ISTITUTO COMPRENSIVO "MAMELI"
Via Dante n. 100 – 81040 CURTI (CE)
 0823/797526 - C.F.: 93103720616- Codice Univoco Ufficio UF0RFKe_
mail: ceic8a700c@istruzione.it -P.E.C. ceic8a700c@pec.istruzione.it

E-Safety Policy

INDICE DEI CONTENUTI

1. Introduzione
- Scopo della Policy.
- Ruoli e Responsabilità
- Condivisione e comunicazione della Policy all'intera comunità scolastica.
- Gestione delle infrazioni alla Policy.
- Monitoraggio dell'implementazione della Policy e suo aggiornamento.
- Integrazione della Policy con Regolamenti esistenti.

2. Formazione e Curricolo
- Curricolo sulle competenze digitali per gli studenti.
- Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) 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.
- Gestione accessi
- E-mail.
- Sito web della scuola
- Social network.
- Protezione dei dati personali.

4. Strumentazione personale
- Per gli studenti: gestione degli strumenti personali - cellulari, tablet, ecc...
- Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc...
- Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc...

5. Prevenzione, rilevazione e gestione dei casi
Prevenzione
- Rischi
- Azioni
- Rilevazione e gestione dei casi
- Che cosa segnalare
- Come segnalare: quali strumenti e a chi.
- Come gestire le segnalazioni.

1. INTRODUZIONE

1.1 Scopo della policy.

Il presente documento ha lo scopo di illustrare all'utenza le regole per un uso corretto e responsabile degli strumenti tecnologici collegati alla "rete" in uso nell'Istituto. La nostra scuola intende promuovere lo sviluppo della competenza digitale che passa attraverso la conoscenza di procedure e competenze tecniche e di norme comportamentali, dettate da un uso consapevole e critico da parte degli alunni, delle tecnologie digitali e di internet. Lo scopo è, dunque, prevenire ed eventualmente rilevare e affrontare situazioni derivanti da un uso pericoloso delle stesse. Il primo passo è informare gli alunni dei rischi cui si espongono nella navigazione in rete; dal canto suo la scuola si attiva per limitare l'accesso a siti potenzialmente dannosi, i cui contenuti possano risultare inadeguati. Gli insegnanti, infine, hanno il ruolo di guidare le attività on-line a scuola e illustrare le regole di comportamento per la navigazione in rete.

L'Istituto" G. Mameli" ha aderito nel 2018 al progetto GENERAZIONI CONNESSE, promosso dal MIUR in collaborazione con la Comunità Europea ed ha elaborato il seguente documento, aggiornato nel corso degli anni, in conformità con le *Linee di Orientamento* per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo, emanate dal MIUR, in collaborazione con Safer Internet Center per l'Italia.

1.2 Ruoli e responsabilità

Nell'ambito di questa e-policy sono individuati i seguenti ruoli e le principali responsabilità correlate:

Il Dirigente Scolastico

- garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- garantire ai propri docenti una formazione di base sulle Tecnologie dell'Informazione e della Comunicazione (TIC) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;
- garantire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on line.

Il Referente d'Istituto per la prevenzione e contrasto del cyberbullismo

- Curare la redazione e la revisione annuale della policy sulla base delle osservazioni ricevute da tutti i soggetti interessati.
- Coordinare le iniziative per la prevenzione e di contrasto del cyberbullismo.
- Riferire al Dirigente Scolastico situazioni o problemi di particolare rilevanza su cui intervenire.

L'Animatore digitale

- Assicurare la massima diffusione della policy all'interno della comunità scolastica mediante pubblicazione sul sito della scuola;
- supportare il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre che porsi quale uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica);
- monitorare e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola;
- avere il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).
-

Il Personale docente

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- aver letto, compreso e sottoscritto la presente policy;
- segnalare qualsiasi abuso, al Dirigente Scolastico o al Referente per la prevenzione per le opportune

indagini / azioni / sanzioni;

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di INTERNET e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di INTERNET siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantire che gli alunni comprendano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di INTERNET;
- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete, ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore per garantire 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;
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all'animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- segnalare al dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di INTERNET, per l'adozione delle procedure previste dalle norme.

Personale ATA

Il personale ATA vigila ed è coinvolto nella segnalazione al Dirigente Scolastico e/o al docente Referente di comportamenti non adeguati e/o episodi bullismo/cyberbullismo.

Studenti e Studentesse

In particolare, sono tenuti a:

- essere responsabili, in relazione al proprio grado di maturità e di apprendimento, nell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti e seguire scrupolosamente le indicazioni ricevute in merito all'utilizzo delle TIC;
- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
- comprendere l'importanza di adottare buone pratiche di sicurezza on line quando si utilizzano le tecnologie digitali per non correre rischi;
- non utilizzare dispositivi personali durante le attività didattiche se non espressamente consentito dal personale docente;
- conoscere e comprendere le politiche sull'uso di dispositivi mobili e di macchine fotografiche digitali;
- capire le politiche di utilizzo delle immagini ed essere consapevoli del significato e della gravità del cyber-bullismo;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- esprimere domande, difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di INTERNET ai docenti e ai genitori.

I genitori devono:

- sostenere la scuola nel promuovere la sicurezza on line e l'accordo di E-SAFETY POLICY;
- contribuire, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- incoraggiare l'impiego delle TIC da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza;
- agire in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure

previste in caso di violazione delle regole stabilite

1.3 Condivisione e comunicazione della Policy all'intera comunità scolastica.
Per evitare che l'adozione di questa policy rappresenti un mero atto formale, l'Istituto si impegna a prendere spunto da essa come base di partenza per una serie di azioni e iniziative.
A partire dalla pubblicazione sul sito della scuola, si possono ipotizzare le seguenti:
Per il corpo docente, discussione collegiale sui contenuti, sulle pratiche indicate e su come inserire nel curricolo le tematiche di interesse della policy.
Per la componente studentesca, la discussione in classe della policy nei primi giorni di scuola, con particolare riguardo al protocollo di accoglienza per le nuove classi prime; l'inserimento di un estratto di questo documento nel diario scolastico e in particolare dei comportamenti da attuare in caso di bisogno.
Per i genitori, l'organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare.

1.4 Gestione delle infrazioni alla Policy
In relazione a quanto specificato in questa policy le infrazioni saranno gestite in modo graduale rispetto alla relativa gravità e, nel caso degli alunni, anche rispetto alla loro età.
È bene che i docenti introducano, preventivamente, attività laboratoriali miranti a sviluppare nei loro alunni una sempre maggiore consapevolezza dei rischi legati a un uso imprudente e improprio del web e che forniscano loro, ogni qualvolta avvenga un'infrazione alle regole stabilite, gli strumenti per affrontare le conseguenze dei loro errori.
I provvedimenti disciplinari da adottare da parte del Consiglio di classe nei confronti dell'alunno che ha commesso un'infrazione alla policy (in proporzione sia all'età dello studente sia alla gravità dell'infrazione commessa) saranno i seguenti:

- richiamo verbale;
- sanzioni estemporanee commisurate alla gravità della violazione commessa (es. assegnazione di attività aggiuntive da svolgere a casa su temi di Cittadinanza e Costituzione);
- nota informativa sul diario e sul registro ai genitori;
- convocazione dei genitori.

Il docente responsabile della sicurezza on line fungerà da primo punto di contatto per qualsiasi reclamo. Ogni notizia di rilievo sarà tempestivamente comunicata al Dirigente Scolastico. Eventuali denunce di bullismo on line saranno trattate in conformità con la normativa vigente.

1.5 Monitoraggio dell'implementazione della Policy e suo aggiornamento
La scuola ha un docente responsabile, che si prenderà cura della revisione e dell'aggiornamento della policy sotto la supervisione del Dirigente Scolastico.
Il monitoraggio dell'implementazione della Policy avverrà all'inizio di ogni anno scolastico, contestualmente alla revisione del PTOF, a cura del Dirigente scolastico, dell'Animatore digitale e dei collaboratori del Dirigente, a seguito di verifica atta a constatare l'insorgenza di nuove necessità e la revisione di tecnologie esistenti.

1.6 Integrazione della policy con Regolamenti esistenti
Il documento di e-policy è integrato con il Regolamento d'Istituto e con Patto di Corresponsabilità.

2.FORMAZIONE E CURRICOLO

2.1 Curricolo sulle competenze digitali per la componente studentesca.
Il **PTOF** dell'Istituto prevede un curricolo digitale verticale che parte dalla scuola dell'infanzia fino alla scuola secondaria di I grado.

2.2 Formazione del corpo docente sull'utilizzo e l'integrazione delle TIC nelle didattica.

2.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
La formazione dei docenti è ampiamente prevista dal **PTOF** dell'istituto.

2.4 Sensibilizzazione delle famiglie

Il nostro istituto ha organizzato già negli anni passati incontri aperti alle famiglie e agli studenti con enti esterni, come l'Arma dei Carabinieri, la Guardia di Finanza, per sensibilizzare docenti, alunni e genitori sui temi della sicurezza online. Anche nei prossimi anni si continuerà ad utilizzare questo approccio per la sensibilizzazione delle famiglie, con incontri che offriranno occasione di confronto e discussione sui rischi rappresentati dall'uso di cellulari, smartphone e chat line senza un'adeguata formazione in merito ai rischi derivanti da un uso inappropriato di tali dispositivi.
La scuola darà inoltre ampia diffusione, tramite pubblicazione sul sito, del presente documento di policy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso inappropriato del digitale.

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

3.1 Accesso ad Internet: filtri, antivirus e sulla navigazione.
Tutta la comunità scolastica è sensibilizzata sull'opportunità di mantenere aggiornati gli antivirus installati sulle macchine personali e controllare i dispositivi di archiviazione esterna che vengono collegati al proprio pc. Data la giovane età degli studenti del nostro istituto è fondamentale fare tutto il possibile per evitare l'esposizione a contenuti inappropriati. Gli alunni non sono mai lasciati soli nelle aule in cui sono presenti dei computer collegati ad internet.

3.2 Gestione dell 'infrastruttura e della strumentazione TIC della scuola.

Gestione accessi

La connessione alla rete wi-fi è riservata ai docenti per fini didattici e per la compilazione del registro elettronico. Agli alunni non sarà comunicata, in nessun caso, la password di accesso alla rete wi-fi scolastica. Essi potranno accedervi solo sotto la supervisione del docente esclusivamente per fini didattici utilizzando i dispositivi delle dotazioni laboratoriali (tablet e computer) sui quali è stata preventivamente impostato l'accesso a INTERNET.

E-mail

Questa scuola non pubblica indirizzi di posta elettronica personali degli alunni o del personale sul sito della scuola. Sulla rete scolastica tutti sono invitati a utilizzare solo account di posta elettronica presenti nel dominio scolastico e per scopi inerenti allo svolgimento didattico/organizzativo. Le comunicazioni tra personale scolastico, famiglie e allieve/allievi via e-mail devono avvenire preferibilmente tramite un indirizzo e-mail della scuola, all'interno della piattaforma Google Workspace, per consentire l'attivazione di protocolli di controllo. E-mail in arrivo da mittenti sconosciuti vanno trattate come sospette ed eventuali allegati non devono essere aperti.

Sito web della scuola

Il sito dell'Istituto Comprensivo è www.icmamelicurti.edu.it, in cui pubblica tutti i contenuti che saranno valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative.

3.3 Protezione dei dati personali

Si fa riferimento a tutto quanto previsto dal Decreto legislativo 30 giugno 2003, n.196 (c.d. Codice della Privacy). In questa prospettiva all'atto dell'iscrizione è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video delle /dei minori, che non violino la legge.

Ogni caso particolare sarà preso in considerazione per stabilire l'opportunità di pubblicare dati personali e sarà presentata apposita richiesta circostanziata che varrà solo per lo specifico evento. L'accesso ai dati riportati nel registro elettronico (ritardi, assenze, note e valutazioni) è riservato ai genitori della Scuola Primaria e Secondaria di primo grado tramite l'invio di una password di accesso strettamente personale.

4. Strumentazione personale

Per gli studenti: gestione degli strumenti personali - cellulari, tablet, ecc. Come da Regolamento d'Istituto agli studenti è vietato l'utilizzo del cellulare all'interno della scuola. Per quanto concerne l'utilizzo dei tablet/ computer questi possono essere utilizzati solo alla presenza del docente e per ragioni esclusivamente didattiche.

Per i docenti e per il personale della scuola: gestione degli strumenti personali - cellulari, tablet, ecc.. I docenti e il personale della scuola possono utilizzare cellulari e tablet a scopo personale non durante l'attività didattica o lavorativa.

5. Prevenzione, rilevazione e gestione dei casi

5.1 prevenzione Rischi

Al personale che opera nella scuola, e in modo particolare agli insegnanti, viene oggi offerta la possibilità di essere promotori e garanti della costruzione dialogica di un percorso formativo partecipato, ma il loro ruolo diventa spesso inevitabilmente quello di confidenti degli alunni e delle loro esperienze. Proprio per questo, gli insegnanti sono anche investiti del ruolo di "supervisori" individuando tempestivamente le problematiche e i rischi che bambini e adolescenti possono trovarsi ad affrontare ogni giorno.

La prima responsabilità degli insegnanti consiste, dunque, nell'imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente. Tra questi, un'attenzione specifica andrà prestata ai fenomeni di bullismo/cyberbullismo, sexting e adescamento**.**

5.2 Azioni

L'obiettivo che l'insegnante deve proporsi dopo avere riconosciuto il pericolo è agire di conseguenza, con azioni di contrasto efficaci e mirate, rispetto ai rischi sopra elencati.

Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli alunni in orario scolastico, vi sono le seguenti:

- diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web;
- far rispettare il divieto di utilizzo di dispositivi digitali propri, quali cellulare e smartphone, agli studenti in orario scolastico;
- dotare i dispositivi della scuola di filtri che impediscano l'accesso a siti web non adatti ai minori (black list);
- bloccare l'accesso a un sito o a un insieme di pagine impedendone la consultazione;
- controllare periodicamente i siti visitati dagli alunni;

A tal proposito, la scuola proporrà incontri formativi atti a favorire momenti di riflessione e attività laboratoriali.

5.3 Rilevazione. Che cosa segnalare

Si considerano da segnalare tutte quelle situazioni caratterizzate da *volontarie e ripetute aggressioni* mirate a insultare, minacciare, diffamare e/o ferire una persona (o un piccolo gruppo) tramite un utilizzo irresponsabile dei social network.

In particolare, si segnaleranno:

- contenuti afferenti alla violazione della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);

- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, immagini o video umilianti, insulti, ecc.);
- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione, foto o video personali, immagini pornografiche, cc.

5.4 Come segnalare: quali strumenti e a chi.

Gli insegnanti, anche con l'ausilio tecnico dell'Animatore digitale, possono provvedere a conservare le prove della condotta incauta, scorretta o dell'abuso rilevate sui pc della scuola: soprattutto la data e l'ora, il contenuto dei messaggi e, se possibile, l'ID del mittente (es. username, mail, numero di telefono cellulare) o l'indirizzo web del profilo ed il suo contenuto. Conservare la prova è utile per far conoscere l'accaduto, in base alla gravità, ai genitori degli alunni, al Dirigente scolastico e per le condotte criminose alla polizia. Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno, quantunque riferite a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte sono comunque comunicate ai genitori e per fatti rilevanti anche al Dirigente scolastico.

In particolare, la segnalazione viene fatta a entrambe le famiglie, se oltre alla vittima anche l'autore della condotta negativa è un altro alunno.

Per le segnalazioni di fatti rilevati sono previsti i seguenti strumenti che i docenti possono utilizzare sulla base della gravità dell'accaduto:

- annotazione del comportamento sul registro e comunicazione scritta ai genitori, che la devono restituire vistata;
- convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti;
- relazione scritta al Dirigente scolastico.

In base all'urgenza le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie brevi.

Per i reati più gravi (es. pedopornografia) gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti).

Inoltre, ci si potrà avvalere dei due servizi messi a disposizione dal Safer **Internet Center** il **"Clicca e Segnala"** di **Telefono Azzurro e "STOP-IT" di Save the Children**. Una volta ricevuta la segnalazione, infatti, gli operatori procederanno a coinvolgere le autorità competenti in materia.