

DIREZIONE DIDATTICA “BALDO BONSIGNORE”

Via Emerigo Amari, 1 - 91026 Mazara del Vallo (TP)

Tel: 0923 942810 - **Fax:** 0923 942810

Email: tpee058003@istruzione.it

PEC: tpee058003@pec.istruzione.it

POLICY DI E-SAFETY

Misure atte a facilitare e promuovere l'utilizzo positivo delle TIC nella didattica e negli ambienti scolastici.

Misure di prevenzione e misure di gestione di situazioni problematiche relative all'uso delle tecnologie digitali.

A.S. 2019/2020

INDICE E-Safety Policy

1. Presentazione della e-Policy
 - 1.1. Scopo della Policy
 - 1.2. Ruoli e Responsabilità
 - 1.3. Condivisione e comunicazione della Policy all'intera comunità scolastica
 - 1.4. Gestione delle infrazioni alla Policy
2. Formazione e Curricolo
 - 2.1. Curricolo sulle competenze digitali per gli studenti
 - 2.2. Piano Nazionale scuola Digitale
 - 2.3. Formazione dei docenti sull'utilizzo delle TIC nella didattica e sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
3. Gestione dell'infrastruttura e della strumentazione ICT della scuola
 - 3.1. Accesso ad Internet: filtri, antivirus e sulla navigazione
 - 3.2. Gestione accessi (password, backup, ecc.)
 - 3.3. Sito web della scuola
 - 3.4. Social network
 - 3.5. Registro della scuola
4. Rischi on line: conoscere, prevenire e rilevare
 - 4.1. Protezione dei dati personali
 - 4.2. Strumentazione personale
 - 4.3. Utilizzo del laboratorio d'informatica
5. Prevenzione, rilevazione e gestione dei casi
 - 5.1. Prevenzione
 - 5.2. Rilevazione
 - 5.3. Gestione dei casi
 - 5.4. Protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi.

1. Presentazione della e-Policy

La scuola ha elaborato questo documento in conformità con le LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo e cyberbullismo (aprile 2015) elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca. L'obiettivo è quello di educare e sensibilizzare gli alunni, gli insegnanti e i genitori all'uso sicuro e consapevole di Internet.

1.1. Scopo di una policy di e-safety

La presente e-Policy costituisce un documento regolativo per tutti i membri della comunità scolastica che hanno accesso ai sistemi informatici della scuola, con lo scopo di dare indicazioni per l'uso corretto e responsabile delle apparecchiature di cui essa dispone. In particolare viene redatta sia per regolare il comportamento degli studenti dentro le aule e nell'aula d'informatica sia per educarli ad adottare buone pratiche comportamentali nell'uso della rete, onde evitare che fenomeni di cyberbullismo si possano verificarsi dentro e/o fuori l'ambiente scolastico. A tal fine la scuola promuove azioni che limitino l'accesso a siti e ad applicazioni illeciti e conferisce ai docenti la responsabilità di guidare gli studenti nelle attività online, indicando loro regole di condotta chiare per un uso critico e consapevole di Internet anche a casa.

1.2. Ruoli e Responsabilità

- Il Dirigente Scolastico è responsabile per la sicurezza dei dati, è informato sulle linee guida contenute nella e-policy ed è garante della sua applicazione. L'Animatore Digitale ed il suo team pubblicano la e-Policy sul sito della scuola e promuovono la diffusione dei suoi contenuti.
- Gli insegnanti inseriscono tematiche legate alla sicurezza online nella didattica e guidano gli alunni nelle attività che prevedono l'accesso alla rete.
- I genitori sostengono la scuola nel promuovere la sicurezza online, leggendo la e-Policy e partecipando agli incontri organizzati dalla scuola sui temi della sicurezza online.
- Gli alunni conoscono e rispettano i regolamenti (generali e specifici delle aule di informatica) e segnalano al docente di classe eventuali usi impropri della rete e dei dispositivi.

1.3. Condivisione e comunicazione della e-Policy all'intera comunità scolastica

La e-Policy è pubblicata sulla Home Page del sito della scuola dopo essere stata approvata dal Collegio dei Docenti. All'inizio di ogni anno scolastico, insieme al Patto di Corresponsabilità Educativa, la e-Policy è illustrata ai genitori e agli alunni della scuola.

2. Formazione e Curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

Il curricolo è strutturato al fine di:

- insegnare ciò che è accettabile nell'utilizzo di Internet e ciò che è vietato, fornendo strumenti per l'utilizzo efficace di Internet e la conoscenza delle conseguenze delle violazioni;
- mostrare come produrre, pubblicare e presentare contenuti digitali in modo appropriato, sia in ambienti privati sia in ambienti condivisi;
- insegnare la valutazione dei contenuti Internet;
- impiegare materiali prelevati da Internet a scopi didattici conformemente al diritto d'autore;
- rendere alunne e alunni criticamente consapevoli dei materiali che si leggono sul web allo scopo di vagliare le informazioni prima di accettarne la fondatezza, la coerenza, le origini;
- mostrare la segnalazione di contenuti Internet sgradevoli o illegali.

2.2. Formazione dei docenti sull'utilizzo delle TIC nella didattica e sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

La formazione del corpo docente viene organizzata su due livelli: interno ed esterno. A livello interno, nel PTOF si prevede che una parte della formazione sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica e ai temi informatici in generale. Un buon punto di riferimento per la formazione online sarà costituito dalla piattaforma "Generazioni Connesse" la quale fornisce diverse tipologie di corsi che analizzano il fenomeno del cyberbullismo da diverse sfaccettature. Per quanto riguarda la formazione esterna, la scuola assicura tempestiva e capillare informazione su corsi e seminari che riguardino tali argomenti, cercando altresì di agevolare il personale che intenda parteciparvi.

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

3.1. Piano Nazionale Scuola Digitale

Per favorire lo sviluppo della didattica digitale la scuola cerca di arricchirsi di nuove strumentazioni digitali per la realizzazione di ambienti didattici coerenti con il Piano Nazionale.

La scuola ha aderito alle varie iniziative connesse al PNSD fra cui:

- Animatori digitali
- Ambienti digitali
- Formazione del personale
- Atelier creativi

La scuola svolge, inoltre, attività di CODING ad integrazione delle competenze digitali previste dalle Indicazioni Nazionali, favorendo negli alunni lo sviluppo del “pensiero computazionale”.

3.2. Accesso ad internet: filtri, antivirus e sulla navigazione

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. Le scuole dell'Istituto sono dotate di antivirus, monitorati e tenuti aggiornati dai responsabili dei laboratori informatici.

3.3. Gestione accessi

I computer, sia nell'aula informatica che nelle classi, hanno un unico nome utente e password. La connessione alla rete Wi-Fi è riservata ai docenti per fini didattici ed è accessibile solo dietro identificazione personale.

3.4. Sito web della scuola

Il sito dell'Istituto è raggiungibile all'indirizzo:

<https://www.terzocircolomazara.edu.it/>.

Il sito viene utilizzato per la pubblicazione di Atti e Circolari, per la comunicazione con le famiglie e per presentare le iniziative e le attività che la scuola rivolge alla propria utenza.

La pagina Facebook della scuola “Direzione Didattica Baldo Bonsignore” pubblica i contenuti pertinenti alle finalità didattiche svolte dagli alunni.

Il Dirigente e lo staff verificano i contenuti destinati alla pubblicazione.

3.5. Social network

In alcune classi della scuola è diffuso l'utilizzo della piattaforma didattica Edmodo e WeSchool.

3.6. Registro elettronico "NUVOLA"

Il registro elettronico della scuola è utilizzato dai genitori per visionare le valutazioni quadrimestrali.

4. Rischi on line: conoscere, prevenire e rilevare

4.1. Protezione dei dati personali

In fase di iscrizione degli alunni alla scuola i genitori sottoscrivono un'informativa sul trattamento dei dati personali in ottemperanza all'art. 13 D.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali). I genitori rilasciano per ogni evento il consenso all'utilizzo di materiale fotografico e audiovisivo riservato ed elaborati degli alunni per esporli anche in sedi diverse da quelle dell'Istituto, quali pubblicazioni in formato digitale e siti web. In caso di utilizzo di piattaforme digitali condivise o di strumenti per la creazione e la gestione di classi virtuali viene acquisito preventivamente il consenso informato dei genitori. In caso di attività di ampliamento dell'offerta formativa, organizzate in collaborazione con Enti esterni, viene richiesto preventivamente ai genitori il consenso informato alle riprese audio/ video e al loro eventuale utilizzo per scopi didattici, informativi e divulgativi anche tramite pubblicazione su siti web.

4.2. Strumentazione personale

Per gli studenti della scuola primaria è vietato l'utilizzo di cellulari per l'intera durata delle attività scolastiche.

Per i docenti, durante il loro orario di servizio, è consentito l'utilizzo di dispositivi elettronici personali solo ed esclusivamente per fini didattici.

4.3. Utilizzo del laboratorio d'informatica

- Gli studenti della scuola potranno accedere al laboratorio solo se accompagnati da un docente. È espressamente vietata la permanenza in laboratorio degli alunni in assenza dell'insegnante.

- L'accesso è garantito a tutte le classi, la precedenza viene riservata agli insegnanti di "Tecnologia" secondo il calendario affisso all'interno dell'aula informatica.
- L'insegnante avrà cura, all'inizio ed alla fine di ogni lezione, di verificare l'integrità di ogni singola postazione e di ogni singolo strumento utilizzato. L'insegnante, qualora alla fine della lezione dovesse rilevare danni che non erano presenti all'inizio, è tenuto a darne tempestiva comunicazione al responsabile di laboratorio che ne informerà il Dirigente Scolastico.
- Ogni docente dovrà compilare dettagliatamente e in ogni parte il registro del laboratorio d'informatica da richiedere al responsabile di laboratori.
- Gli utenti sono tenuti a garantire il corretto utilizzo delle apparecchiature e ad usarle in modo da evitare qualsiasi danneggiamento hardware e software. In casi particolarmente gravi potranno essere ritenuti responsabili di eventuali danneggiamenti delle attrezzature.

5. Prevenzione, rilevazione e gestione dei casi

5.1. Prevenzione

La scuola si impegna ad attrezzare le aule con dispositivi elettronici sicuri e protetti. I docenti si impegnano ad organizzare per gli alunni momenti di riflessione sui temi 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.

5.2. Rilevazione

Si considerano da segnalare tutte quelle situazioni che si configurano come episodi di cyberbullismo (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), ma anche usi inappropriati della rete (siti d'odio, contenuti non adatti all'età degli alunni...). I docenti di classe informano il referente per il bullismo/cyber bullismo. Il referente informa il Dirigente Scolastico, il quale procede ad informare le famiglie. Tutte le segnalazioni riportate dai docenti vengono registrate su apposita scheda (diario di bordo).

5.3. Gestione dei casi

La gestione dei casi rilevati va differenziata a seconda della loro gravità; fermo restando che è opportuna la condivisione a livello di Consiglio di Classe di ogni episodio rilevato, anche minimo, alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e su come rimediare. Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire.

5.4. Protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi.

Non vi sono protocolli siglati, ma forme ricorrenti di collaborazione nella prevenzione e contrasto del bullismo e del cyberbullismo da parte dell'Ente Locale, del Comando dei Carabinieri, della Polizia Postale e di associazioni.

Il Dirigente scolastico
Prof.ssa Serafina Di Rosa