Ministero dell'istruzione e del merito
Istituto Comprensivo Statale "Don Milani"
Via Don Milani snc – 20085 LOCATE DI TRIULZI (MI) - Tel. 02 90780494
CM MIIC88500B - e-mail: MIIC88500B@istruzione.it - pec: MIIC88500B@pec.istruzione.it
C.F. 97029000151 - IPA: istsc_miic88500B - CODICE UNIVOCO: UFG4BB
sito: https://scuolalocate.edu.it

E-Policy IC Don Milani di Locate di Triulzi

1. INTRODUZIONE

L'Istituto Comprensivo Don Milani di Locate di Triulzi negli ultimi anni ha rafforzato la propria vocazione all'uso delle nuove tecnologie garantendo la presenza in tutte le classi dei plessi di scuola dell'infanzia, primaria e secondaria di una LIM o di uno schermo di grande formato e di un dispositivo PC/iPad/Apple TV per il collegamento alla Rete. In tutto l'istituto sono presenti una rete internet veloce e carrelli con tablet in ogni plesso. Alla scuola secondaria, in tutte le classi, è previsto un modello diffuso di didattica con il digitale che prevede l'uso di un dispositivo individuale iPad per ciascuno degli alunni.

L'istituto, quindi, distribuisce al personale e agli alunni, a partire dalla classe prima della scuola primaria, un account grazie all'adozione di Google Workspace for Education (si veda il "Piano scolastico per la didattica digitale d'istituto" sul sito della scuola) e attiva i blog di classe.

L'uso delle nuove tecnologie, però, espone gli utenti a grandi rischi soprattutto quando non affiancato da un'adeguata formazione sui modi legittimi di usare la rete.

La nostra Scuola ha deciso di sviluppare e attuare il progetto "Generazioni Connesse" (www.generazioniconnesse.it) attraverso la realizzazione di tre linee di intervento:

A. 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;

B. la promozione nei confronti degli alunni della competenza digitale e della cultura del rispetto di regole comuni nell'uso dei servizi telematici (**competenza di cittadinanza digitale**) e lo sviluppo di regole di buon comportamento (Netiquette) riferite specialmente ai Social Network e della conoscenza delle condizioni del loro utilizzo (in questa direzione, l'inserimento di un'ora di cittadinanza digitale nelle classi prime, seconde e terze a tempo prolungato della scuola secondaria);

C. la messa a punto di una procedura per la gestione delle problematiche e di un insieme di attività per la prevenzione dei rischi, articolate in interventi nelle classi.

Le presenti linee guida sono state concepite come parte integrante del Regolamento di Istituto, dopo essere state portate a conoscenza degli Organi Collegiali. La scuola ne promuove la conoscenza presso tutta la comunità.

2. RIFERIMENTI NORMATIVI

Il bullismo e il cyberbullismo devono essere conosciuti e combattuti. I principali riferimenti legislativi sul tema – per quanto riguarda i diritti degli alunni, la tutela del loro benessere, i possibili reati che potrebbero configurarsi con condotte di bullismo e cyberbullismo - sono rinvenibili:

- negli art. 3 (Principio di uguaglianza) e 34 della Costituzione italiana (diritto allo studio)
- nella Direttiva Ministeriale n.16 del 5 febbraio 2007 recante "*Linee di indirizzo generali ed azioni a livello nazionale per la prevenzione e la lotta al bullismo*";
- nella direttiva Ministeriale n. 30 del 15 marzo 2007 recante *"Linee di indirizzo ed indicazioni in materia di utilizzo di '*telefoni cellulari' *e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità dei genitori e dei docenti*";
- nella direttiva Ministeriale n. 104 del 30 novembre 2007 recante "*Linee di indirizzo e chiarimenti interpretativi ed applicativi in ordine alla normativa vigente posta a tutela della privacy con particolare riferimento all'utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire e/o divulgare immagini, filmati o registrazioni vocali*";
- nei DPR 249/1998 e 235/2007 ("*Statuto delle studentesse e degli studenti*") per la scuola secondaria;
- nelle Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo, MIUR aprile 2015;
- negli art. 581 (percosse) - 582 (lesione personale) - 595 (diffamazione) - 610 (violenza privata) - 612 (minaccia) - 635 (danneggiamento) del Codice Penale;
- negli art. 2043 (risarcimento per fatto illecito) - 2047 (danno cagionato dall'incapace) – 2048 (responsabilità dei genitori, dei tutori, dei precettori e dei maestri d'arte) del Codice Civile.
- nelle Linee di orientamento per la prevenzione e il contrasto del cyberbullismo, MIUR ottobre 2017;
- nella Legge del 29 maggio 2017 n.71 *("Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo*"), così come aggiornata dalla legge 17 maggio 2024, n. 70;

3. RUOLI E RESPONSABILITÀ

RUOLO	RESPONSABILITÀ

Il Dirigente Scolastico	• Ha la responsabilità generale per i dati e la sicurezza dei dati. • Individua attraverso il Collegio dei Docenti un referente del bullismo e cyberbullismo. • Favorisce la discussione all'interno della scuola, attraverso gli organi collegiali, creando i presupposti di regole condivise di comportamento per il contrasto e la prevenzione dei fenomeni del bullismo e del cyberbullismo. • Si assicura che il personale riceva una formazione adeguata per svolgere i ruoli di sicurezza online e per la formazione di altri colleghi. • È a conoscenza delle procedure da seguire in caso di infrazioni della E–Safety Policy. • Stabilisce e rivede la E-Safety Policy. • Si coordina con le autorità locali e le agenzie competenti. • Coinvolge nella prevenzione e contrasto al fenomeno del bullismo/cyberbullismo tutte le componenti della comunità scolastica.
I responsabili della sicurezza online (DS, DSGA e DPO)	• Si attivano affinché tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente per la sicurezza online. • Vigilano in relazione a probabili azioni di cyberbullismo.
L'Animatore Digitale/referente per la prevenzione del Bullismo/Cyberbullismo, le funzioni strumentali relative al digitale, i referenti per il digitale dei plessi, i docenti di cittadinanza digitale	• Promuovono la diffusione dei contenuti della E-Policy e organizzano formazioni e/o attività volte all'uso sicuro e consapevole del web. • Promuovono la formazione educativa sul rispetto della privacy. • Propongono soluzioni metodologiche didattiche innovative e tecnologiche sostenibili. • Installano e aggiornano frequentemente il programma antivirus.
Gli insegnanti	• Inseriscono tematiche legate alla sicurezza online nelle progettazioni annuali e in altre attività scolastiche. • Supervisionano e guidano gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono la tecnologia online. • Garantiscono che gli alunni siano pienamente consapevoli delle capacità di ricerca e dei problemi legali relativi ai contenuti elettronici come, per esempio, le leggi sul copyright. • Controllano l'accesso a materiali illegali /inadeguati. • Segnalano eventuali malfunzionamenti o danneggiamenti. • Si assicurano che il device eventualmente in uso alla classe sia custodito. • Sono tenuti a conoscere e mettere in pratica i regolamenti redatti dall'Istituto. • Segnalano al dirigente scolastico e alla referente per il Bullismo / Cyberbullismo abusi rilevati a scuola nei confronti degli alunni in relazione all'uso delle tecnologie digitali o di Internet, per l'adozione delle procedure previste dalle norme e della comunicazione ai genitori. • Sono invitati a partecipare alle attività di formazione proposte dai referenti. • Garantiscono che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali. • Assicurano la riservatezza dei dati personali e sensibili trattati ai sensi della normativa vigente anche nelle comunicazioni digitali.
Il personale scolastico	• Comprende e contribuisce a promuovere politiche di sicurezza digitale. • È consapevole dei problemi di sicurezza online e usa comportamenti sicuri, responsabili e professionali nell'uso della tecnologia. • È tenuto a conoscere e mettere in pratica i regolamenti redatti dall'Istituto. • Segnala qualsiasi abuso sospetto o problema ai responsabili della sicurezza online.

Gli alunni	• Leggono, comprendono ed accettano la E-Safety Policy, compreso il regolamento all'uso dell'account Google Workspace for Education e il Patto di corresponsabilità. • Capiscono l'importanza di segnalare abusi, o l'uso improprio o l'accesso a materiali inappropriati. • Conoscono quali azioni intraprendere se loro o un compagno si sente preoccupato o vulnerabile quando si utilizza la tecnologia online; • Capiscono l'importanza di adottare buone pratiche di sicurezza online anche quando si usano le tecnologie digitali fuori dalla scuola.
I genitori	• Sostengono la scuola nel promuovere la sicurezza online e approvano l'accordo di E-Safety Policy con la scuola; • Si assicurano di aver preso tutte le precauzioni necessarie circa un uso corretto della tecnologia da parte degli alunni.

3. RILEVAZIONE DELLE INFRAZIONI

a. Che cosa segnalare

Le tipologie di comportamenti online da segnalare sono:

- offese e insulti tramite messaggi di testo, e-mail, pubblicati su social network o tramite telefono;
- diffusione di foto o video che ritraggono situazioni intime, violente o spiacevoli tramite il cellulare, siti web o social network;
- esclusione dalla comunicazione online, dai gruppi;
- furto, appropriazione, uso e rivelazione ad altri di informazioni personali come le credenziali d'accesso all'account e-mail, social network, ecc.

Per "*cyberbullismo*" si intende 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 (legge n.71/2017 - art 1 comma 2).

Per "*bullismo*" si intendono l'aggressione o la molestia reiterate, da parte di una singola persona o di un gruppo di persone, in danno di un minore o di un gruppo di minori, idonee a provocare sentimenti di ansia, di timore, di isolamento o di emarginazione, attraverso atti o comportamenti vessatori, pressioni o violenze fisiche o psicologiche, istigazione al suicidio o all'autolesionismo, minacce o ricatti, furti o danneggiamenti, offese o derisioni (Legge 70/2024 - art. 1 comma 1 lettera a) numero 2).

Rientrano tra le condotte di Cyberbullismo:

- **FLAMING**: Litigi nei forum di discussione, con l'uso di un linguaggio violento e volgare;
- **HARASSMENT**: molestie attuate attraverso l'invio ripetuto di messaggi offensivi;
- **CYBERSTALKING**: invio ripetuto di messaggi che includono esplicite minacce fisiche;
- **DENIGRAZIONE**: sparlare di qualcuno per danneggiare gratuitamente e con cattiveria la sua reputazione;
- **OUTING ESTORTO**: registrazione di confidenze per poi inserirle integralmente in un blog pubblico;
- **TRICKERY**: spinta, attraverso l'inganno, a rivelare informazioni imbarazzanti e riservate per renderle poi pubbliche in rete;
- **IMPERSONATION**: insinuazione all'interno dell'account di un'altra persona;
- **ESCLUSIONE**: estromissione intenzionale di una persona da un gruppo online
- **HAPPY SLAPPING**: ripresa, con il videotelefono, macchina fotografica o videocamera, di scene violente al fine di mostrarle ad amici o di diffonderle sulla rete;
- **EXPOSURE**: pubblicare informazioni private e/o imbarazzanti su un'altra persona;
- **SEXTING**: invio di messaggi via smartphone ed Internet, corredati da immagini a sfondo sessuale.

b. **Come accorgersi se un alunno/un'alunna è coinvolto/a in casi di (cyber)bullismo**

Accorgersi di episodi di (cyber)bullismo non è sempre facile perché le prevaricazioni talvolta avvengono in luoghi virtuali in cui gli adolescenti si ritrovano. Per cui è necessario cogliere i segnali che i ragazzi ci lanciano quando si trovano in una situazione di disagio o di difficoltà, eventualmente avvalendosi dello sportello psicologico presente in ogni plesso.

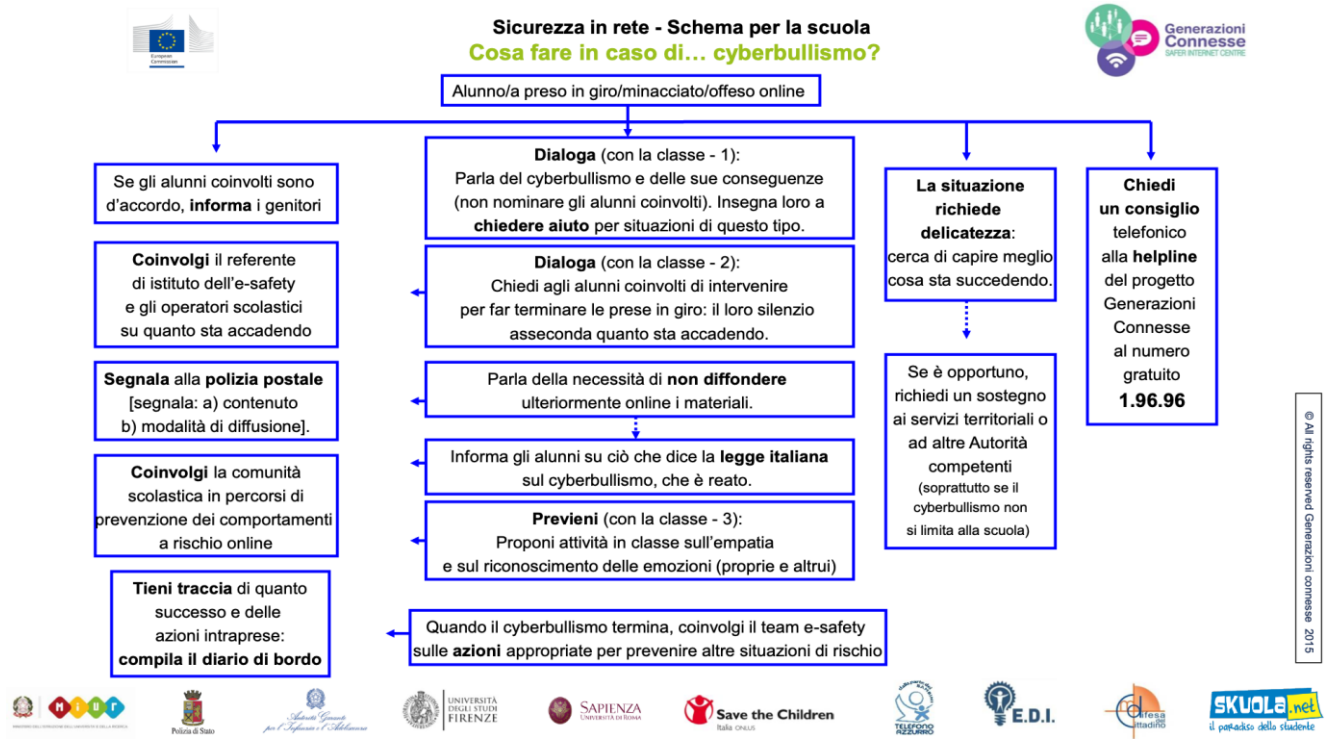
c. **Come gestire le segnalazioni**

Il docente informato del caso di bullismo o cyberbullismo, dopo aver ricostruito fatti e responsabilità informa il coordinatore di classe che a sua volta informerà il Dirigente scolastico ed eventualmente il Referente del cyberbullismo. Viene proposta e condivisa la procedura descritta nel seguente schema:

4. **Procedure operative per la gestione delle infrazioni alla E-Safety Policy.**

Per le violazioni della E-Safety Policy si rinvia al Piano per la didattica digitale d'istituto, al Regolamento d'Istituto e al Patto di Corresponsabilità. Qualora tali infrazioni dovessero configurarsi come reato, il Dirigente Scolastico ne darà segnalazione all'autorità competente fatto obbligo di denuncia (ex art. 331 del Codice di Procedura Penale).

Devono essere denunciati alle autorità competenti (carabinieri, polizia, polizia postale) i seguenti reati perseguibili d'ufficio: rapina ed estorsione (art 628 c.p. e art 629 c.p.) riferibili a episodi di minacce e violenze per ottenere (o sottrarre) oggetti o somme di denaro; lesioni gravissime (art 582 c.p. e art. 585 c.p.) e lesioni guaribili in più di 40 giorni o che comportano una diminuzione permanente della funzionalità di un organo; violenza sessuale (art 609 c.p.) commessa singolarmente o in gruppo – in questo caso viene considerata più grave e punita più severamente (per chiarire cosa si intende per violenza sessuale, bisogna considerare che



ogni atto sessuale rientra in questa definizione, ad esempio: se un gruppo di minori blocca fisicamente una compagna palpeggiandola, rispondono tutti penalmente e non solo la persona che materialmente esegue l'atto); violenza o minaccia a pubblico ufficiale per alunni che hanno compiuto il quattordicesimo anno di età (art. 336 c.p. e art. 337 c. p.). Devono altresì essere segnalati in caso di querela episodi relativi a: lesioni, percosse, minacce, ingiurie, diffamazione, molestia, atti persecutori/Stalking (art. 582, 581, 612, 591, 595, 660, 612 del codice penale): in questi casi è necessario informare la famiglia (e/o i Servizi Sociali).

A CHI RIVOLGERSI:

- Numero verde Ministero dell'Istruzione 800669696
- Numero unico Telefono Azzurro: 19696
- Polizia Postale Lombardia Compartimento Milano Via Moisè Loria, 74 – tel. 02/43333011
- CORECOM Lombardia SPORTELLO HELP WEB-REPUTATION GIOVANI
  https://www.corecomlombardia.it/wps/portal/site/comitato-regionale-comunicazioni/servizi/infopoint-web-reputation
- Garante per l'Infanzia e l'Adolescenza di Regione Lombardia:
  garanteinfanziaeadolescenza@pec.consiglio.regione.lombardia.it
- Referenti del Bullismo/Cyberbullismo degli Uffici Scolastici Territoriali
  - USR per la Lombardia Simona Chinelli - drlo.urp@istruzione.it
  - AT MILANO Vincenzo Capaldo - Laura Stampini - usp.mi@istruzione.it
- Polizia di stato www.commissariatodips.it
- Stazione dei Carabinieri di Pieve Emanuele (competente per il nostro territorio)
- Stop-it di Save the Children www.stop-it.it

Il presente documento (revisione di quello approvato il 2 novembre 2023) è stato approvato dal collegio docenti il 7 novembre 2024 e si intende valido fino ad eventuale successiva modifica.