



Ministero dell'istruzione e del merito



We prepare for



Ministero dell'Istruzione



ISTITUTO COMPRENSIVO "G. CALÒ- G. DELEDDA- S.G. BOSCO"
di Scuola dell'Infanzia, Primaria e Secondaria di 1° Grado ad indirizzo Musicale
V.le M. D'UNGHERIA N. 86 -74013 GINOSA (TA)
tel. +390998245663 - C.F. 90283560739
PEO: TAIC878009@istruzione.it – PEC: TAIC878009@pec.istruzione.it
Sito web: www.scuolacalo.edu.it

E- Safety Policy

POLICY DI E-SAFETY 2025

Istituto Comprensivo "G. Calò – G. Deledda – S. G. Bosco"

1. Introduzione

L'Istituto Comprensivo "G. Calò – G. Deledda – S. G. Bosco", a seguito del dimensionamento scolastico, ha ritenuto necessario aggiornare la propria policy di e-safety per rispondere all'evoluzione tecnologica e normativa che ha caratterizzato gli ultimi anni. La trasformazione digitale ha accelerato notevolmente, con l'introduzione di nuove tecnologie come l'intelligenza artificiale generativa, dispositivi di realtà aumentata e virtuale, e una sempre maggiore centralità degli ambienti digitali nella vita quotidiana degli studenti.

La presente policy si pone come obiettivo quello di fornire linee guida aggiornate per un utilizzo sicuro, consapevole ed etico delle tecnologie digitali, implementando quanto previsto dal Piano Scuola 4.0 e dalle più recenti normative in materia di sicurezza informatica, protezione dei dati personali e prevenzione dei rischi online.

1.1 Scopo della Policy

Le tecnologie digitali sono diventate parte integrante della vita quotidiana e dell'esperienza educativa. Gli studenti interagiscono con esse fin dalla più tenera età, configurandosi come "nativi digitali avanzati" che hanno familiarità con interfacce sempre più intuitive, ma spesso non possiedono gli strumenti critici necessari per navigare consapevolmente nel mondo digitale.

La presente policy si propone di:

- Garantire un utilizzo sicuro e responsabile delle Tecnologie dell'Informazione e della Comunicazione (TIC) in ambito scolastico
- Proteggere studenti e personale dai rischi associati all'uso improprio delle tecnologie digitali
- Fornire strumenti per l'identificazione e la gestione di problematiche legate all'uso delle tecnologie
- Promuovere una cultura della cittadinanza digitale responsabile
- Regolamentare l'uso di tecnologie emergenti come l'intelligenza artificiale generativa
- Integrare le competenze digitali nel curriculum scolastico

1.2 Ruoli e Responsabilità

Dirigente scolastico:

- Garantire la tutela degli aspetti legali relativi alla privacy e alla protezione dei dati
- Assicurare adeguata formazione sulle TIC al personale
- Supervisionare l'implementazione dei protocolli di sicurezza digitale
- Coordinare le risposte agli incidenti di sicurezza informatica
- Garantire l'aggiornamento periodico della policy

Direttore dei Servizi Generali e Amministrativi:

- Gestire gli aspetti tecnici e amministrativi delle infrastrutture digitali
- Coordinare gli interventi di manutenzione e aggiornamento
- Supervisionare la gestione dei dati amministrativi digitali
- Garantire l'applicazione delle misure di sicurezza per i dati sensibili

Animatore digitale:

- Coordinare la formazione interna sui temi del PNSD e del Piano Scuola 4.0
- Promuovere la partecipazione della comunità scolastica alle iniziative digitali
- Individuare soluzioni metodologiche e tecnologiche innovative
- Supportare il corpo docente nell'implementazione delle tecnologie
- Monitorare e valutare l'efficacia degli interventi digitali

Team per l'innovazione digitale:

- Supportare l'Animatore digitale nelle sue funzioni
- Fornire assistenza tecnica di primo livello
- Promuovere la diffusione di buone pratiche
- Collaborare alla gestione delle piattaforme digitali d'istituto

Docenti facilitatori digitali (nuova figura):

- Supportare i colleghi nell'uso delle tecnologie in classe
- Promuovere metodologie didattiche innovative
- Facilitare l'integrazione delle TIC nelle pratiche quotidiane
- Fornire consulenza sui temi della sicurezza digitale

Docenti:

- Integrare le tecnologie digitali nella didattica in modo sicuro e consapevole
- Vigilare sull'uso delle TIC da parte degli studenti
- Educare gli alunni ai rischi della rete e alle strategie di protezione
- Rilevare e segnalare eventuali problematiche
- Aggiornare continuamente le proprie competenze digitali
- Utilizzare responsabilmente i sistemi di intelligenza artificiale come supporto alla didattica

Studenti:

- Rispettare le regole di utilizzo delle TIC a scuola
- Segnalare situazioni problematiche o di potenziale rischio
- Utilizzare in modo consapevole e responsabile le tecnologie
- Rispettare la privacy propria e altrui negli ambienti digitali
- Sviluppare un approccio critico nell'utilizzo delle risorse digitali e dell'IA

Genitori:

- Collaborare con la scuola nella supervisione dell'uso delle tecnologie
- Partecipare alle iniziative di formazione proposte dalla scuola
- Monitorare l'utilizzo dei dispositivi a casa
- Segnalare eventuali situazioni problematiche

1.3 Condivisione e comunicazione della Policy

La policy sarà condivisa con l'intera comunità scolastica attraverso:

Per il personale scolastico:

- Pubblicazione sul sito web della scuola e sull'area riservata

- Discussione negli organi collegiali (collegio docenti, dipartimenti, consigli di classe)
- Sessioni di formazione dedicate
- Repository di materiali e risorse sulla sicurezza digitale
- Comunicazioni periodiche sugli aggiornamenti
- Per gli studenti:
 - Presentazione all'inizio dell'anno scolastico
 - Integrazione nei percorsi di educazione civica digitale
 - Workshop e laboratori dedicati
 - Progetti peer-to-peer sulla sicurezza online
 - Visualizzazione della policy in formato semplificato nelle aule e nei laboratori
- Per i genitori:
 - Presentazione durante le assemblee di inizio anno
 - Incontri formativi specifici
 - Newsletter periodica sulle tematiche della sicurezza online
 - Area dedicata sul sito web della scuola
 - Vademecum stampato e digitale

1.4 Gestione delle infrazioni alla Policy

Le infrazioni saranno gestite in modo graduale rispetto alla gravità e all'età degli alunni.

Infrazioni degli alunni:

- Richiamo verbale
- Riflessione guidata sul comportamento inappropriato
- Attività educative sul tema della cittadinanza digitale
- Limitazione temporanea dell'accesso alle risorse digitali
- Nota sul registro elettronico
- Comunicazione alla famiglia
- Colloquio con i genitori
- Convocazione dal Dirigente Scolastico
- Nei casi più gravi, provvedimenti disciplinari secondo il regolamento d'istituto

Infrazioni del personale scolastico:

- Richiamo verbale
- Richiamo scritto
- Intervento del Dirigente Scolastico
- Provvedimenti disciplinari secondo la normativa vigente

Infrazioni dei genitori:

- Comunicazione del problema
- Colloquio con i docenti
- Convocazione da parte del Dirigente Scolastico
- Limitazione dell'accesso alle piattaforme d'istituto

1.5 Monitoraggio e aggiornamento della Policy

Il monitoraggio sarà effettuato:

- Trimestralmente dal Team per l'innovazione digitale

- Annualmente in sede di revisione del PTOF
- Su segnalazione di problematiche specifiche
- In seguito a modifiche normative
- L'aggiornamento della policy avverrà:
- Con cadenza biennale
- In caso di innovazioni tecnologiche significative
- In caso di modifiche normative rilevanti
- Su indicazione degli organi competenti

2. Formazione e Curricolo

2.1 Curricolo sulle competenze digitali per gli studenti

Il curricolo digitale è stato aggiornato in base al DigCompEdu 2.2 (versione 2023) e al quadro di riferimento per le competenze digitali dei cittadini e integrato con le indicazioni del Piano Scuola 4.0. In particolare, si prevedono i seguenti traguardi:

Scuola dell'infanzia:

- Approccio ludico alle tecnologie
- Prime nozioni di sicurezza digitale
- Esplorazione guidata di contenuti digitali educativi

Scuola primaria:

- Alfabetizzazione digitale di base
- Uso consapevole dei dispositivi digitali
- Ricerca guidata di informazioni online
- Riconoscimento di contenuti inappropriati
- Principi base di cittadinanza digitale
- Approccio critico all'uso dell'IA generativa

Scuola secondaria di primo grado:

- Uso autonomo e responsabile delle TIC
- Valutazione critica delle fonti di informazione
- Comprensione dei meccanismi della comunicazione digitale
- Conoscenza dei rischi online e strategie di protezione
- Principi di protezione dei dati personali
- Comprensione del funzionamento base dell'intelligenza artificiale
- Uso etico degli strumenti digitali di collaborazione e creazione

2.2 Formazione dei docenti sull'utilizzo delle TIC nella didattica

La formazione dei docenti prevede:

- Percorsi base per i neofiti digitali
- Percorsi avanzati per i docenti con competenze intermedie
- Formazione specialistica per il Team dell'innovazione
- Corsi sulle metodologie didattiche innovative (flipped classroom, didattica

immersiva, gamification)

- Workshop sull'uso responsabile dell'intelligenza artificiale nella didattica
- Formazione sulla creazione di contenuti digitali accessibili
- Autoformazione attraverso piattaforme dedicate

2.3 Formazione sulla sicurezza online

La formazione specificamente dedicata alla sicurezza online include:

- Aggiornamenti sulle nuove minacce digitali
- Formazione sul riconoscimento e la gestione del cyberbullismo
- Workshop sulla protezione dei dati personali
- Seminari sui rischi dell'IA generativa (deepfake, disinformazione)
- Corsi sulla gestione dell'identità digitale
- Formazione sul riconoscimento delle dipendenze digitali

2.4 Sensibilizzazione delle famiglie

Le attività di sensibilizzazione per le famiglie comprendono:

- Incontri periodici con esperti di sicurezza informatica
- Collaborazioni con la Polizia Postale
- Workshop pratici sull'uso dei controlli parentali
- Vademecum digitale periodicamente aggiornato
- Sportello di consulenza digitale
- Newsletter mensile sulle tematiche della sicurezza online
- Percorsi di formazione genitori-figli sulla cittadinanza digitale

3. Gestione dell'infrastruttura e della strumentazione ICT

3.1 Accesso a Internet e sistemi di protezione

L'accesso a Internet è disponibile in tutti gli ambienti scolastici attraverso:

- Rete Wi-Fi dedicata al personale con autenticazione
- Rete Wi-Fi dedicata agli studenti con filtri di navigazione
- Connessioni cablate nei laboratori informatici
- Gestione centralizzata degli accessi

Sistemi di protezione:

- Firewall di nuova generazione con filtri per contenuti inappropriati
- Sistema di monitoraggio del traffico di rete
- Filtri DNS per il blocco di siti pericolosi
- Antivirus centralizzato con aggiornamenti automatici
- Sistema di prevenzione delle intrusioni
- Protezione anti-malware avanzata

3.2 Gestione degli accessi e delle identità digitali

L'accesso ai sistemi informatici è regolato attraverso:

- Sistema di Single Sign-On (SSO) per le piattaforme didattiche
- Autenticazione a due fattori per gli account del personale
- Identità digitali per studenti con permessi differenziati per età

- Password policy aggiornata (complessità, scadenza, ecc.)
- Gestione centralizzata degli account istituzionali
- Sistema di backup automatizzato dei dati critici
- Procedura di revoca immediata degli accessi

3.3 Piattaforme digitali e cloud

L'istituto utilizza:

- Google Workspace for Education Plus come ambiente principale di apprendimento
- Registro elettronico con accesso differenziato per docenti, genitori e studenti
- Piattaforma dedicata per la formazione online del personale
- Repository sicuro per la condivisione di materiali didattici
- Ambiente cloud protetto per l'archiviazione dei documenti
- Piattaforme didattiche specifiche autorizzate dal Team digitale

3.4 Sito web e comunicazione digitale

Il sito web dell'istituto è conforme alle linee guida AGID e prevede:

- Area pubblica informativa
- Area riservata accessibile tramite credenziali
- Sezione dedicata alla sicurezza online
- Repository di risorse educative digitali
- Sistema di newsletter per le comunicazioni
- Integrazione con i social media ufficiali dell'istituto
- Accesso da dispositivi mobili ottimizzato

3.5 Protezione dei dati personali

La protezione dei dati è garantita attraverso:

- Conformità al GDPR e al Codice Privacy aggiornato
- Nomina e formazione periodica dei responsabili del trattamento
- Registro dei trattamenti regolarmente aggiornato
- Valutazioni d'impatto sulla protezione dei dati (DPIA) per nuove tecnologie
- Procedure di data breach notification
- Informative specifiche per il trattamento dei dati nell'ambiente digitale
- Contratti di responsabilità con i fornitori di servizi digitali

4. Strumentazione personale e BYOD

4.1 Policy BYOD (Bring Your Own Device) per gli studenti

In linea con il Piano Scuola 4.0, l'istituto ha implementato una policy BYOD che prevede:

Scuola primaria:

- Uso dei dispositivi personali non consentito durante l'orario scolastico
- Dispositivi consegnati spenti all'ingresso e custoditi in appositi contenitori

- Eccezioni solo per studenti con BES e su indicazione del PDP/PEI

Scuola secondaria di primo grado:

- Uso dei dispositivi personali consentito solo per attività didattiche programmate
- Registrazione obbligatoria dei dispositivi presso il coordinatore di classe
- Connessione solo tramite rete Wi-Fi dedicata agli studenti
- Divieto di utilizzo durante l'intervallo e i cambi d'ora
- Divieto di registrazioni audio/video non autorizzate
- Divieto di accesso a social network personali durante le lezioni
- Responsabilità personale per la custodia dei dispositivi

4.2 Gestione dei dispositivi per il personale docente

I docenti possono utilizzare dispositivi personali per attività didattiche alle seguenti condizioni:

- Connessione attraverso la rete Wi-Fi dedicata al personale
- Rispetto delle norme sulla privacy degli studenti
- Divieto di installazione di software non autorizzato sui dispositivi della scuola
- Divieto di condivisione delle credenziali personali
- Obbligo di segnalazione di eventuali violazioni della sicurezza

4.3 Dispositivi per il personale ATA

Il personale ATA è autorizzato all'uso di dispositivi personali con le seguenti limitazioni:

- Utilizzo consentito solo durante le pause
- Divieto di accesso ai dati sensibili da dispositivi personali
- Divieto di connessione alla rete amministrativa da dispositivi personali
- Obbligo di rispetto della policy di sicurezza dell'istituto

5. Rischi, prevenzione e gestione dei casi

5.1 Tipologie di rischi online

Gli studenti possono essere esposti a diversi rischi online, tra cui:

Contenuti:

- Esposizione a materiale inappropriato
- Fake news e disinformazione
- Contenuti che promuovono comportamenti dannosi
- Materiale generato dall'IA potenzialmente fuorviante

Contatti:

- Cyberbullismo e molestie online
- Adescamento (grooming)
- Furto d'identità
- Violazione della privacy

Comportamenti:

- Sexting e condivisione di immagini intime
- Dipendenza digitale
- Uso improprio dell'IA generativa
- Violazione del copyright
- Comportamenti illegali online

5.2 Azioni di prevenzione

L'istituto implementa le seguenti azioni preventive:

A livello tecnico:

- Filtri di navigazione aggiornati
- Monitoraggio dell'uso della rete
- Software di protezione aggiornati
- Backup regolari dei dati critici

A livello educativo:

- Percorsi di cittadinanza digitale
- Workshop sulla sicurezza online
- Attività di peer education
- Progetti specifici sul cyberbullismo

A livello organizzativo:

- Protocolli di intervento chiari
- Formazione specifica del personale
- Collaborazione con enti esterni specializzati
- Team anti-bullismo e cyberbullismo attivo

5.3 Rilevazione dei casi problematici

La rilevazione dei casi avviene attraverso:

- Osservazione diretta del comportamento degli studenti
- Segnalazioni da parte degli studenti
- Segnalazioni da parte delle famiglie
- Monitoraggio dei social network ufficiali
- Rilevazioni periodiche attraverso questionari anonimi
- Sistema di segnalazione online sul sito della scuola

5.4 Gestione dei casi

La gestione dei casi segue un protocollo strutturato:

Casi di contenuti inappropriati:

1. Blocco immediato dell'accesso ai contenuti
2. Documentazione dell'accaduto
3. Comunicazione ai genitori
4. Attività educative mirate

Casi di cyberbullismo:

1. Raccolta di informazioni e prove
2. Colloqui individuali con le parti coinvolte
3. Coinvolgimento delle famiglie
4. Intervento del Team anti-bullismo
5. Sanzioni disciplinari secondo il regolamento
6. Supporto psicologico alle vittime
7. Percorsi rieducativi per i responsabili
8. Nei casi gravi, segnalazione alle autorità competenti

Casi di adescamento o situazioni gravi:

1. Documentazione immediata delle evidenze
2. Segnalazione al Dirigente Scolastico
3. Comunicazione alle famiglie
4. Segnalazione alle autorità competenti
5. Supporto psicologico agli studenti coinvolti

6. Integrazione con il curriculum di Educazione Civica Digitale

La policy è integrata nel curriculum di Educazione Civica, con particolare riferimento all'asse della cittadinanza digitale, attraverso:

- Moduli specifici sulla sicurezza online
- Percorsi interdisciplinari sulla verifica delle fonti digitali
- Progetti sull'uso consapevole dei social media
- Attività di analisi critica dell'informazione digitale
- Laboratori sull'uso etico dell'intelligenza artificiale
- Riflessioni sulla propria identità digitale
- Educazione alla privacy e alla protezione dei dati personali

Glossario

- Adescamento online (grooming): processo attraverso cui un adulto stabilisce una relazione di fiducia con un minore per scopi inappropriati.
- BYOD: Bring Your Own Device, pratica che consente l'utilizzo di dispositivi personali in contesto scolastico.
- Cyberbullismo: forma di bullismo attuata attraverso l'uso di mezzi elettronici.
- Deepfake: contenuti multimediali manipolati tramite IA per creare false rappresentazioni di persone o eventi.
- DigCompEdu: quadro europeo delle competenze digitali per gli educatori.
- GDPR: General Data Protection Regulation, regolamento europeo sulla protezione dei dati.
- IA generativa: sistemi di intelligenza artificiale in grado di creare contenuti originali (testi, immagini, video, ecc.).
- Piano Scuola 4.0: piano di investimento per la trasformazione digitale delle scuole italiane.
- Sexting: invio o ricezione di messaggi, immagini o video a sfondo sessuale.
- Sistema SSO: Single Sign-On, sistema che permette l'accesso a più applicazioni

con un'unica autenticazione.

Ginosa, 09/04/2025

La Dirigente Scolastica
Prof.ssa Marianna Galli (f.to digitalmente)