MINISTERO DELL' ISTRUZIONE, DELL' UNIVERSITA' E DELLA RICERCA
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
Istituto Comprensivo Statale "VIA SORISO"
Via Soriso, 41 - 00166 ROMA - Tel./Fax 06.6636948
Ambito 8 – Cod. Mecc. RMIC8GL00N – C.F. 80240210585
e-mail: RMIC8GL00N @ ISTRUZIONE.IT
pec:RMIC8GL00N@PEC.ISTRUZIONE.ITsito:www.icviasoriso.gov.it

INDICE
E-Safety Policy

5.1 Prevenzione: - Rischi ; - Azioni
5.2 Rilevazione: - Che cosa segnalare; -Come segnalare: quali strumenti e a chi; - Come gestire le segnalazioni.
5.3 Gestione dei casi: Definizione delle azioni da intraprendere a seconda della specifica del caso.

1. Introduzione

1.1 Scopo della Policy. Questa Policy ha come obiettivo educare alunni, insegnanti e genitori all'uso sicuro, critico e consapevole delle tecnologie digitali e di Internet, promuovendo l'integrazione delle TIC nella didattica, ma al tempo stesso le norme comportamentali per un uso corretto delle stesse, la conoscenza dei rischi, le misure per la prevenzione, la rilevazione e gestione delle problematiche connesse ad un uso non consapevole o non responsabile delle tecnologie digitali. L'I.C. Via Soriso ha aderito al progetto "Generazioni connesse" e, se necessario, opera in collegamento con le forze dell'ordine
1.2 Ruoli e Responsabilità (che cosa ci si aspetta da tutti gli attori della Comunità Scolastica).

RUOLO	**RESPONSABILITA'**
Il Dirigente Scolastico	• garantisce che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle diversità, nonché un utilizzo positivo e responsabile delle TIC; • garantisce l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line; • garantisce che la scuola utilizzi un Internet Service filtrato approvato, conforme ai requisiti di legge vigenti
DSGA	• assicura, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni ; • garantisce il funzionamento dei diversi canali di comunicazione della scuola (circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente Scolastico nell'ambito dell'utilizzo delle tecnologie digitali e di Internet.
Docente referente del bullismo	• cura la redazione della Policy e ne assicura la massima diffusione nella comunità scolastica in tutte le sue componenti mediante pubblicazione sul sito della scuola; • fa in modo che tutto il personale sia a conoscenza delle procedure che devono

	essere seguite in caso di incidente per la sicurezza online; • coordina le azioni della scuola con le autorità locali e le agenzie competenti; • controlla probabili azioni di cyber-bullismo.
Animatore Digitale e Team Digitale	• Promuovono l'aggiornamento dei docenti • Propongono e promuovono l'uso delle TIC • Cura la tenuta del registro di incidenti di sicurezza online;
Docenti	• danno chiare indicazioni sul corretto utilizzo della strumentazione multimediale e di Internet, agli alunni; • segnalano prontamente eventuali malfunzionamenti o danneggiamenti al Team digitale • non divulgano le credenziali di accesso alla rete Wi-Fi; • si informano/si aggiornano sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e sulla politica di sicurezza adottata dalla scuola; • garantiscono che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di Internet; • nelle lezioni in cui è programmato l'utilizzo di Internet, guidano gli alunni a siti controllati e verificati come adatti per il loro uso; • segnalano 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.
Il Personale ATA	• ha adeguata consapevolezza circa le questioni di sicurezza informatica, la politica dell'Istituto e relative buone pratiche; • segnala qualsiasi abuso, anche sospetto, al Dirigente Scolastico, o ai suoi collaboratori, o all'Animatore Digitale per le opportune indagini / azioni / sanzioni.
Gli studenti	• utilizzano le TIC su indicazione e sotto il controllo del docente; • in caso di riscontro di malfunzionamenti della strumentazione e/o di contatto accidentale con informazioni, immagini e/o applicazioni inappropriate devono comunicarlo immediatamente all'insegnante; • portano a scuola e utilizzano i propri dispositivi esterni personali solo con il

	permesso da parte dell'insegnante e per motivi didattici; • chiudono correttamente la propria sessione di lavoro; • archiviano i propri documenti in maniera ordinata e facilmente rintracciabile in una cartella personale (con il proprio nome e classe) • devono essere consapevoli dei problemi di sicurezza connessi con l'uso di telefoni cellulari, telecamere e dispositivi portatili; • hanno massima cura nell'utilizzo delle attrezzature tecnologiche della scuola e devono comprendere l'importanza di adottare buone pratiche di E-Safety anche quando utilizzano tecnologie digitali al di fuori della scuola
I genitori	• devono sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle Tecnologie dell'Informazione e delle Comunicazioni nella didattica; • seguono gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllano l'utilizzo del pc e di Internet; • concordano con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di Internet; • fissano delle regole per l'utilizzo del computer e controllano l'uso che i figli fanno di Internet e del telefono cellulare in generale.

1.3 Condivisione e comunicazione della Policy alla comunità scolastica. Il presente documento sarà diffuso tra tutto il personale scolastico. Gli alunni saranno informati che l'uso della rete e di tutti i dispositivi digitali, sia di proprietà della scuola sia dell'alunno, sarà possibile solo con l'autorizzazione e il controllo degli insegnanti. Contestualmente verranno informati gli alunni dei rischi connessi ad un uso improprio della rete. Le famiglie saranno informate della Policy di E-Safety in Consiglio di Istituto, nelle assemblee di inizio anno e tramite la pubblicazione sul sito.
Annualmente verranno organizzati incontri dedicati alla prevenzione dei rischi associati all'utilizzo di Internet e delle tecnologie digitali, rivolti agli studenti delle classi V e/o ai genitori, con il coinvolgimento di esperti e di Forze dell'ordine.

1.4 Gestione delle infrazioni alla Policy. Si prevede di aggiornare ed integrare il regolamento scolastico vigente nella parte che riguarda l'uso dei dispositivi digitali, sia di proprietà dell'alunno, sia della scuola. Riguardo le sanzioni alle infrazioni, essendo gli alunni ancora piuttosto piccoli, si interverrà eventualmente, nelle forme e modi previsti dal regolamento di istituto dando, contemporaneamente, particolare rilievo all'educazione all'affettività ed alla cittadinanza, cercando di portare l'alunno ad una maggiore consapevolezza di sé e al rispetto degli altri. In base alla gravità del comportamento si provvederà alla convocazione dei genitori.

1.5 Monitoraggio dell'implementazione della Policy e suo aggiornamento. Il monitoraggio dell'implementazione della Policy e il suo eventuale aggiornamento sarà svolto annualmente dal Dirigente Scolastico con la collaborazione dell'Animatore Digitale, del Team per l'innovazione e del Referente per il bullismo e cyberbullismo. Il monitoraggio potrà essere svolto anche tramite questionari da somministrare a docenti, alunni e genitori per verificare l'efficacia della Policy e la necessità di eventuali miglioramenti.

1.6 Integrazione della Policy con Regolamenti esistenti. La Policy va ad integrarsi con gli obiettivi del PTOF, con il regolamento di istituto e con la normativa vigente.

2. Formazione e Curricolo

2.1 Curricolo sulle competenze digitali per gli studenti. Inserita nelle otto Competenze chiave di cittadinanza attiva indicate dal Consiglio di Lisbona nel marzo 2000 e definita dalla "Raccomandazione del Parlamento europeo e del Consiglio" del 18 dicembre 2006, relativa a competenze chiave per l'apprendimento permanente (2006/962/CE), "La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione per il lavoro, il tempo libero e la comunicazione. Essa implica abilità di base nelle tecnologie dell'informazione e della comunicazione (TIC): l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet." Il Curricolo della scuola del primo ciclo di istruzione sulle competenze digitali per gli alunni è trasversale alle discipline previste dalle Indicazioni Nazionali 2012. Pertanto tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione.
L'I.C. Via Soriso ha partecipato e vinto alcuni progetti PON, inoltre faparte di una rete di istituzioni scolastiche tra le quali si possono realizzare collegamenti in rete e attività didattiche aggiuntive anche in modalità e-learning e con il supporto di un docente e/o tutor. Si ritengono prioritari per la scuola i seguenti obiettivi di cui al comma 7 della legge 107/15: H) sviluppo delle competenze digitali degli studenti, con particolare riguardo al pensiero computazionale, all'utilizzo critico e consapevole dei social network e dei media nonché alla produzione; L) prevenzione e contrasto di ogni forma di discriminazione e del bullismo, anche informatico.

2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica. Una elevata percentuale di docenti ha partecipato nell'a. s. 2016/2017 al Corso Flipnet sulla classe capovolta per la Scuola Primaria (ambito 08) ed alcune docenti hanno deciso di adottare questa metodologia nella propria classe dal corrente anno scolastico.Tutte le insegnanti sono disponibili ad accogliere iniziative di formazione sulle competenze avanzate di didattica digitale, o alla formazione che proporrà l'Animatore Digitale e i docenti del Team per l'Innovazione, come previsto dal PNSD.

2.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali. La formazione dei docenti sull'utilizzo consapevole e sicuro di Internet, è cominciata con l'adesione al progetto di autoaggiornamento "Generazioni Connesse" del Safer Internet Center dove le insegnanti possono consultare materiali informativi sulla sicurezza in Internet reperibili sul sito www.generazioniconnesse.it. Numerosi insegnanti hanno partecipato ad un corso di formazione organizzato dalla Questura di Roma su bullismo e cyberbullismo.

2.4 Sensibilizzazione delle famiglie. La scuola provvederà alla pubblicazione e diffusione del presente documento di Policy di E-Safety, contenente le informazioni e le procedure sull'utilizzo delle nuove tecnologie all'interno dell'Istituto, al fine di prevenire i rischi legati a un utilizzo non

corretto di Internet. Allo scopo, verranno privilegiati gli incontri degli Organi Collegiali partecipativi.
Si prevede anche di organizzare incontri di formazione con i genitori e le Forze dell'ordine (Polizia Postale, Carabinieri).

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

3.1 Accesso ad internet: filtri, antivirus e navigazione. L'accesso ad Internet è possibile e consentito per la didattica nei due plessi dell'Istituto, attraverso reti LAN e WiFi,; il lavoro sulle postazioni fisse è controllato dai docenti.

3.2 Gestione accessi (password, backup, ecc.). L'accesso alla rete è comune per ogni plesso e permette tramite rete LAN o WiFi (attraverso l'impostazione di una password) di accedere al web per esigenze didattiche e per redigere giornalmente il registro elettronico.

3.3 E-mail. La posta elettronica istituzionale gestita dalla segreteria è protetta da antispam così come quella certificata.

3.4 Sito web della scuola. La scuola attualmente ha un sito web aggiornato, all'occorrenza, anche quotidianamente.

3.5 Social network. Attualmente nella didattica non si utilizzano social network, né l'istituzione scolastica vi ha creato una pagina col proprio profilo o ha autorizzato il personale scolastico a utilizzarli per nome e per conto della stessa.

3.6 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 ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione).
All'atto dell'iscrizione, viene fornita ai genitori una specifica informativa e l' autorizzazione all'utilizzo dei dati personali degli alunni.
Per ogni progetto e/o concorso, al quale le docenti aderiscono, se necessario, viene chiesta ai genitori un'autorizzazione particolareggiata per quella determinata iniziativa.

4. Strumentazione personale

4.1 Per gli studenti: gestione degli strumenti personali. Durante l'orario scolastico è consentito l'uso di dispositivi elettronici solo con l'autorizzazione ed il controllo da parte degli insegnanti e solo per motivi didattici. I predetti dispositivi, quando non in uso per scopi didattici, dovranno essere spenti. All'interno di tutti i locali della scuola, nelle sedi utilizzate per l'attività didattica come palestre, aule e laboratori sono vietate riprese audio e video di ambienti e persone, salvo in caso di esplicita autorizzazione del docente responsabile. La violazione di tale divieto configura un'infrazione disciplinare rispetto alla quale la scuola è tenuta ad applicare apposite sanzioni ispirate al criterio di gradualità e alle finalità educative della scuola.

4.2 Per i docenti: gestione degli strumenti personali. Durante le lezioni è consentito l'utilizzo di smartphone, tablet, ecc. personali solo a scopo didattico, ad integrazione degli strumenti scolastici disponibili.

5. Prevenzione, rilevazione e gestione dei casi

5.1 Prevenzione – Rischi. I rischi in cui possono incorrere gli studenti nell'uso delle tecnologie digitali a scuola sono legati principalmente a: 1) uso improprio degli strumenti personali; 2) rischi legati alla navigazione in Internet mediante gli strumenti presenti a scuola. Nel primo caso, gli strumenti potrebbero essere usati per scopi non didattici. I rischi principali sono: a) acquisire e pubblicare su chat, social, ecc. foto o video propri o di altri, b) pubblicare messaggi o commenti lesivi della dignità o della reputazione altrui c) accedere a contenuti e siti non adatti ai minori, d) utilizzare giochi, chat, ecc. e) entrare in contatto con sconosciuti

Nel secondo caso i rischi principali sono: a) visionare contenuti inappropriati b) infettare i computer o i tablet con virus o malware scaricando materiali, installando programmi e applicazioni, utilizzando dispositivi personali di memoria come pennette USB c) utilizzare materiale illegale, violare il diritto d'autore o di proprietà.

- Azioni. La scuola si propone di intervenire per limitare tali rischi e prendere tutte le misure atte a favorire e migliorare la sicurezza informatica, che riguardano anche i tipi di software utilizzabili. Si consiglia inoltre agli insegnanti di non archiviare dati su strumenti personali.

Le azioni specifiche adottate dalla scuola sono riportate sul modulo di implementazione della sicurezza informatica di cui alla circolare AGID 2/17 pubblicato all'albo on-line.

La scuola può avvalersi della collaborazione di enti e Forze dell'ordine per realizzare incontri rivolti agli alunni di V e alle famiglie con l'intento di fornire ogni elemento utile alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica. L'I.C. Via Soriso attiva ogni anno uno sportello di ascolto psicologico al quale i genitori si possono rivolgere per avere consigli e sostegno.

L'azione principale della scuola va verso l'educazione degli alunni ad un uso consapevole e responsabile di Internet e delle tecnologie digitali, sia a scuola sia a casa. Pertanto sarà necessario insegnare agli alunni a:

- proteggere la propria identità, non divulgando i dati personali;
- creare password efficaci;
- riflettere sulle possibili conseguenze prima di postare foto o video propri e non postare foto e video di altri senza il loro consenso;
- rispettare il copyright, quando si utilizza materiale trovato in rete, citando le fonti;
- confidarsi con un adulto quando ci si trovi di fronte a situazione che possono spaventare, far sentire a disagio, offendere, o quando si ricevano richieste inappropriate di informazioni, foto..;
- essere a conoscenza dei servizi messi a disposizione dal Safer Internet Center per segnalazioni, anche anonime, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la rete: "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children e della linea di ascolto 1.96.96 di Telefono Azzurro che accoglie qualsiasi richiesta di ascolto e di aiuto da parte di bambini/e e ragazzi/e fino ai 18 anni o di adulti che intendono confrontarsi su situazioni di disagio/pericolo in cui si trova un minorenne e relativamente a dubbi, domande o problemi legati all'uso delle nuove tecnologie digitali e alla sicurezza online.

5.2 Rilevazione. I docenti che dovessero rilevare una situazione di rischio o di disagio in cui venga a trovarsi un alunno, sia sulla base delle proprie osservazioni, sia su segnalazioni dell'alunno interessato o dei compagni, valuteranno caso per caso la necessità di attivare interventi educativi in classe, informare il Dirigente Scolastico e le famiglie . Nei casi più gravi il Dirigente provvederà ad

informare le Forze dell'ordine. Allo stesso modo i docenti saranno tenuti a segnalare ogni tipo di utilizzo improprio delle tecnologie digitali all'interno della scuola, che possano mettere a rischio la propria o altrui sicurezza.
Nell'ambito del PNSD l'I.C. Via Soriso si propone un programma di progressiva educazione alla sicurezza online come parte del curriculum scolastico. Si impegna a sviluppare una serie di competenze e comportamenti adeguati all'età degli alunni tra cui:

- programmare attività e far partecipare gli alunni a laboratori di Coding in occasione della Settimana del codice;
- sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettare l'esattezza;
- sapere come restringere o affinare una ricerca;
- capire il comportamento accettabile quando si utilizza un ambiente online, vale a dire, essere educato, non utilizzare comportamenti inappropriati, mantenere le informazioni personali private;
- capire come le fotografie possono essere manipolate e individuare contenuti web in grado di attrarre il tipo sbagliato di attenzione;
- capire perché "amici" on-line potrebbero non essere chi dicono e comprendere perché dovrebbero fare attenzione in un ambiente online;
- capire il motivo per cui non dovrebbero inviare o condividere resoconti dettagliati della loro vita personale e informazioni di contatto;
- capire il motivo per cui non devono pubblicare foto o video di altri senza il loro permesso;
- sapere di non scaricare alcun file - come i file musicali - senza permesso;
- comprendere l'impatto di bullismo online, sexting, grooming e sapere come cercare aiuto se sono in pericolo;
- comprendere che giocare in modalità on-line non è privo di pericoli;
- sapere come segnalare eventuali abusi tra cui il bullismo on-line e come a chiedere aiuto ai docenti, ai genitori, se si verificano problemi quando si utilizzano le tecnologie Internet;
- utilizzare con attenzione Internet per garantire che si adatti alla loro età e supporti gli obiettivi di apprendimento per le aree curriculari specifiche.

Che cosa segnalare? Le tipologie di comportamenti online da segnalare sono:
1. Offese e insulti tramite messaggi di testo, e-mail, pubblicati su social network o tramite telefono (ad esempio telefonate mute);
2. Diffusione di foto o video che ritraggono situazioni intime, violente o spiacevoli tramite il cellulare, siti web o social network;
3. Esclusione dalla comunicazione on-line, dai gruppi;
4. Furto, appropriazione, uso e rivelazione ad altri di informazioni personali come le credenziali d'accesso all'account e-mail, social network, ecc.
Come accorgersi se un alunno/un'alunna è coinvolto/a in casi di (cyber)bullismo? Esempi di domande stimolo utili per arrivare all'identificazione del problema sono presenti nei materiali di supporto dell'area scuole del sito generazioni connesse www.generazioniconnesse.it (6.1.1 agire).

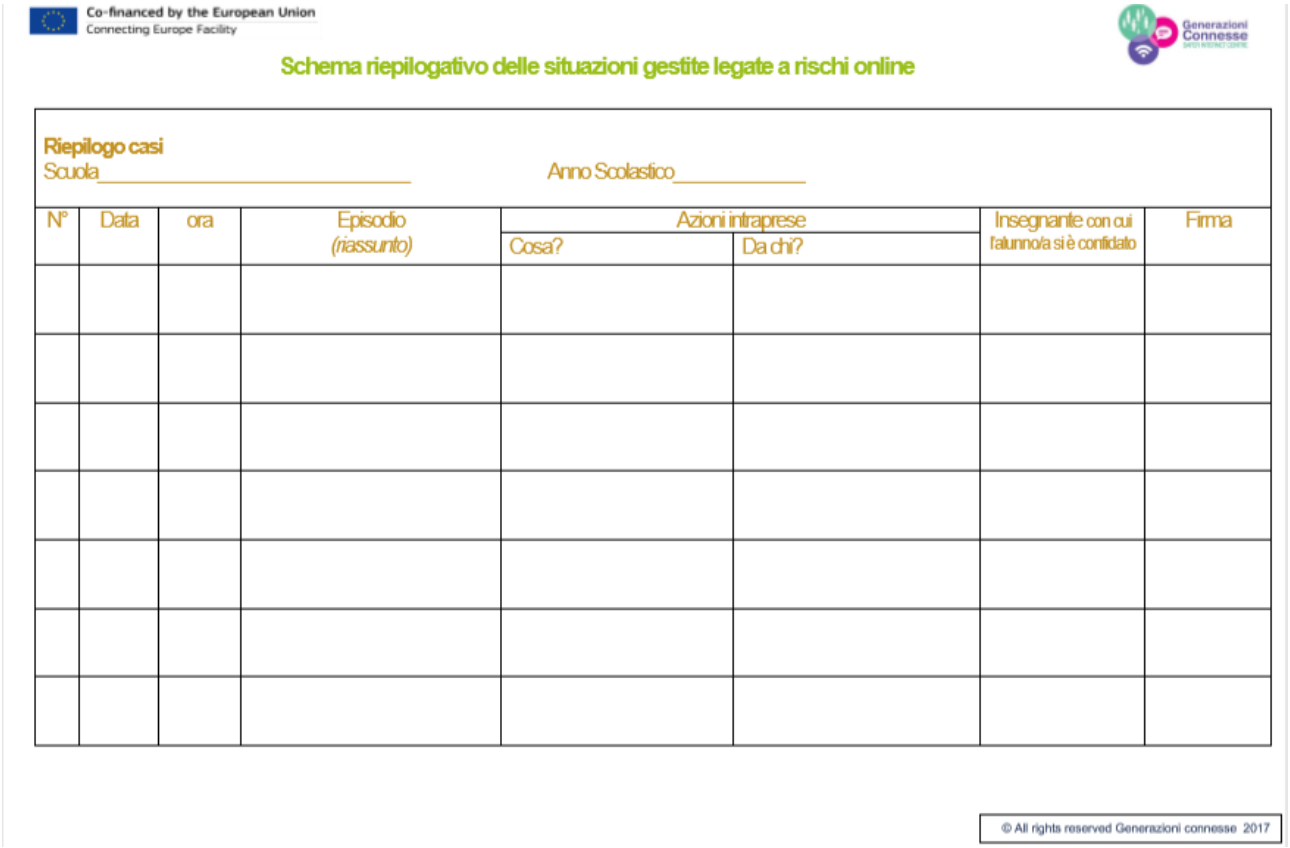
5.3 Gestione dei casi. Come gestire le segnalazioni? Le tappe da seguire quando si presenta un caso di bullismo o cyberbullismo sono:

- fermare immediatamente l'abuso;
- dare sostegno alla vittima;
- lavorare sul gruppo classe affinché riconosca la gravità dell'accaduto;
- dare supporto al bullo con un programma educativo.

Come già detto per la prevenzione, 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

La Scuola in quanto comunità scolastica solidale si dichiara contraria ad ogni forma di bullismo e cyberbullismo. Perciò verrà proposta e condivisa la procedura descritta nel seguente schema per la rilevazione di eventuali casi e suggerita dal sito "Generazioni connesse":



Co-financed by the European Union
Connecting Europe Facility

Generazioni Connesse

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?		

Il presente documento è stato approvato dal Collegio dei Docenti in data 25/01/18 con delibera n. 25. Verrà, quindi, presentato al Consiglio di Istituto per la relativa delibera.

Il docente referente
Viviana Balzamonti

IL DIRIGENTE SCOLASTICO
Daniela Porfiri
(Firma autografa sostituita a mezzo stampa ex art. 3, c.2 D.Lgs n. 39/93)