MINISTERO DELL'ISTRUZIONE DELL'UNIVERSITÀ E DELLA
RICERCA UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
ISTITUTO COMPRENSIVO STATALE "POGGIALI-SPIZZICHINO"
00147 Roma - via A. Leonori 74 - Tel. 06.95955222 - Fax 06.5404346 - C.F. 97712300587 -
Cod. Mecc. RMIC8FF00E - e-mail: rmic8ff00e@istruzione.it - PEC: rmic8ff00e@pec.istruzione.it

E-Safety Policy

LA POLICY CYBERBULLISMO

Lo sviluppo e l'integrazione dell'uso delle TIC nella didattica, nonché la presenza sempre più diffusa delle tecnologie digitali nella vita di tutti i giorni pone nuove attenzioni dal punto di vista del loro uso sicuro e consapevole. Vi sono numerose evidenze scientifiche sui benefici che l'uso delle tecnologie digitali possono apportare nel processo di insegnamento/apprendimento. È compito dell'intera comunità scolastica, genitori inclusi, garantire che gli studenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato. È in questo quadro che si inserisce la necessità di dotare la scuola di una propria Policy di E-safety, nell'ottica della gestione delle infrazioni attraverso il monitoraggio continuo della Policy e dell'integrazione con il Regolamento d'istituto.

RIFERIMENTI LEGISLATIVI E RESPONSABILITA' GIURIDICA

La nuova legge

Il Parlamento ha dato il via libera alle nuove disposizioni contro il fenomeno del cyberbullismo. Nella Gazzetta del 3 giugno 2017 è stata pubblicata la Legge 29 maggio 2017 n. 71 recante "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo".

Le principali novità introdotte dal provvedimento sono le seguenti:

- **Definizione di «cyberbullismo»**: con questa espressione 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".

- **Obiettivo della legge**: il provvedimento intende contrastare il fenomeno del cyberbullismo in tutte
le sue manifestazioni, con azioni a carattere preventivo e con una strategia di attenzione, tutela ed educazione nei confronti dei minori coinvolti, sia nella posizione di vittime sia in quella di responsabili di illeciti, assicurando l'attuazione degli interventi senza distinzione di età nell'ambito delle istituzioni scolastiche.

- **Oscuramento del web**: la vittima di cyberbullismo, che abbia compiuto almeno 14 anni, e i genitori o esercenti la responsabilità sul minore, può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore, diffuso nella rete internet. Se non si provvede entro 48 ore, l'interessato può rivolgersi al Garante della Privacy che interviene direttamente entro le successive 48 ore.

- **Ruolo della scuola nel contrasto al cyberbullismo**: in ogni istituto tra i professori viene individuato un referente per le iniziative contro il bullismo e il cyberbullismo. Al dirigente spetterà informare subito le famiglie dei minori coinvolti in atti di bullismo e, se necessario, convocare tutti gli interessati per adottare misure di assistenza alla vittima e sanzioni e percorsi rieducativi per l'autore. Più in generale, il Miur ha il compito di predisporre linee di orientamento di prevenzione e contrasto puntando, tra l'altro, sulla formazione del personale scolastico e la promozione di un ruolo attivo degli studenti, mentre ai singoli istituti è demandata l'educazione alla legalità e all'uso consapevole di internet. Alle iniziative in ambito scolastico collaboreranno anche polizia postale e associazioni del territorio. Il dirigente scolastico che venga a conoscenza di atti di cyberbullismo (salvo che il fatto costituisca reato) deve informare tempestivamente i soggetti che esercitano la responsabilità genitoriale o i tutori dei minori coinvolti e attivare adeguate azioni di carattere educativo.

- **Ammonimento da parte del questore:** è stata estesa al cyberbullismo la procedura di ammonimento prevista in materia di stalking (art. 612-bis c.p.). In caso di condotte di ingiuria (art.
  594 c.p.), diffamazione (art. 595 c.p.), minaccia (art. 612 c.p.) e trattamento illecito di dati personali (art. 167 del codice della privacy) commessi mediante internet da minori ultraquattordicenni nei confronti di altro minorenne, fino a quando non è proposta querela o non è presentata denuncia è applicabile la procedura di ammonimento da parte del questore. A tal fine il questore convoca il minore, insieme ad almeno un genitore o ad altra persona esercente la responsabilità genitoriale; gli effetti dell'ammonimento cessano al compimento della maggiore età.

- **Piano d'azione e monitoraggio**: presso la Presidenza del Consiglio è istituito un tavolo tecnico con il compito di redigere un piano di azione integrato per contrastare e prevenire il bullismo e realizzare una banca dati per il monitoraggio del fenomeno.

SCOPO DELLA POLICY

La scuola si è impegnata alla realizzazione e redazione di un documento di Policy e-safety, per descrivere il fenomeno del cyber-bullismo, favorire lo sviluppo di una cittadinanza attiva e responsabile, le norme comportamentali e le procedure per l'utilizzo delle TIC in ambiente scolastico, le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali, per favorire lo sviluppo di una cittadinanza attiva e responsabile. In questo contesto, gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole della rete, anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose. Chi vive all'interno della comunità scolastica, con particolare attenzione per gli studenti minorenni, potrà fare riferimento alla Policy, sentirsi

supportato e guidato rispetto all'eventuale protocollo da seguire qualora si ritrovasse coinvolto da vittima e/o da spettatore in manifestazioni di bullismo e cyberbullismo. Gli alunni, infatti, potranno

essere coinvolti non solo in quanto destinatari, ma anche come interlocutori attivi di azioni ed interventi finalizzati alla piena attuazione della Policy.
Il documento potrà essere revisionato annualmente.

RUOLI E RESPONSABILITÀ'

IL DIRIGENTE SCOLASTICO DEVE

- essere adeguatamente formato ed informato sulle " Linee guida di orientamento per azione di prevenzione e di contrasto di bullismo e cyberbullismo" (MIUR, maggio 2015);
- presentare questo documento all'attenzione del Consiglio di Istituto e al Collegio dei Docenti;
- essere promotore di un'azione di tutela della sicurezza online per tutti i componenti della comunità scolastica e garantire la sicurezza nella gestione dell'infrastruttura e della strumentazione TIC a scuola;
- essere promotore della formazione e dell'informazione di tutti i componenti della comunità scolastica sulle tematiche della sicurezza informatica;
- assicurare un'adeguata diffusione della Policy di E-Safety e programmare un regolare monitoraggio;
- garantire la presenza di un gruppo di lavoro con il compito di controllare le procedure interne per la sicurezza informatica e di mettere in atto adeguate procedure in caso di gravi incidenti connessi all'utilizzo del web;
- fungere da intermediario tra l'istituzione scolastica e gli enti esterni del territorio preposti per il contrasto del fenomeno.

IL REFERENTE DI ISTITUTO DEVE

- essere adeguatamente formato ed informato sulle "Linee guida di orientamento per azione di prevenzione e di contrasto di bullismo e cyberbullismo" (MIUR, maggio 2015);
- partecipare alla stesura annuale della Policy di E-Safety e curare la sua massima diffusione all'interno di tutta la comunità scolastica;
- prendere atto dei risultati dei monitoraggi in itinere e finali per il controllo delle procedure interne per la sicurezza informatica;
- verificare ed implementare, alla fine dell'anno scolastico, la validità della Policy di ESafety;
- garantire una formazione sulla sicurezza informatica a tutti i componenti della comunità scolastica (personale scolastico, alunni e famiglie);
- raccogliere tutte le segnalazioni effettuate dai docenti, offrire consulenza e coordinarli relativamente alle procedure da seguire per una corretta gestione dei casi;
- informare e collaborare costantemente con il D.S. per il monitoraggio e l'implementazione della Policy di E-Safety;
- mantenere i contatti con le autorità locali e con le agenzie presenti sul territorio.

I DOCENTI DEVONO

- essere adeguatamente formati ed informati sulle " Linee guida di orientamento per azione di prevenzione e di contrasto di bullismo e cyberbullismo" (MIUR, maggio 2015);
- conoscere la Policy di E-Safety di Istituto, ossia le procedure da seguire in caso di gravi incidenti sulla sicurezza informatica;

- guidare gli alunni nelle attività di apprendimento che coinvolgono la tecnologia online, dando indicazioni chiare e precise per un uso consapevole;
- cercare di contrastare l'illecita diffusione dei dati personali e vigilare sull'uso delle tecnologie digitali, dispositivi mobili, tablet, macchine fotografiche, ecc, durante le lezioni e in tutte quelle attività scolastiche che ne prevedono la necessità a scopi didattici;
- favorire l'insorgere e il perfezionarsi delle competenze digitali degli alunni, descrivendo i vari rischi connessi all'utilizzo del web;
- illustrare ai propri alunni le regole di utilizzo contenute nel presente documento e segnalare eventuali malfunzionamenti o danneggiamenti delle apparecchiature;
- informare gli alunni affinché siano pienamente consapevoli dei risvolti legali relativi ad eventuali comportamenti pericolosi;
- adottare un comportamento responsabile e corretto nell'uso delle tecnologie informatiche e segnalare qualsiasi abuso, anche sospetti o casi di un uso improprio e/o rischioso delle stesse al Referente di Istituto;
- garantire la riservatezza dei dati personali trattati e quella delle password wifi e delle credenziali di accesso al registro elettronico e ad account personali;

IL PERSONALE ATA DEVE

- conoscere la presente Policy;
- segnalare eventuali abusi, anche sospetti, al gruppo di progetto per le necessarie azioni/sanzioni e a mantenere tutte le comunicazioni a livello riservato e personale.

GLI ALUNNI DEVONO

- essere responsabili ed utilizzare correttamente i sistemi informatici della tecnologia digitale, in attinenza ai termini previsti da questa policy che devono conoscere e comprendere; non possono utilizzare dispositivi personali durante le attività didattiche, salvo diversa indicazione;
- essere formati sui pericoli della rete, al fine di evitare rischi legati alla diffusione dei propri dati personali;
- cogliere l'importanza della segnalazione di ogni abuso, uso improprio o accesso a materiali inappropriati, comunicando immediatamente con gli insegnanti e capire l'importanza di adottare buone pratiche di sicurezza informatica in tutti i momenti della vita. Inoltre, in caso di malfunzionamento della strumentazione scolastica a disposizione, non dovranno eseguire tentativi di modifica della configurazione di sistema delle macchine, ma comunicarlo a un docente;
- capire l'importanza di adottare buone pratiche di sicurezza informatica in tutti i momenti della vita, per poter tutelare l'incolumità propria e altrui e per evitare di commettere reati punibili sia a livello scolastico sia a da parte della magistratura.

LE FAMIGLIE DEVONO

- conoscere la Policy E-Safety di istituto;
- conoscere e rispettare le norme di regolamento d'istituto relative alla sicurezza informatica;
- condividere con la scuola strategie per l'uso consapevole delle tecnologie informatiche dentro e fuori la scuola.

Rilevazione casi di cyberbullismo

Si configurano come atti di bullismo/cyberbullismo, caratterizzati da ripetute e volontarie aggressioni mirate a insultare, diffamare, minacciare e/o ferire una persona fisicamente. Costituisce aggravante da configurarsi come forma di vero e proprio cyberbullismo 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 del 29/05/2017 -Art 1 comma 2).

Casi che rientrano nel 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.

L'intervento in casi di cyberbullismo: misure correttive e sanzioni.

Le segnalazioni di episodi di bullismo e cyberbullismo da parte di genitori ed alunni, dovranno essere presentate presso la segreteria dell'Istituto e saranno raccolte dal docente referente, che segnalerà il caso al Dirigente Scolastico. Nell'analisi e nella ricerca delle possibili soluzioni il Dirigente ed il docente referente potranno avvalersi dell'intervento delle Forze dell'Ordine, a seconda della gravità del caso.
L'Istituto Comprensivo Poggiali Spizzichino considera come infrazione grave i comportamenti accertati che si configurano come forme di bullismo e cyberbullismo e li sanziona sulla base di quanto previsto nel Regolamento di Istituto.

Referente Cyberbullismo IC Poggiali Spizzichino :
Numeri utili di riferimento:

HELPLINE: −tel. 1.96.96, operativa 24 ore su 24

POLIZIA POSTALE: − tel. 06588831. Email: compartimento.polposta.rm@pecps.poliziadistato.it.
STAZIONE CARABINIERI COMPETENTE PER L'ISTITUTO COMPRENSIVO POGGIALI SPIZZICHINO: Carabinieri Comando Compagnia Roma EUR, Viale Asia 48 – tel 06 5427 4800