E-SAFETY POLICY

1. INTRODUZIONE

Scopo della E –Safety Policy

Scopo del presente documento è di stabilire i principi e le linee guida per una E. Safety Policy dell'Ic di Sovizzo cioè un ***codice di condotta*** per quanto riguarda l'utilizzo delle nuove tecnologie e di Internet. Internet è un'inestimabile risorsa per l'educazione e l'informazione e offre infinite opportunità per fare ricerca, comunicare, documentare il proprio lavoro. Allo stesso tempo l'uso sempre più pervasivo di piattaforme di rete e dispositivi portatili ha esposto gli utenti e in particolare i minori a nuovi rischi, tanto più rilevanti quanto meno è diffusa una cultura relativa ai modi legittimi di usare la rete e alla consapevolezza del suo utilizzo.
Le linee guida della E-Safety Policy intendono dare un impulso allo sviluppo di una **cultura d'uso corretto e consapevole di Internet** attraverso il richiamo **a norme vigenti** per educare e sensibilizzare **gli alunni, gli insegnanti e i genitori**. Con l'indicazione di *prassi opportune* si intende inoltre favorire un *atteggiamento sempre più professionale*, da parte di tutto il personale dell'Istituto, nella *prevenzione* e nella *gestione* delle emergenze legate all'uso scorretto delle Tecnologie dell'informazione e della comunicazione (TIC).
Questo documento sarà soggetto ad aggiornamenti e farà parte integrante del Ptof dell'Istituto.

Ruoli e responsabilità (che cosa ci si aspetta da tutti gli attori della Comunità scolastica)

RUOLO	RESPONSABILITA'
Dirigente	• Garantisce la sicurezza, anche on-line, dei membri della comunità scolastica. • Individua attraverso il Collegio dei docenti un referente del Bullismo e del Cyberbullismo ed un team antibullismo; • Individua attraverso il Collegio dei docenti un Animatore Digitale. • Prevede, all'interno del PTOF corsi di aggiornamento e formazione in materia di inclusione, di rispetto dell'altro/a, delle differenze e di un utilizzo positivo e responsabile delle TIC e degli strumenti di IA. • Promuove azioni nel territorio in rete con enti, associazioni, istituzioni locali ed altre scuole, coinvolgendo docenti, alunni e genitori. Guida e supporta i docenti nella gestione deicasi di infrazione della E-Policy. • Prevede azioni culturali ed educative rivolte agli studenti, per acquisire le competenze necessarie all'esercizio di una cittadinanza consapevole.

	Guida e supporta i docenti nella gestione deicasi di infrazione della E-Policy. Assicura che gli utenti possano accedere allarete della scuola solo tramite account personale.

Animatore digitale	● Promuove la formazione interna all'Istituto nell'ambito della "Scuola digitale" sull'utilizzo delle TIC, sulla prevenzione e gestione dei rischi on line. ● Monitora e rileva le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di Internet a scuola. ● Propone soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola. ● Coinvolge la comunità scolastica nella partecipazione ad attività e progetti attinentialla "Scuola digitale". Supporta la comunità scolastica nell'introduzione ed uso degli strumenti di IA

Il personale scolastico	● Promuove negli alunni la consapevolezza nell'uso delle TIC e degli strumenti di IA adottati dall'Istituto. ● Adotta comportamenti sicuri, responsabili e professionali nell'uso della tecnologia. ● Conosce i problemi di sicurezza on line legati all'uso di cellulari, fotocamere e dispositivi portatili. ● Monitora e controlla l'uso delle TIC da parte degli alunni. ● Segnala problemi o abusi legati all'uso scorretto delle TIC anche all'esterno della scuola al DS e ai referenti Bullismo/Cyberbulismo. ● Garantisce che le comunicazioni digitali con gli studenti siano a livello professionale e solo attraverso sistemi scolastici (e-mail dell'Istituto, Classroom), non attraverso sistemi personali (e mail personali, telefoni cellulari, chat di Whatsapp ecc).

Alunni	● Leggono, comprendono e rispettano la e-policy guidati dai docenti. ● Dimostrano responsabilità nell'utilizzo dei sistemi delle tecnologie digitali conformemente da quanto richiesto dai docenti. ● Conoscono l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali. ● Conoscono le regole fondamentali per rispettare gli altri quando sono connessi in rete facendo attenzione alle comunicazioni che inviano. ● Non acquisiscono, durante le attività didattiche o all'interno della scuola, mediante telefonini o altri dispositivi elettronici, immagini, filmati o registrazioni vocali. ● Non possono usare, durante le lezioni, cellulari, tablet, giochi elettronici e riproduttori di musica.
Genitori	● Conoscono il regolamento di E – safety policy, lo condividono e aiutano i propri figli a comprenderlo e rispettarlo. ● Vigilano sull'uso delle tecnologie da parte dei loro figli. ● Conoscono le sanzioni previste dal regolamento d'Istituto nei casi di bullismo, cyber bullismo e navigazione on line a rischio.

Condivisione e comunicazione della Policy all'intera comunità scolastica

La E-Safety Policy d'Istituto si applica a tutti i membri della scuola (personale, studenti) compresi i genitori e gli utenti della comunità che ne hanno accesso.
La Policy sarà inserita nel Ptof, condivisa e comunicata al personale, agli alunni e alla comunità nei seguenti modi:

1. Pubblicazione della E-Safety Policy sul sito della scuola
2. Condivisione tramite il RE.

Gestione delle infrazioni alla Policy

Al personale, agli alunni e ai genitori vengono comunicate le possibili eventuali infrazioni e le sanzioni relative tramite questo documento. In particolare si veda il punto n. 5
Gli interventi correttivi previsti per gli alunni saranno rapportati all'età e al livello di sviluppo dell'alunno e alla gravità dell'infrazione.

Monitoraggio dell'implementazione della Policy e suo aggiornamento

La E-Safety Policy potrà essere riesaminata annualmente o quando si verificano cambiamenti significativi inerenti alle tecnologie in uso all'interno dell'Istituto.

Integrazione della Policy con Regolamenti esistenti

Il presente documento si integra con i Regolamenti presenti nell'Istituto e con il PUIA (piano di utilizzo dell'intelligenza artificiale).

2. FORMAZIONE E CURRICOLO

Curricolo delle competenze digitali per gli alunni
L'Ic di Sovizzo ha adottato un curricolo digitale sottoponendolo a revisione ogni qualvolta lo si rende necessario.

Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica

Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

Sensibilizzazione delle famiglie

3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA.

- Accesso ad internet: filtri antivirus e sulla navigazione.
  Tutti i plessi hanno la connessione alla rete Internet. Per la navigazione sicura è stato attivato il filtro direttamente sul firewall, in modo che non possa essere disattivato dai singoli utenti.
- Gestione accessi (password, backup, ecc.).
  Nei computer destinati ai docenti saranno attivati account/docenti con password. La rete LAN e Wi-Fi richiede l'accesso con password. Gli studenti accedono alla rete attraversoi pc o i tablet delle scuole utilizzati per la didattica sotto il monitoraggio dei docenti.
- E-mail.
  Tutti i docenti, il personale Ata e gli alunni (di scuola secondaria) possiedono un account Google for Education, con permessi o restrizioni diversi in base all'organizzazione di appartenenza. Per gli alunni lo scambio di email e la condivisione da e per l'esterno del dominio sono bloccati dall'amministratore.
- Sito web della scuola. Il sito istituzionale presenta un'area pubblica e una riservata alpersonale con autenticazione. Sono pubblicati documenti aggiornati per la Privacy.
- Social network.
  I social network non sono utilizzati né concessi.
- Protezione dei dati personali.
  È stata effettuata la formazione al personale scolastico sulla privacy anche connessa all'uso di strumenti digitali. Il personale di nuova nomina viene costantemente formato su questi temi.
- Viene utilizzato il registro elettronico per la didattica, gli scrutini e le comunicazioni con le famiglie e che è collegato con il gestionale di segreteria. Il personale accede con credenziali,i privilegi di accesso sono differenziati a seconda dei ruoli.

4. STRUMENTAZIONE PERSONALE

Gli alunni non possono usare, durante l'attività didattica, cellulari, tablet, giochi elettronici e riproduttori di musica a meno che tale strumentazione non sia prevista all'interno di un Piano educativo personalizzato.

Viene autorizzato l'utilizzo dei dispositivi personali unicamente per motivi lavorativi qualora i dispositivi in uso alla scuola non siano momentaneamente utilizzabili.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

a. Prevenzione

a 1. Rischi

La scuola deve coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio nell'utilizzo delle TIC. In particolare, i rischi consistono in un uso non corretto dei dispositivi della scuola.

La scuola si impegna ad attrezzare le aule con dispositivi elettronici sicuri e protetti.

Per i rischi connessi all'utilizzo delle nuove tecnologie (grooming, cyberbullismo, furto di identità, sexting), la scuola si affida a consulenti esterni.La scuola si impegna inoltre ad adeguare i propri curricoli affinché si promuovano conoscenze e competenze relative al bullismo ed al cyberbullismo.

I docenti si impegnano ad organizzare per gli alunni momenti di riflessione sui temi del cyberbullismo, dell'utilizzo consapevole di internet e a formarsi su queste tematiche.

I genitori si impegnano a prendere visione della E-Safety Policy e a seguire le azioni promosse dalla scuola per l'utilizzo consapevole della rete.

Gli alunni si impegnano a rispettare i regolamenti e a partecipare attivamente alle occasioni di confronto su queste tematiche organizzate dalla scuola.

a 2. Azioni

- Formazione del personale.
- Non consentire l'uso del cellulare o di altri dispositivi personali collegati alla rete a scuola da parte degli alunni;
- Utilizzare filtri e software che impediscono il collegamento a determinati siti (black list) ○ Inserimento nel curricolo di attività di sensibilizzazione al fenomeno del bullismo/cyber bullismo;
- Organizzazione di incontri con esperti e forze dell'ordine (Carabinieri, Magistrati, Polizia Postale).

b. Rilevazione

b 1. Che cosa segnalare

I comportamenti online da segnalare sono:

Offese e insulti tramite email o pubblicati nei gruppi whatapp o sui social network

Diffusione di foto e video intimi, violenti nei gruppi whatapp o sui social network

Esclusione daigruppi allo scopo di provocare un sentimento di emarginazione.

Rientrano nel Cyberbullismo:

- *Flaming:* messaggi online violenti e volgari mirati a suscitare battaglie verbali in un forum.

- *Harassment* (molestie): spedizione ripetuta di messaggi insultanti mirati a ferire qualcuno. ○ *Cyberstalking*: invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità. ○ *Denigrazione*:

pubblicazione all'interno di comunità virtuali di pettegolezzi e commenti crudeli, calunniosi e denigratori, al fine di danneggiare la reputazione della vittima.

- *Esclusione*: escludere deliberatamente una persona da un gruppo online per provocare in essa un sentimento di emarginazione.
- Trickery (inganno): ottenere la fiducia di qualcuno con l'inganno per poi pubblicare o condividere con altri le informazioni confidatevia web, anche attraverso la pubblicazione di audio e video confidenziali.
- *Impersonation*(sostituzione di persona): farsi passare per un'altra persona per spedire messaggi o pubblicare testi reprensibili.
- *Sexting:* invio di messaggi via smartphone ed Internet, corredati da immagini a sfondo sessuale

b 2. Come segnalare e a chi

Si veda il protocollo per la prevenzione del bullismo e cyberbullismo con il relativo modello di segnalazione.