ISTITUTO COMPRENSIVO STATALE "DE ZERBI – MILONE"
Scuola dell'Infanzia, Primaria e Secondaria I Grado a indirizzo musicale
Piazza Martiri d'Ungheria, 89015 Palmi (RC) – Tel.: 0966/22604 – 22802
C.M. RCIC82100T – C.F. 91006790801
Email: rcic82100t@istruzione.it – PEC: rcic82100t@pec.istruzione.it
Sito web: www.icdezerbimilone.gov.it

"Allegato B.5" PTOF
E-SAFETY POLICY D'ISTITUTO

Anno Scolastico 2018-2019

1. Introduzione

Che cos'è una *E-safety Policy*?

Ogni impresa moderna è dotata di una *policy* aziendale, costituita da un insieme di norme adottate in modo unilaterale volte a disciplinare la condotta dei dipendenti in settori specifici e in particolar modo nell'uso dei personal computer e nella fruizione della rete messa loro a disposizione.

La scuola, in quanto impresa formativa, deve stabilire anch'essa, in modo condiviso, come ciascun membro della comunità scolastica debba approcciarsi alle TIC, stilando in modo autonomo e personalizzato alle proprie esigenze una *E-safety Policy*, ovverosia un documento che da un lato individui le procedure corrette di approccio alle tecnologie digitali, dall'altro specifichi le misure per prevenire e gestire le problematiche derivate da un uso non consapevole, e dunque non corretto, di esse.

Qual è lo scopo primario della *E-safety Policy*?

La *E-safety Policy* è finalizzata a veicolare codici di condotta verso internet che risultino adeguati a garantire sicurezza per l'intera comunità scolastica. Ciascun attore di essa deve approcciarsi alla rete in modo responsabile, sia quando lo fa per motivi didattici o amministrativi, sia quando lo scopo è personale o ricreativo, acquisendo consapevolezza delle aree di rischio nelle quali si può ricadere e delle conseguenze disciplinari, se non giudiziarie, di un comportamento pericoloso o illecito assunto nel web.

A chi è indirizzata la *E-safety Policy*?

La *E-safety Policy* non è indirizzata al solo corpo docente ma a tutto il personale scolastico, nonché agli alunni e ai genitori: la salvaguardia dell'utenza, infatti, è imprescindibile dall'assunzione di Responsabilità di tutti quanti operino, a vario titolo, nella scuola o usufruiscano dei suoi servizi.

LA DIRIGENTE SCOLASTICA

- E' la responsabile generale per i dati e la sicurezza dei dati
- E' garante dell'utilizzo di un Internet Service dotato di filtraggio in conformità alla legislazione vigente in materia
- Assicura la formazione dei docenti con ruoli relativi alla sicurezza on-line e agevola la formazione del personale scolastico sul tema
- Favorisce la formazione degli alunni e gli incontri informativi con i genitori
- Coordina con ruolo primario stesura e revisioni della Policy
- Elabora eventuali azioni strategiche in base ai dati emergenti dalle relazioni periodiche di monitoraggio redatte dal responsabile della sicurezza online e mette in atto le procedure stabilite in caso di infrazione della Policy

---

IL DSGA E IL DOCENTE RESPONSABILE DELLA SICUREZZA ONLINE

- Sono responsabili per le problematiche inerenti la sicurezza on line
- Promuovono, in tutti gli attori della comunità scolastica, l'impegno consapevole a contribuire alla sicurezza on line
- Facilitano i percorsi di formazione dei docenti e del personale scolastico sull'argomento e garantiscono la loro consulenza
- Collaborano alle azioni di informazione-formazione per alunni e genitori
- Assicurano che i docenti di ogni ordine di grado e di ogni disciplina a livello programmatico forniscano un contributo all'educazione alla sicurezza on line dei loro alunni
- Supervisori del registro degli incidenti on-line, garantiscono l'attivazione delle corrette procedure, da parte del personale, in caso di incidenti che minano la sicurezza on line
- Svolgono un'azione di controllo per la tutela di dati personali oggetto di pubblicazione e sull'accesso a contenuti inappropriati
- Si coordinano con il docente referente per l'Istituto per la prevenzione e il contrasto del bullismo e del cyberbullismo in un'azione congiunta di controllo di tutte le forme illegali di uso del web
- Curano i rapporti con le autorità competenti in materia

L'ANIMATORE DIGITALE E I DOCENTI DEL TEAM PER L'INNOVAZIONE DIGITALE	▪ Sono preposti alla stesura della *E-Safety Policy*, assicurandosi della sua pubblicazione nel PTOF in vigore e nel sito della scuola ▪ Hanno il compito di diffondere la conoscenza della Policy attraverso incontri con il personale della scuola, gli alunni e i genitori e mediante la predisposizione di materiale illustrativo
IL PERSONALE DOCENTE ED EDUCATIVO	▪ Considera parte integrante della programmazione disciplinare il tema della sicurezza on-line ▪ Si prende l'impegno di avvalersi di metodologie di apprendimento attraverso le TIC solo garantendo la loro guida e supervisione agli alunni coinvolti ▪ Considera un obiettivo primario sviluppare negli alunni la capacità di sottoporre a giudizio critico i contenuti online e la consapevolezza che il loro uso è regolamentato per legge ▪ Fanno un uso della tecnologia responsabile e professionale, promuovendo in prima persona la sicurezza on line
IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARE	▪ Collaborano con consapevolezza al mantenimento della sicurezza online, in particolar modo i collaboratori scolastici monitorando l'uso di dispositivi personali negli spazi esterni alle aule scolastiche ▪ Segnalano con tempestività utilizzi non idonei di cellulari dotati di fotocamere e videocamere ▪ Fanno un uso della tecnologia responsabile e professionale, promuovendo in prima persona la sicurezza on line
GLI STUDENTI	▪ Si impegnano a leggere la E-Safety Policy e, attraverso una consapevole comprensione dei principi che la ispirano, ne accettano le norme e le applicano ▪ Imparano a condurre ricerche sul web in modo critico e attingendo ai contenuti in modo legale ▪ Non accedono a siti inappropriati e non contribuiscono alla diffusione di materiale inappropriato, segnalando abusi al proposito ▪ Conoscono e si adeguano al codice comportamentale da adottare a scuola nell'approcciarsi alle TIC e nel far uso dei propri dispositivi personali ▪ Capiscono l'importanza della sicurezza in rete anche al di fuori dell'ambiente scolastico e si comportano per garantirla a sé e agli altri ▪ Non mettono a rischio il loro benessere psicofisico utilizzando la rete per un numero di ore elevato ▪ Sono consapevoli dei pericoli del web e in particolar modo del fenomeno del cyberbullismo

I GENITORI

- Controfirmano la E-Safety Policy, impegnandosi a contribuire alla promozione della sicurezza on line e garantendo la continuità di comportamenti corretti dei loro figli nelle ore extrascolastiche
- Vigilano sulle misure adottate dalla scuola circa l'uso corretto delle tecnologie e la prevenzione dei rischi

Come viene messa in atto la *E-safety Policy*?

La scuola si impegna a controllare con periodicità il sistema informatico, al fine di evidenziare eventuali alterazioni dei parametri di protezione. Si impegna inoltre a vigilare sulle azioni compiute attraverso la rete della scuola, in modo da far emergere illeciti quali navigazioni per interessi privati e personali o su siti inadeguati o senza il rispetto della normativa su diritto d'autore e copyright, avendo cura di archiviare i tracciati del traffico internet per successivi controlli.

Il Regolamento disciplinare d'Istituto indica in dettaglio le norme comportamentali in relazione all'uso delle tecnologie e all'accesso al web a cui devono attenersi gli alunni e le sanzioni disciplinari per le eventuali infrazioni.

Per quanto riguarda i comportamenti rientranti nella categoria del cyberbullismo, la scuola adotta le linee di orientamento contenute nell'art. 4 della legge n. 71 del 29/05/2017 «*Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo*».

L'accordo di utilizzo accettabile dell'E-Safety Policy da parte dei docenti avviene attraverso l'approvazione nel Collegio Docenti, da parte del personale scolastico attraverso un documento di accordo, da parte degli studenti e delle loro famiglie con un documento di accordo per gli alunni degli anni successivi.

Come viene revisionata la *E-safety Policy*?

La revisione della E-safety Policy ha cadenza annuale e spetta al docente responsabile della sicurezza on-line che coadiuverà un gruppo di lavoro costituito da: il team per l'innovazione digitale, i referenti di progetti di educazione all'uso consapevole della rete (ad esempio Generazioni Connesse), il referente per la prevenzione e il contrasto del bullismo e del cyberbullismo. Il tutto avverrà sotto la supervisione della Dirigente Scolastica in collaborazione con il DSGA.

Modifiche potranno avvenire anche in occasione di cambiamenti significativi per quanto riguarda le tecnologie in uso nella scuola, purché siano memorizzate in un documento di registrazione che tracci la storia della Policy dalla sua prima definizione in bozza alla versione più aggiornata in uso.

2. Il PNSD e l'educazione alla sicurezza on-line

L'attuazione del PNSD nel nostro Istituto, in piena coerenza con le indicazioni del D.M. 851 del 27/10/2015, ha molteplici fini che vanno a confluire nell'obiettivo principale di sviluppare e potenziare le competenze digitali degli alunni.

Le Indicazioni nazionali parlano chiaro circa la natura non esclusivamente tecnica di tali competenze, che, al contrario, includono la capacità di assumere un atteggiamento consapevole, critico e responsabile nell'uso delle tecnologie della comunicazione, sia al momento di ricercare informazioni sia nell'interagire con le altre persone.

La scuola deve offrire agli studenti un'*alfabetizzazione civica* che contribuisca al loro sviluppo come futuri *cittadini digitali*, rendendoli consapevoli delle specificità dell'informazione in rete nonché delle problematiche emergenti dalle dinamiche sociali online.

L'educazione 'con i media' implica, dunque, l'educazione 'ai media', che il corpo docenti deve assumere come impegno programmatico, indipendentemente dalla disciplina insegnata, potendo contare del supporto dell'Animatore digitale con il team per l'innovazione digitale. I tre punti da sviluppare sono qui di seguito riassunti in linee essenziali esplicitate nella loro integrità in documenti specifici da elaborare come allegati all'E-Safety Policy e nel Documento programmatico d' Istituto per la Prevenzione e il Contrasto del Bullismo e del Cyberbullismo:

- Conoscere la *Dichiarazione dei Diritti in internet* elaborata dalla Commissione per i diritti e i doveri in internet (Camera dei Deputati)
- Comprendendone il valore costitutivo di tale Dichiarazione in piena coerenza e ad integrazione della Dichiarazione universale dei diritti umani delle Nazioni Unite, della Carta dei diritti fondamentali dell'Unione Europea, delle Costituzioni nazionali e delle Dichiarazioni internazionali in materia

- Adottare strategie di valutazione e verifica delle informazioni
- Riconoscere acriticità delle fonti per pregiudizi di varia natura
- Essere consapevoli della passibilità di manipolazione del materiale fotografico, video e sonoro
- Imparare a rispettare diritti di autore e copyright
- Avere la consapevolezza dell'importanza di scaricare materiale in modo legale

- Riconoscere l'esistenza di un Netiquette e applicare le regole di tale 'galateo' dell'ambiente virtuale
- Stabilire i limiti e i pericoli delle amicizie virtuali
- Comprendere l'importanza della privacy, propria e altrui
- Partecipare con spirito critico alla vita sociale online, rifuggendo siti e persone che si contraddistinguono per hate-speech
- Essere coscienti dell'esistenza di vere e proprie patologie da iperconnessione (like addiction, challenge, nomofobia, vamping)
- Riconoscere i pericoli della rete (grooming, sexting)
- Conoscere la legge n. 71/29-05-2017 e le *Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo* in essa contenute, rifuggendo da atteggiamenti di bullismo on-line sia attivi sia passivi

3. Gestione dell'infrastruttura internet e degli spazi web dell'Istituto

Il nostro Istituto garantisce:

- la sicurezza della LAN (Local Area Network) attraverso un dominio su rete locale (segreteria) cui accedono i computer dell'amministrazione. Le postazioni sono protette con sistemi antivirus regolarmente aggiornati. Per il servizio di backup è consigliato fare copia dei propri dati su supporti personali (pen-drive, hard-disk esterni, …)
- l'utilizzo aggiornato di antivirus e filtraggio delle email per proteggere gli utenti da spam, phishing e virus
- la rete wireless (in alcuni plessi)

Il nostro istituto ha un proprio sito web : www.icdezerbimilone.gov.it. La gestione del sito è pienamente rispondente alle normative riguardanti i contenuti (accuratezza, appropriatezza, aggiornamento). La scuola detiene i diritti d'autore dei documenti pubblicati o per quei documenti per i quali è stato chiesto e ottenuto il permesso

dall'autore. Tutte le informazioni pubblicate tutelano la privacy degli studenti e del personale secondo la normativa vigente.

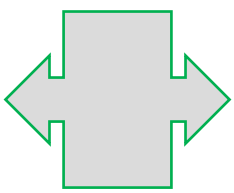
La comunicazione istituzionale sarà integrata da una pagina ufficiale su Facebook : https://www.facebook.com/icdezerbimilone, con lo scopo di connettere la scuola alla famiglie in modo più immediato e tempestivo, permettendo una condivisione veloce delle informazioni. L'utilizzo di tale pagina è in coerenza con funzioni e obiettivi della scuola così come esplicitati nel PTOF e nel rispetto della normativa vigente in materia di protezione dei dati.

La Dirigente Scolastica, attraverso i docenti responsabili della gestione della pagina, potrà avvalersene per comunicare le attività in programma e eventuali variazioni nella tempistica, come pure quanto rappresenti un imprevisto rispetto al regolare svolgimento della giornata scolastica, ferma restando la notifica attraverso avvisi e comunicazioni nel sito web.

La pagina Facebook si presta alla presentazione, attraverso immagini e video, delle attività didattiche laboratoriali, iniziative legate a specifiche tematiche, manifestazioni sportive, teatrali, musicali, uscite didattiche e viaggi di istruzione: la loro pubblicazione avverrà nel pieno rispetto della normativa che regola la pubblicazione di riproduzioni fotografiche e video di minori.

4. La strumentazione personale

Il Regolamento di istituto definisce le modalità di utilizzo degli strumenti personali (cellulari, tablet, portatili…) sia per i docenti sia per gli alunni. Il divieto di utilizzo durante l'attività didattica deve coesistere con l'attivazione di una politica attiva per il BYOD (Bring your own device): le potenzialità economiche della scuola non sono al momento adeguate ad assicurare una fornitura di strumentazione informatica nelle singole classi per ogni singolo studente e, dunque, è auspicabile la promozione a scopi didattici dell'uso di apparecchiature personali.

PROCEDURE DA ATTIVARE	**BYOD**	VANTAGGI OTTENUTI
Consentire l'uso della connessione internet		Risparmio economico
Richiedere consenso delle famiglie		Inclusione integrale nell'utilizzo dei media
Progettare un intervento mirato		Accelerazione dell'innovazione tecnologica a scuola

5. Le azioni di prevenzione

La prevenzione passa attraverso il rispetto dei seguenti principi generali:

- conoscere il regolamento dei servizi dei Social Network e delle applicazioni web, per essere consapevoli dei propri diritti e dei propri doveri, assumendo un atteggiamento critico anche attraverso un costante aggiornamento sulle problematiche inerenti l'utilizzo di questi canali
- gestire la propria identità digitale con cautela e stabilire in modo meditato come e con chi condividere dati personali
- trattare i dati altrui solo ed esclusivamente a seguito di un esplicito consenso
- stabilire se un contenuto costituisca un abuso e, se commesso involontariamente, contattare l'utente per ricondurlo a comportamenti leciti; se l'abuso è passibile di segnalazione perché volontario, segnalarlo secondo le modalità offerte da ciascun social network.

Internet favorisce la libertà di espressione, della quale gli alunni possono fare un uso scorretto, utilizzando il mondo virtuale come ambiente dove esplicare atteggiamenti di violenza e prevaricazione. Il fenomeno del cyberbullismo (ovverosia «qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito dei dati personali in danno di minorenni, nonché la diffusione di contenuti online 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») ha raggiunto dimensioni così allarmanti che una legge dello stato ha recentemente stabilito precise disposizioni a tutela dei minori per prevenirlo e contrastarlo (n. 71/29-05-2017).

Proprio in ottemperanza a tale disposizione legislativa, l'Istituto ha individuato un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo e si propone di potenziare la già avviata promozione dell'educazione all'uso consapevole della rete internet.

Per una politica efficacia di prevenzione occorre definire un Patto di corresponsabilità dove gli attori della comunità scolastica prendono precisi impegni, al pari di quanto fanno nei confronti dei diritti e dei doveri sottoscrivendo il Patto di corresponsabilità educativa (DPR 235/2007).

	si impegna a:
LA SCUOLA	◆ riconoscere il Dirigente Scolastico come titolare del trattamento di dati personali secondo la legge sulla privacy (D.Lgs 196/203, art. 41.f) ◆ riconoscere come responsabili della sicurezza on-line il DSGA e un docente su nomina del Dirigente Scolastico ◆ riconoscere il ruolo di coordinamento delle attività connesse alla sicurezza on-line all'Animatore digitale e al team per l'innovazione digitale ◆ riconoscere il ruolo di coordinamento delle attività connesse alla prevenzione del cyberbullismo al docente referente per la prevenzione e il contrasto del bullismo e del cyberbullismo di nomina del Dirigente scolastico
I DOCENTI	◆ guidare gli alunni nella navigazione in rete, insegnando ad utilizzarne le risorse e mettendoli in guardia dai pericoli ◆ approfondire a scuola la conoscenza del cyberbullismo partecipando in maniera attiva alle attività progettuali dell'istituto ◆ curare la propria formazione sulla sicurezza on-line, partecipando agli incontri informativi e formativi e consultando il materiale messo a disposizione dalla scuola
I GENITORI	◆ a prendere visione della E-safety Policy pubblicata nel sito della scuola come parte integrante del PTOF ◆ a controfirmare il Patto di corresponsabilità per la sicurezza in rete ◆ a seguire le strategie messe in atto dalla scuola per garantire la sicurezza in rete e partecipare agli incontri organizzati sulle tematiche dell'uso corretto delle tecnologie digitali, sui pericoli della rete e sul cyberbullismo
GLI ALUNNI	◆ fare un uso corretto delle tecnologie digitali ◆ rispettare le norme che regolano l'uso dei dispositivi personali a scuola ◆ prendere visione della E-safety Policy e del Patto di corresponsabilità per la sicurezza in rete ◆ partecipare attivamente alle attività organizzate dalla scuola in materia di sicurezza on line ◆ considerare i docenti come interlocutori privilegiati per ogni problematica relativa alla frequentazione di ambienti virtuali

6. Le procedure operative per la rilevazione, il monitoraggio e la gestione dei casi

La gestione delle infrazioni avverrà attraverso sanzioni coerenti al Regolamento disciplinare d'Istituto, prevedendo, in un apposito schema allegato alla Policy, una diversificata scala di possibili sanzioni su cui avrà discrezionalità la Dirigente Scolastica.

l'E-safety policy d'Istituto è stata approvata
dal Collegio dei Docenti nella seduta del 21 /11/2018.