ISTITUTO COMPRENSIVO STATALE COMO ALBATE

e-mail: coic81200t@istruzione.it || pec: coic81200t@pec.istruzione.it
codice amministrazione: UFW1C2
Piazza IV Novembre, 1 - 22100 Como • tel. 031 524656 - fax 031 505110

DOCUMENTO DI E-POLICY

1. INTRODUZIONE E PROCESSO DI REVISIONE

L'Istituto Comprensivo Statale Como Albate ha ritenuto opportuno dotarsi di una policy di e-safety per essere pronto a cogliere i cambiamenti in atto nell'attuale società della conoscenza in cui opera, in particolare per quanto riguarda la formazione dei cittadini del futuro, destinatati a vivere in un ambiente in cui tutto viene gestito attraverso l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC).

Tali tecnologie diventano abilitanti, quotidiane, ordinarie, al servizio dell'attività scolastica e di tutti i suoi ambienti, coinvolgendo sia le attività orientate alla formazione e all'apprendimento sia l'amministrazione, con ricadute estese al territorio. Con questo documento si vuole regolamentare l'uso di Internet per rendere responsabili tutti gli utenti dell'Istituto in modo tale da garantire la privacy all'interno dei plessi e degli uffici di segreteria. Le indicazioni nazionali pongono l'accento sulle competenze digitali degli studenti, ai quali è richiesto di sapersi orientare nelle molteplici possibilità offerte dal Web, analizzando criticamente i materiali disponibili, scambiando informazioni ed esperienze in modo consapevole e responsabile.

Occorre in tal senso informare e formare le componenti scolastiche, in particolare gli alunni, in merito a eventuali rischi e fornire misure atte a prevenirli, permettendo di beneficiare in sicurezza delle opportunità offerte da Internet e dalle TIC. La policy di e-safety verrà revisionata e aggiornata periodicamente in base a eventuali variazioni delle norme, delle dotazioni tecnologiche e dei protocolli dell'Istituto.

2. SCOPO DELLA POLICY DI E-SAFETY

Scopo del presente documento è quello di informare l'utenza al fine di garantire un uso corretto e responsabile delle apparecchiature informatiche in dotazione alla scuola, nel rispetto della normativa vigente. È pertanto fondamentale conoscere 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 la gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali.

Tutti gli utenti devono conoscere i rischi cui sono esposti ogni volta che navigano in Internet: esiste, infatti, la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale. L'Istituto, pertanto, promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti. 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 di Internet anche a casa, al fine di prevenire il verificarsi di situazioni potenzialmente pericolose.

I docenti, consapevoli che è impossibile garantire una navigazione totalmente priva di rischi negli ambienti scolastici, non possono assumersi responsabilità derivanti da accessi accidentali e/o impropri a siti illeciti o dal reperimento e uso di materiali inappropriati.

3. VALUTAZIONE DEI RISCHI

L'uso di internet e delle nuove tecnologie è diventato sempre più precoce, frequente ed intenso per le nuove generazioni, che si ritrovano quindi ad affrontare dinamiche specifiche dei nuovi ambienti in rete, legate all'identità, alle relazioni, alla privacy, alla reputazione, alla produzione, distribuzione e fruizione di contenuti. Peraltro, recenti ricerche (EU kids online) hanno mostrato che all'aumentare delle opportunità aumentano anche i rischi, suggerendo quindi di lavorare a strategie di mediazione e prevenzione per un uso consapevole, corretto e creativo.

Nella valutazione dei possibili rischi, oltre a considerare le minacce provenienti dall'esterno rispetto al contesto scolastico, si ritiene opportuno non sottovalutare la possibilità che ad agire in modo illecito, provocando i danni più seri, siano spesso proprio quei soggetti che operano dall'interno e che, pertanto, conoscono la struttura della rete in qualità di fruitori dei servizi. Ciò posto, i principali rischi connessi all'uso delle tecnologie digitali risultano essere:

- ✓ la possibile dipendenza (patologica) dalla rete (social network, gambling, vamping, ecc.);
- ✓ l'uso improprio e scorretto dei dati personali (furto di identità – frode con carte di credito);
- ✓ episodi di cyberbullismo;
- ✓ esposizione a filmati violenti o a contenuto pedopornografico;
- ✓ relazioni pericolose/adescamento in rete;
- ✓ incitazione all'odio;
- ✓ persuasori con finalità commerciali;
- ✓ divulgazione di notizie false;
- ✓ uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare.

4. STATO DI FATTO: SPAZI FISICI E VIRTUALI DISPONIBILI NELLA SCUOLA

Nell'Istituto la qualità e la quantità degli strumenti è in continua implementazione:

- ✓ la dotazione di nuovi strumenti informatici è un obiettivo prioritario, a partire dalla presenza della LIM in tutte le classi della scuola primaria e della scuola secondaria;
- ✓ il registro elettronico è in uso sia alla scuola primaria sia alla scuola secondaria;
- ✓ i laboratori di informatica, presenti nei vari plessi, sono dotati di connessione Internet attraverso rete WIFI e cavo, postazioni PC per alunni;
- ✓ la segreteria, seguendo la normativa vigente, sta progressivamente raggiungendo l'obiettivo della completa dematerializzazione; si presta particolare attenzione al potenziamento delle attrezzature informatiche, al mantenimento e al costante aggiornamento della rete informatica, al potenziamento dei servizi digitali scuola-famiglia-studente.

I referenti dei diversi laboratori hanno il compito di verificarne il funzionamento e il rispetto del regolamento. Gli insegnanti e il personale ATA sono tenuti a utilizzare con il massimo rispetto gli strumenti presenti nella scuola, seguendo i regolamenti vigenti e minimizzando gli sprechi delle risorse a disposizione. I docenti devono servirsi con criterio delle TIC nelle attività didattiche e hanno il fondamentale compito di responsabilizzare gli studenti, per renderli consapevoli dell'importanza della salvaguardia di un bene comune, mediante corrette norme di utilizzo.

5. RUOLI E RESPONSABILITÀ

La pervasività delle nuove tecnologie nella vita personale, i rischi ad esse connesse, le sue potenzialità e l'esponenziale crescita dei contatti e delle relazioni, pone spesso il singolo di fronte ad una duplice situazione da vivere: la realtà "concreta" e quella virtuale, tra loro oramai fortemente connesse, influenzate e spesso determinate. La nascita poi di gruppi in rete richiedono capacità comunicative e socio-relazionali adeguate. È fondamentale quindi conoscere come comportarsi in questi gruppi, quali regole vanno rispettate e quali ruoli e responsabilità hanno i soggetti che vi partecipano. È opportuno quindi che anche nell'ambito scolastico ci sia chiarezza sui ruoli e sulle responsabilità di ciascun attore del percorso formativo.

- ➢ Il **Dirigente scolastico** è il soggetto su cui incombe la responsabilità di garantire la sicurezza dei membri della comunità scolastica e, conseguentemente, anche della sicurezza in rete. In quest'ottica egli si preoccupa di:
  - ✓ promuovere per tutti i docenti ed alunni la formazione per l'uso responsabile e corretto delle Tecnologie dell'Informazione e della comunicazione (alcune ore di lezione

all'anno sulla websecurity nelle TIC), oltre che nell'uso personale, anche nella didattica;

- ✓ dotare la scuola di un sistema in grado di consentire il controllo della sicurezza in rete;
- ✓ seguire le procedure relative agli eventi dannosi eventualmente occorsi agli alunni nell'utilizzo delle TIC a scuola.

- Il **Direttore dei Servizi Generali e Amministrativi** deve:
  - ✓ assicurare, nei limiti delle risorse finanziarie, la manutenzione delle strutture informatiche ai fini del suo funzionamento, della sua sicurezza e tutela da un uso improprio, e da attacchi esterni;
  - ✓ garantire la comunicazione all'interno dell'istituto, tra la rete di scuole (sportello, circolari, sito web, ecc.), e fra la scuola e le famiglie degli alunni per la diffusione di informazioni nell'ambito dell'utilizzo delle tecnologie digitali e della rete.

- I **docenti** si impegnano a:
  - ✓ informarsi e ad aggiornarsi su tema della sicurezza in rete uniformandosi alle politiche di sicurezza adottate dalla scuola di cui rispettano il regolamento;
  - ✓ supportare gli alunni nel corretto utilizzo delle tecnologie digitali per finalità didattico-educative (controllo nel rispetto delle leggi, del regolamento interno, del plagio, del diritto d'autore, ecc.);
  - ✓ guidare gli studenti nella scelta della fonte di informazioni;
  - ✓ garantire che le comunicazioni con i mezzi informatici avvengano nel rispetto dei ruoli e dei rispettivi codici comportamentali, mediante canali ufficiali e verificabili (posta elettronica col dominio istituzionale "istruzione.it", ecc.);
  - ✓ rispettare l'obbligo di riservatezza dei dati personali trattati e non, in conformità alla normativa vigente;
  - ✓ interagire con i genitori, coordinando con gli stessi l'intervento educativo, nei casi di disagio, manifestato dall'alunno, collegato all'utilizzo delle tecnologie digitali;
  - ✓ segnalare eventuali criticità nei sistemi informativi soprattutto in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
  - ✓ seguire le procedure interne di segnalazione di eventuali abusi subiti dagli alunni e connessi all'uso delle tecnologie digitali;

- ✓ aver cura degli strumenti in dotazione, in particolare spegnendo correttamente tablet, PC, LIM e videoproiettori al termine del periodo di utilizzo collocandoli nel luogo predisposto;
- ✓ il docente dell'ultima ora di lezione è tenuto a verificare che tutti gli strumenti siano correttamente spenti e riposti;
- ✓ accedere personalmente al registro elettronico attraverso il tablet o dal pc in uso e provvedere a compilare quanto di competenza; il tablet o il pc devono essere custoditi, tenuti fuori dalla portata degli alunni; sarà cura del docente non lasciare incustoditi i dispositivi in uso negli spostamenti della classe in altri luoghi della scuola;
- ✓ custodire la segretezza delle credenziali d'accesso al registro elettronico e all'area riservata del sito della scuola;
- ✓ non divulgare agli alunni le credenziali di accesso alla rete WIFI riservata ai docenti;
- ✓ installare e utilizzare solo software autorizzati;
- ✓ lasciare invariate le impostazioni dei dispositivi della scuola;
- ✓ non salvare sui dispositivi utilizzati file contenenti dati personali e/o sensibili;
- ✓ non memorizzare credenziali, email, file personali sui dispositivi;
- ✓ assicurarsi di aver effettuato il logout da ogni servizio prima di lasciare la postazione;
- ✓ salvare file di lavoro in cartelle personali o di classe e non sul desktop; i file non salvati in tal modo saranno eliminati dal responsabile delle attrezzature;
- ✓ utilizzare il laboratorio attendendosi all'orario concordato a inizio anno, firmare il registro d'accesso compilando i campi richiesti, segnalare eventuali malfunzionamenti riscontrati prima, durante o alla conclusione dell'attività svolta;
- ✓ permettere l'accesso al laboratorio agli alunni solo se accompagnati da docenti;
- ✓ prima di lasciare il laboratorio, accertarsi che tutti i pc siano stati spenti nel modo corretto; se necessario, compilare il modulo per la segnalazione di problemi;
- ✓ premurarsi che l'accesso degli alunni alla Rete avvenga sempre sotto la propria supervisione, informarli sui rischi cui sono potenzialmente esposti e sul corretto uso della Rete (motori di ricerca, piattaforme online, classi virtuali);
- ✓ visionare preventivamente i siti da proporre, verificandone accuratamente la sicurezza e il rispetto dei diritti di proprietà intellettuale.

- ➢ Agli **alunni** è richiesto di:
  - ✓ utilizzare responsabilmente le tecnologie digitali uniformandosi alle indicazioni dei docenti nonché rispettando le norme codificate nei regolamenti di istituto;

- ✓ rispettare le buone pratiche di sicurezza in rete;
- ✓ saper distinguere, con l'aiuto dei docenti, le fonti di informazione attendibili in rete per utilizzarle in modo appropriato senza violazione dei diritti d'autore altrui;
- ✓ comunicare in rete in modo appropriato rispettando le posizioni altrui;
- ✓ segnalare ai genitori e/o ai docenti situazioni di difficoltà o di bisogno di aiuto nell'utilizzo delle tecnologie digitali;
- ✓ utilizzare la strumentazione della scuola solo per scopi didattici e non personali;
- ✓ lasciare immutata la configurazione di sistema dei dispositivi.

- Anche i **genitori** sono coinvolti a pieno titolo. Ad essi è richiesto di:
  - ✓ leggere, comprendere e promuovere la policy di e-safety con i loro figli;
  - ✓ controllare con regolarità il registro elettronico e il sito istituzionale dell'Istituto;
  - ✓ sostenere i docenti nell'azione educativa diretta al corretto utilizzo delle tecnologie digitali;
  - ✓ educare (vigilando sui propri figli) al corretto utilizzo delle tecnologie digitali in ambiente domestico fissando regole comportamentali e di utilizzo;
  - ✓ collaborare con i docenti nell'adozione di linee di intervento coerenti per contrastare l'uso non responsabile, scorretto o pericoloso delle tecnologie digitali.

6. DISPOSITIVI PERSONALI

- STUDENTI

Gli alunni possono portare il dispositivo (smartphone, tablet o computer) a scuola. Secondo con quanto indicato dalla Direttiva Ministeriale n. 30 del 15 marzo 2007, dall'accordo BYOD POLICY, e dal Garante sulla Privacy, gli studenti devono a tenere lo smartphone spento quando sono a scuola, indipendentemente dall'attività svolta (lezione, ricreazione, accesso ai servizi igienici, pause, ecc.). Se il docente lo ritiene opportuno, è consentito l'uso del dispositivo personale dello studente, incluso lo smartphone. Gli studenti a cui è stato consigliato dai docenti l'uso del computer o del tablet come strumenti compensativi, sono sempre autorizzati a portarli a scuola e ad utilizzarli secondo le indicazioni dell'insegnante. La custodia, la cura ed il corretto utilizzo dei dispositivi personali sono una responsabilità dello studente. Si recepisce in questo documento quanto previsto dalla Direttiva Ministeriale n. 30 del 15 marzo 2007: "le famiglie si assumono

l'impegno di rispondere direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone".

- DOCENTI

È consentito l'uso di smartphone e di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili. Per il restante orario di servizio è consentito l'uso del dispositivo (smartphone) solo per importanti comunicazioni personali urgenti.

- PERSONALE DELLA SCUOLA

Il personale scolastico è autorizzato ad usare il proprio dispositivo se non sta svolgendo un ruolo didattico, solo se l'utilizzo non intralci il normale svolgimento delle attività scolastiche, né distragga dal corretto svolgimento delle proprie mansioni.

7. COMUNICAZIONE SCUOLA-FAMIGLIA

L'Istituto si impegna a promuovere una comunicazione chiara ed esplicita con il personale, le famiglie e il territorio, in particolare attraverso:

- ✓ il sito istituzionale, costantemente aggiornato, che fornisce un'informazione puntuale e trasparente sulla documentazione e le attività relative alla scuola;
- ✓ il registro elettronico, costantemente aggiornato dai docenti, sul quale le famiglie possono controllare assenze, voti e annotazioni (compiti assegnati, avvisi, note…). Nella scuola primaria non è possibile la consultazione delle valutazioni;
- ✓ la posta elettronica istituzionale ("istruzione.it"), canale preferenziale per la trasmissione di informazioni e comunicazioni tra gli utenti.

L'Istituto fornisce un supporto alle famiglie per le iscrizioni online ai diversi ordini di scuola mediante postazioni informatiche dedicate e personale applicato di segreteria.

8. GARANZIA E TUTELA DELLA PRIVACY

L'Istituto opera a ogni livello rispettando tutte le normative vigenti in merito alla tutela della privacy, come indicato sul sito istituzionale. La compilazione della liberatoria riguardante il trattamento immagini e audiovisivi degli alunni è richiesta:

- ✓ a chi si iscrive per la prima volta nell'Istituto oppure nel passaggio all'ordine successivo attraverso la compilazione del modulo di iscrizione;
- ✓ a ciascun alunno all'inizio di ogni anno scolastico attraverso l'apposita modulistica presente sul sito istituzionale.

Sono permesse a titolo gratuito le riprese video e fotografiche di visite o viaggi di istruzione, saggi e rappresentazioni scolastiche se destinate a un ambito familiare e non alla diffusione. Deve essere prestata grande attenzione all'eventuale pubblicazione delle medesime immagini in internet e, in particolare, sui social network per i quali è indispensabile il consenso informato delle persone presenti nel video e nelle immagini/fotografie, se minorenni, dei rispettivi genitori.

Per riprese video e fotografiche nell'ambito di progetti didattici specifici (eventualmente in collaborazione con esperti o enti esterni) richiedono una precisa autorizzazione. Tutti i moduli per autorizzare le riprese sono disponibili in segreteria.

9. PREVENZIONE, RILEVAZIONE E GESTIONE DI CASI DI BULLISMO E CYBERBULLISMO

L'Istituto si impegna a formare e aggiornare i docenti affinché siano capaci di riconoscere eventuali casi di bullismo/cyberbullismo, o situazioni a rischio e possano mettere in atto le procedure più indicate. Per i casi di bullismo o cyberbullismo, l'Istituto si prodiga nella tutela dei minori coinvolti, senza renderli in alcun modo identificabili.

Obiettivo principale di questo Regolamento è quello di orientare la nostra Scuola nell'individuazione e prevenzione dei comportamenti devianti quali bullismo e cyberbullismo.

- ➢ DEFINIZIONE DI BULLISMO: comportamento che mira deliberatamente a far del male o danneggiare; spesso è persistente, talvolta dura settimane, mesi e persino anni. Il bullismo, quindi, è l'abuso di potere sistematico e pianificato di uno, spesso sostenuto da gregari, su una vittima. Il bullismo presenta caratteristiche che lo distinguono da semplici giochi o ragazzate:

  - ✓ asimmetria di poteri;
  - ✓ intenzionalità e pianificazione;
  - ✓ sistematicità;
  - ✓ isolamento della vittima.

Le prepotenze messe in atto dal bullo possono essere:

- ✓ DIRETTE (molestie esplicite): spintoni, calci, schiaffi; danneggiamenti o furti di beni personali; offese, prese in giro, denigrazioni; minacce, estorsioni;
- ✓ INDIRETTE (molestie nascoste): diffusione di storie non vere a danni di un/una compagno/a; esclusione di un/una compagno/a da attività comuni.

- DEFINIZIONE DI CYBERBULLISMO: forma di bullismo online che colpisce soprattutto i giovanissimi, prevalentemente attraverso i social network; con questa espressione si intende quindi "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 29 maggio 2017 n.71).

  Il cyberbullismo è un fenomeno molto grave perché in pochissimo tempo le vittime possono vedere la propria reputazione danneggiata in una comunità molto ampia, anche perché i contenuti, una volta pubblicati, possono riapparire a più riprese in luoghi diversi.

  Nel Cyberbullismo distinguiamo:

  - ✓ FLAMING: litigi on line 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 di pettegolezzi e commenti crudeli, calunniosi e denigratori all'interno di comunità virtuali, quali newsgroup, blog, forum di discussione, messaggistica immediata, siti internet;
  - ✓ OUTING ESTORTO: registrazione delle confidenze - raccolte all'interno di un ambiente privato - creando un clima di fiducia e poi inserite integralmente in un blog;
  - ✓ 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 dall'attività on line. SEXTING: invio di messaggi via smartphone ed Internet, corredati da immagini a sfondo sessuale;
- ✓ SEXTORTION: pratica utilizzata dai cyber criminali per estorcere denaro, la vittima viene convinta a inviare foto e/o video osé e poi le si chiede un riscatto per non pubblicarle.

Tali comportamenti devono essere conosciuti e combattuti da tutti in tutte le forme, così come previsto:

- ✓ dagli artt. 3- 33- 34 della Costituzione Italiana;
- ✓ dalla Direttiva MIUR n.16 del 5 febbraio 2007 recante "Linee di indirizzo generali ed azioni a livello nazionale per la prevenzione e la lotta al bullismo";
- ✓ dalla direttiva MPI 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";
- ✓ dalla direttiva MPI 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";
- ✓ dalla direttiva MIUR n.1455/06 sulla partecipazione studentesca;
- ✓ dal D.P.R. 249/98 e 235/2007 recante "Statuto delle Studentesse e degli Studenti";
- ✓ dalle "Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo", MIUR aprile 2015;
- ✓ dalla legge 13 luglio 2015 n. 107, art.1, comma 7;
- ✓ dalla legge 29 maggio 2017 n. 71 recante "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo";
- ✓ dagli artt. 581-582-594-595-610-612-635 del Codice Penale;
- ✓ dagli artt. 2043-2047-2048 Codice Civile.

Si ricorda che l'art.2 della legge 29 maggio 2017 n.71 recita:

“Ciascun minore ultraquattordicenne, nonché ciascun genitore o soggetto esercente la responsabilità del minore che abbia subito taluno degli atti di cui all'articolo 1, comma 2, della presente legge, 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 […] Qualora, entro le ventiquattro ore successive al ricevimento dell'istanza di cui al comma 1, il soggetto responsabile non abbia comunicato di avere assunto l'incarico di provvedere all'oscuramento, alla rimozione o al blocco richiesto, ed entro quarantotto ore non vi abbia provveduto, o comunque nel caso in cui non sia possibile identificare il titolare del trattamento o il gestore del sito internet o del social media, l'interessato può rivolgere analoga richiesta, mediante segnalazione o reclamo, al Garante per la protezione dei dati personali, il quale, entro quarantotto ore dal ricevimento della richiesta, provvede […]”.

Sulla base delle più recenti disposizioni di legge è stato individuato nel nostro istituto un REFERENTE DEL “BULLISMO E CYBERBULLISMO” che:

- ✓ accoglie segnalazioni di disagio da parte di studenti, docenti e genitori;
- ✓ 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, anche con eventuale affiancamento di genitori e studenti;
- ✓ si rivolge anche a partner esterni alla scuola per realizzare progetti di prevenzione;
- ✓ cura rapporti di rete fra scuole per eventuali convegni/seminari/corsi.

Chiunque entri in possesso di dati certi ha la possibilità di denunciarli in forma tutelata. Nel momento in cui si è a conoscenza di situazioni di cyberbullismo

- ✓ il docente allerta immediatamente il referente al cyberbullismo che di conseguenza informa il dirigente scolastico;
- ✓ È necessario redigere il modulo di segnalazione presente alla fine di questo documento;
- ✓ il dirigente scolastico convoca, separatamente, le famiglie degli alunni coinvolti per informarle dell’accaduto e mette in atto le procedure previste dal Regolamento d’Istituto.

Si ricorda che, in caso di necessità ci si può rivolgere ai servizi di supporto appositamente attivi a livello nazionale. Per segnalare contenuti inopportuni visionati sui media si può far riferimento al sito del CoReCom all’indirizzo http://www.corecomlombardia.it/opencms/index.html. La Polizia

Postale e delle Comunicazioni https://www.commissariatodips.it/ è attualmente impegnata in attività a sostegno della navigazione protetta dei minori ed è competente a ricevere segnalazioni in merito a qualsiasi tipo di reato informatico.

10. OPERAZIONI RELATIVE AL MANCATO RISPETTO DELLA E-POLICY

Si riporta di seguito un elenco non esaustivo di possibili azioni:

- ✓ richiamo verbale;
- ✓ richiamo verbale con annotazione disciplinare sul registro e/o sul diario personale;
- ✓ prelievo del dispositivo, rimozione della SIM (restituita all'interessato), spegnimento e consegna all'ufficio alunni per il ritiro dello stesso da parte dei genitori;
- ✓ convocazione della famiglia e/o degli attori dell'episodio segnalato;
- ✓ raccolta del materiale informatico lesivo della dignità delle figure presenti nell'istituto;
- ✓ sanzione disciplinare grave;
- ✓ accesso alla commissione di garanzia;
- ✓ segnalazione alle forze dell'ordine.

Le figure interessate alla definizione dell'azione da intraprendere sono le seguenti, in ordine di gravità:

- ✓ personale scolastico/docente verso il coordinatore di classe (bassa entità);
- ✓ personale scolastico/docente verso consiglio di classe ed eventuale coinvolgimento della famiglia (media entità);
- ✓ personale scolastico/docente verso consiglio di classe, dirigente scolastico e coinvolgimento della famiglia (entità grave);
- ✓ personale scolastico/docente verso dirigente scolastico, coinvolgimento della famiglia ed agenti esterni quale le forze dell'ordine e/o la polizia postale (entità gravissima).

La Legge 71/2017, nell'articolo 2, cui si rimanda, indica tempi e modalità per richiedere la rimozione di contenuti ritenuti dannosi per i minori. La Legge 71/2017, agli articoli 5 e 7, cui si rimanda, riporta due sanzioni nei confronti dei trasgressori della legge stessa, minorenni e di età superiore ai quattordici anni (rispettivamente sanzioni disciplinari in ambito scolastico con percorsi di recupero, ammonimento con la famiglia presso il questore).

La Scuola potrà, altresì, segnalare episodi di cyberbullismo nonché la eventuale presenza di materiale pedopornografico in rete al servizio Helpline di Telefono Azzurro 1.96.96, alla Hotline "Stop-it" di Save the Children, all'indirizzo www.stop-it.it affinché trasmettano dette segnalazioni al

Centro Nazionale per il Contrasto alla Pedopornografia su Internet, istituito presso la Polizia Postale e delle Comunicazioni, per consentire le attività di investigazione necessarie.

Le azioni individuate hanno la finalità di sostenere le vittime, le famiglie e tutti coloro che sono stati spettatori attivi o passivi di quanto avvenuto, e di realizzare interventi educativi nei confronti di coloro che hanno messo in atto comportamenti lesivi del rispetto degli altri. In ogni caso, i docenti predisporranno specifiche rilevazioni ed azioni preventive sulla base dei protocolli suggeriti dalla piattaforma "Generazioni Connesse", e dei percorsi formativi anche in rete. A tal fine, sono stati predisposti dei moduli ad hoc reperibili sul loro sito, che costituiscono parte integrante del presente documento.

11. MODULO DI SEGNALAZIONE

Si riporta in allegato al documento, il modulo per la rilevazione di casi di cyberbullismo, conseguente alla Legge 71/17 da inviare tramite mail all'Autorità competente.

12. DIFFUSIONE DELLA POLICY DI E-SAFETY

La policy di e-safety e le regole in essa contenute sono approvate dal Collegio dei Docenti con delibera n. _____ in data _____ e dal Consiglio di Istituto con delibera n. _____ in data _____ sono pubblicate online sul sito istituzionale dell'Istituto. Il personale scolastico è tenuto alla lettura e sottoscrizione della policy di e-safety, nonché allo sviluppo delle linee guida e all'applicazione scrupolosa delle istruzioni sull'uso sicuro e responsabile della Rete. Gli studenti e i genitori sono tenuti a conoscere i contenuti del presente documento.

Il presente documento, approvato dal Consiglio di Istituto in data _____ con delibera n. _____ costituisce parte integrante del Regolamento di Istituto.