dell'a.s. 2018-2019 di questo documento all'attenzione del Consiglio di Istituto e al Collegio dei Docenti
-valuta l'efficacia della policy e ne monitora l'attuazione.

Referente del bullismo e cyberbullismo
-promuove la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale
-coordina le attività di prevenzione ed informazione sulle sanzioni previste e sulle responsabilità di natura civile e penale rivolgendosi anche a partner esterni alla scuola
-cura i rapporti di rete fra scuole sul tema
-interviene in caso di segnalazioni di comportamenti scorretti

Referente del bullismo e cyberbullismo in collaborazione con animatore digitale
-cura la redazione e la revisione annuale della policy sulla base delle osservazioni ricevute da tutti i soggetti interessati
-ne assicura la massima diffusione dentro la comunità scolastica in tutte le sue componenti mediante pubblicazione sul sito della scuola

-riferisce al Dirigente Scolastico situazioni o problemi di particolare rilevanza su cui intervenire

Personale docente, con particolare riferimento ai Coordinatori dei Consigli di Classe
- segnala tempestivamente qualsiasi abuso, anche sospetto, o comportamento scorretto al Dirigente Scolastico, al referente del cyberbullismo e all'animatore digitale per le opportune indagini/azioni/sanzioni
- controlla l'uso delle tecnologie digitali e dei dispositivi mobili nelle lezioni e nelle altre attività scolastiche che ne prevedono la necessità a scopi didattici;
- guida la navigazione verso siti controllati nelle lezioni in cui l'uso di Internet è pianificato
-promuove scelte didattiche ed educative, anche in collaborazione con altre scuole in rete, per la prevenzione del fenomeno
- legge, comprende e sottoscrive la presente policy

Personale ATA
- assicura di avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto
- segnala qualsiasi abuso, anche sospetto, al Dirigente Scolastico, al referente del cyberbullismo o all'animatore digitale per le opportune indagini / azioni / sanzioni;
-legge, comprende e sottoscrive la presente policy

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

- non utilizzano dispositivi personali durante le attività didattiche se non espressamente consentito dal personale docente
-non possono acquisire mediante cellulare o altri dispositivi elettronici immagini, filmati o registrazioni vocali se non per finalità didattiche e con l'autorizzazione del docente. La divulgazione del materiale acquisito all'interno dell'istituto è utilizzabile solo per fini esclusivamente personali di studio o documentazione e comunque nel rispetto del diritto alla riservatezza di tutti
-imparano le regole basilari per rispettare gli altri quando sono connessi alla rete
- sono consapevoli del significato e della gravità del cyberbullismo
-segnalano tempestivamente qualsiasi abuso, anche sospetto, o comportamento scorretto al Dirigente Scolastico, al referente del cyberbullismo e all'animatore digitale per le opportune indagini/azioni/sanzioni

Genitori
- sostengono la scuola nel promuovere le buone pratiche di e-safety, partecipano attivamente alle azioni di formazione/informazione istituite dalla scuola sui comportamenti sintomatici del bullismo e del cyberbullismo
-vigilano sull'uso delle tecnologie da parte dei propri figli, con particolare attenzione ai tempi, alle modalità, agli atteggiamenti conseguenti
-conoscono le azioni messe in campo dalla scuola e collaborano secondo le modalità previste dal Patto di corresponsabilità firmato
- seguono le linee guida sull'uso appropriato di immagini digitali e video registrati in occasione di eventi scolastici (anche al di fuori delle aule), sull'accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico e sull'uso di dispositivi personali da parte dei loro figli nella scuola (dove ciò è consentito).

-conoscono le sanzioni previste nei casi di bullismo, cyberbullismo e navigazione on-line a rischio

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

La policy sarà pubblicata sul sito della scuola. L'Istituto si impegna a prendere spunto da essa come base di partenza per una serie di azioni e iniziative.

Per il corpo docente:
- discussione collegiale sui contenuti, sulle pratiche indicate e su come inserire nel curricolo le tematiche di interesse della policy;

Per la componente studentesca:
- la discussione in classe della policy nei primi giorni di scuola

Per i genitori:
- l'organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare

- **Gestione delle infrazioni alla Policy.**

Al personale e agli alunni saranno date informazioni sulle infrazioni dei comportamenti corretti previsti dalla policy e sulle eventuali sanzioni.

Il fenomeno del cyberbullismo è definito dalla Legge 29 maggio 2017, n 71 come "*qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on-line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso o la loro messa in ridicolo".*
In particolare rientrano nel cyberbullismo:

- Flaming: litigi online nei quali si fa uso di un linguaggio violento e volgare
- Harassment: molestie attuate attraverso l'invio ripetuto di linguaggi offensivi
- Cyberstalking: invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità
- Denigrazione: pubblicazione all'interno di comunità virtuali, quali newsgroup, blog, forum di discussione, messaggistica immediata, siti internet, ecc, di pettegolezzi e commenti crudeli, calunniosi e denigratori
- Outing estorto: registrazione delle confidenze- raccolte all'interno di un ambiente privato- creando un clima di fiducia e poi inserite integralmente in un blog pubblico
- Impersonificazione: insinuazione all'interno dell'account di un'altra persona con l'obiettivo di inviare dal medesimo messaggi ingiuriosi che screditino la vittima
- Esclusione: estromissione intenzionale dell'attività online
- Sexting: invio di messaggi via smartphone ed Internet, corredati da immagini a sfondo sessuale

Ulteriori comportamenti rientranti nelle fattispecie previste dalla Legge 71/2017.

I comportamenti scorretti, opportunamente accertati, verranno considerati mancanze gravi e conseguentemente sanzionati sulla base di quanto previsto nel Regolamento di disciplina.

Quando possibile saranno privilegiate le sanzioni disciplinari di tipo riparativo, convertibili in attività a favore della comunità scolastica.
Le denunce di cyberbullismo saranno trattate in conformità con la legge attuale.

- **Monitoraggio dell'implementazione della Policy e suo aggiornamento.**

Il referente del cyberbullismo in collaborazione con l'animatore digitale si prenderà cura della revisione e/o aggiornamento della Policy sotto la supervisione del Dirigente Scolastico.

La policy sarà revisionata annualmente o quando si verificano cambiamenti significativi per quanto concerne le tecnologie in uso nell'Istituto, le modifiche saranno discusse con i membri del collegio docenti.

- **Integrazione della Policy con Regolamenti esistenti.**

La presente policy è allegata in appendice al Regolamento di disciplina. Il Patto di corresponsabilità riprende alcuni dei principi espressi nella policy.

2. Formazione e Curricolo

- **Curricolo sulle competenze digitali per gli studenti.**

  Nell'ambito del Piano nazionale scuola digitale il nostro Istituto si propone di seguire un programma di progressiva educazione alla sicurezza online come parte del curriculum scolastico.
  In particolare il curricolo 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
  - promuovere la prevenzione al cyberbullismo
  - 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

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

  La formazione del corpo docente verrà organizzata su due livelli: interno ed esterno. A livello interno, nel PTOF si prevede che una parte della formazione in servizio ai sensi della L. 107/2015, sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica e ai temi informatici in generale. Tale formazione è svolta in particolare dai docenti dell'Istituto che fanno parte del team digitale, per cui si prevedono opportuni percorsi la cui ricaduta viene annualmente tarata secondo le esigenze formulate dal Collegio Docenti, ed è improntata alla condivisione di esperienze significative e di buone pratiche (corsi previsti dalla Bottega dell'Insegnante).
  Per quanto riguarda la formazione esterna, la scuola assicura tempestiva e capillare informazione su corsi, convegni e seminari che riguardino tali argomenti, cercando di agevolare il personale che intenda parteciparvi. L'Istituto appartiene alla rete generazione web che ha come scopo la formazione digitale.

- **Sensibilizzazione delle famiglie.**

  La Policy viene condivisa con le famiglie. La scuola si propone di organizzare periodicamente incontri genitori-figli sui temi della sicurezza on-line.

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

- Accesso ad internet: filtri, antivirus e sulla navigazione.

Il nostro Istituto prevede di configurare un proxy server per monitorare il traffico web e per bloccare l'accesso a siti inappropriati a 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.

Nei laboratori destinati agli allievi della Scuola Primaria il sistema operativo installato è in parte una distribuzione Linux, allo scopo di ridurre al minimo i costi delle licenze acquistate dalla scuola, formare gli allievi all'uso di prodotti open source, fornire una maggiore protezione da infezioni di virus.

Gestione accessi

L'Istituto attualmente è dotato di una rete wireless destinata all' utilizzo didattico da parte del corpo docente. La password è differenziata a seconda dei plessi.

Ciascun utente connesso alla rete dovrà: rispettare il presente regolamento e la legislazione vigente succitata, tutelare la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui ha accesso e rispettare la cosiddetta netiquette (insieme di regole, comunemente accettate e seguite da quanti utilizzano Internet e i servizi di rete, che disciplinano il comportamento di un utente nel rapportarsi agli altri utenti attraverso risorse come wiki, newsgroup, mailing list, forum, blog o e-mail).

La componente studentesca dovrà impegnarsi a rispettare le norme di buon utilizzo prima che sia concesso l'accesso a Internet.

E-mail

L'Istituto prevede di fornire una casella di posta elettronica univoca a tutto il personale docente e ATA.

Sito web della scuola

I dati di contatto sul sito web devono essere: indirizzo della scuola, e-mail e numero di telefono.

Il personale che è in possesso delle credenziali per la gestione dei contenuti sul portale si assumerà la responsabilità editoriale di garantire che il contenuto inserito sia accurato e appropriato.

Social network

Nella pratica didattica si cerca di educare la componente studentesca all'uso sicuro dei 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.

La componente studentesca non deve pubblicare senza permesso foto personali proprie o altrui su qualsiasi spazio di social network previsto nella piattaforma di apprendimento scolastico (Socloo).

Registro elettronico

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. L'uso del registro elettronico è spiegato alle famiglie nel corso del primo consiglio di classe dell'anno scolastico e la pubblicazione delle informazioni attraverso tale strumento assolve l'obbligo di comunicare

prontamente ed efficacemente ogni evento riguardante l'alunno/a. Coloro che non possono accedere a Internet e di conseguenza non possono consultare il registro elettronico sono pregati di darne segnalazione al coordinatore del consiglio di classe, che verificherà la trascrizione delle comunicazioni sul diario e la firma dei genitori.

Protezione dei dati personali.

Si fa riferimento a tutto quanto previsto dal Decreto legislativo 30 giugno 2003, n. 196 (c. d. Codice della Privacy). Tuttavia, si possono individuare al riguardo alcune linee guida di e-safety:
il personale non deve condividere numeri di telefono personali o indirizzi di posta elettronica privati con la componente studentesca e con i genitori. Un telefono o una e-mail della scuola sarà fornito al personale cui è richiesto il contatto con la componente studentesca o con i genitori.

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

4. Strumentazione personale

Per la componente studentesca

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.
Si chiede alle famiglie di non lasciare tali dispositivi ad alunne e alunni.
Studenti con disturbi specifici di apprendimento, previa consultazione con il Consiglio di Classe, concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili.
Il cellulare sarà requisito dal docente che ravvisa l'infrazione, depositato nella cassaforte della segreteria e consegnato al genitore/tutore convocato, che sarà contestualmente informato dell'eventuale sanzione disciplinare comminata al trasgressore.
Nel caso in cui debbano comunicare con la famiglia durante l'orario scolastico, alunne e alunni possono usare gratuitamente la linea fissa della scuola rivolgendosi a un operatore; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di parlare con i propri figli. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.
L'invio di materiali abusivi, offensivi o inappropriati è vietato, anche se avviene all'interno di cerchie o gruppi di discussione privati.

Per il personale docente/ATA

Le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali. 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 (studenti, genitori, operatori esterni).
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.
Durante l'attività didattica è opportuno che ogni insegnante: - dia chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti ecc.), condividendo con gli studenti la netiquette e indicandone le regole; - si assuma la responsabilità di segnalare prontamente eventuali

malfunzionamenti o danneggiamenti; - non salvi sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili -proponga agli alunni attività di ricerca di informazioni in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento.

5. Prevenzione, rilevazione e gestione dei casi

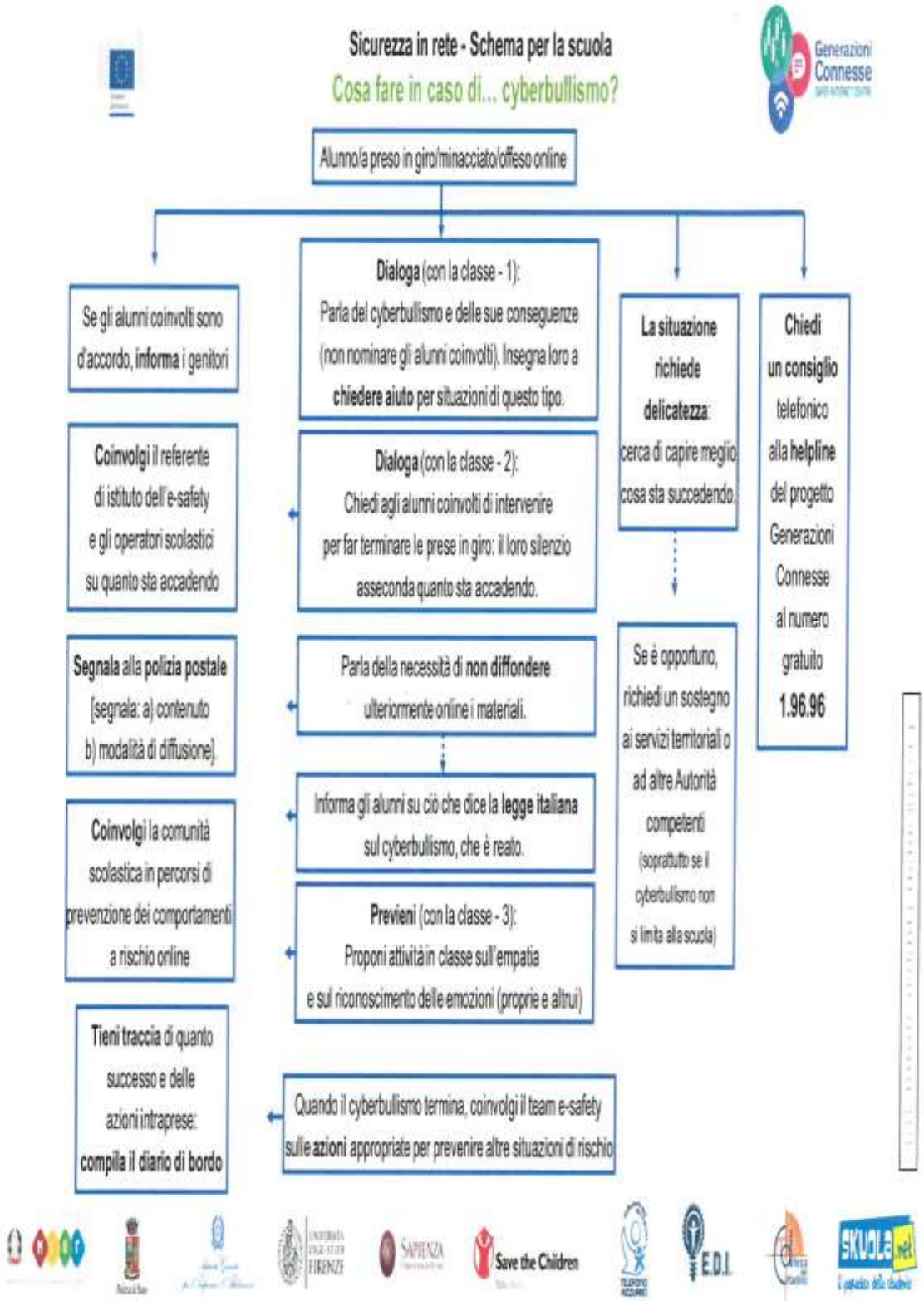
Le misure di prevenzione comprendono l'integrazione nel curricolo dei temi legati al corretto utilizzo delle TIC e di Internet. È previsto inoltre uno specifico percorso di prevenzione al Cyberbullismo per le classi seconde, tale percorso si inserisce nelle ore di Cittadinanza e Costituzione.
La scuola 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; le famiglie sono invitate a proporre tematiche di particolare interesse su cui la scuola focalizzerà il proprio intervento (Progetto famiglia).

La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti. I docenti possono periodicamente monitorare il fenomeno del cyberbullismo nelle classi somministrando agli alunni dei questionari sulla propria esperienza scolastica ed extrascolastica.

La gestione dei casi rilevati va differenziata a seconda della loro gravità; è opportuna la condivisione a livello di Consiglio di Classe e con il referente del cyberbullismo 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 alunni coinvolti per riflettere insieme su quanto accaduto e su come rimediare. Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire. Per un'efficace gestione dei casi la scuola si riserva di utilizzare lo schema messo a disposizione sul sito www.generazioniconnesse.it (Allegato1).

PREVENZIONE, RILEVAZIONE E GESTIONE RISCHI	**AZIONI**
Adescamento online (grooming)	Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione. Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.
Cyberbullismo	Campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni. I casi possono essere molto diversi (dal semplice scherzo di cattivo gusto via sms/Whatsapp a vere e proprie minacce verbali e fisiche, che costituiscono reato). Occorre segnalare ogni caso e confrontarsi con il referente del cyberbullismo e il Dirigente Scolastico sulle azioni da intraprendere.
Dipendenza da Internet. Esposizione a contenuti pornografici, violenti, razzisti.	Informazioni sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito. Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli. Verso la componente studentesca: inserimento nel curricolo di temi legati alla affidabilità delle fonti online, all'interculturalità e al rispetto delle diversità.
Uso di un device senza autorizzazione	Si fa spegnere il device, lo si deposita in segreteria e lo si restituisce al termine delle lezioni ai genitori contestualmente convocati. Nota disciplinare. Se il device è stato utilizzato durante una verifica per copiare, la verifica viene ritirata e viene assegnata una valutazione gravemente insufficiente.

ALLEGATO N.1


Sicurezza in rete - Schema per la scuola
Cosa fare in caso di... cyberbullismo?
Generazioni Connesse
Alunno/a preso in giro/minacciato/offeso online
Se gli alunni coinvolti sono d'accordo, informa i genitori
Dialoga (con la classe - 1): Parla del cyberbullismo e delle sue conseguenze (non nominare gli alunni coinvolti). Insegna loro a chiedere aiuto per situazioni di questo tipo.
La situazione richiede delicatezza: cerca di capire meglio cosa sta succedendo.
Chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse al numero gratuito 1.96.96
Coinvolgi il referente di istituto dell'e-safety e gli operatori scolastici su quanto sta accadendo
Dialoga (con la classe - 2): Chiedi agli alunni coinvolti di intervenire per far terminare le prese in giro: il loro silenzio asseconda quanto sta accadendo.
Segnala alla polizia postale (segnala: a) contenuto b) modalità di diffusione)
Parla della necessità di non diffondere ulteriormente online i materiali.
Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola)
Coinvolgi la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online
Informa gli alunni su ciò che dice la legge italiana sul cyberbullismo, che è reato.
Previeni (con la classe - 3): Proponi attività in classe sull'empatia e sul riconoscimento delle emozioni (proprie e altrui)
Tieni traccia di quanto successo e delle azioni intraprese: compila il diario di bordo
Quando il cyberbullismo termina, coinvolgi il team e-safety sulle azioni appropriate per prevenire altre situazioni di rischio
Save the Children
E.D.I.
SKUOLA.net