CIRCOLO DIDATTICO 2 CD.PROF.ARC.CAPUTI - C.F. 83004410722 C.M. BTEE06900L - AFAE306 - UFFICIO_PROTOCOLLO
Prot. 0004099/U del 18/09/2026 13:43 I.1.2 - norme e regolamenti interni(regolamento dell'istituto, carta dei servizi, regolamenti della bibliote

Il Circolo Didattico Statale Bisceglie "Prof. Arc. Caputi"

Generazioni Connesse
SAFER INTERNET CENTRE



E-Safety Policy





"Una rivoluzione non avviene quando la società adotta nuovi strumenti, avviene quando la società adotta nuovi comportamenti"
— Clay Shirky

1. INTRODUZIONE

Oggi viviamo in una realtà sempre più digitale in cui le tecnologie dell'informazione e della comunicazione (TIC) sono diventate parte integrante della nostra società. Le informazioni digitali rappresentano il linguaggio comune attraverso il quale comunichiamo e interagiamo quotidianamente, contribuendo all'affermazione di modelli comunicativi fortemente interattivi.

La scuola è chiamata in primo luogo a confrontarsi con questa realtà, a preparare gli alunni a vivere da protagonisti la moderna società delle tecnologie digitali e a insegnare a cogliere attivamente le potenzialità positive che esse offrono (in linea con i principi della *Dichiarazione dei diritti in Internet* del 14 luglio 2015).

Tuttavia, all'ampiezza delle opportunità si affiancano specifici rischi. L'elevata interconnessione espone gli utenti a minacce sempre più numerose e diversificate (in conformità con la **Legge 29 maggio 2017, n. 71** e la **Legge 17 maggio 2024, n. 70**, nonché con le relative *Linee di orientamento per la prevenzione e il contrasto del bullismo e del cyberbullismo* del Ministero dell'Istruzione e del Merito).

In questo contesto emerge la necessità di promuovere un uso consapevole, critico e responsabile delle tecnologie digitali, attraverso azioni educative finalizzate a formare gli alunni quali futuri cittadini digitali (*e-citizen*) consapevoli, aggiornati e creativi.

Il nostro Circolo, avendo aderito al progetto **SIC (Safer Internet Centre) - Generazioni Connesse**, promosso dal Ministero dell'Istruzione e del Merito (MIM) in collaborazione con la Commissione Europea, ha intrapreso un percorso strutturato per favorire un uso corretto e sicuro delle nuove tecnologie e della rete Internet, promuovendo comportamenti idonei a prevenire i rischi connessi a un utilizzo improprio dei mezzi digitali.

L'**E-SAFETY POLICY** definisce la condotta adottata dall'Istituzione Scolastica nell'impiego delle tecnologie dell'informazione e della comunicazione nella didattica, sia in ambito scolastico sia extrascolastico (relativamente alle attività di studio e approfondimento domestico qualora sia esplicitamente richiesto l'uso di tali strumenti). Il documento delinea una visione integrata del fenomeno della Rete e comprende:

- le norme comportamentali e di *netiquette*;
- le procedure per l'utilizzo delle TIC negli ambienti di apprendimento scolastici;
- le misure volte alla prevenzione, rilevazione e gestione delle criticità connesse all'uso delle tecnologie digitali.

La promozione della sicurezza in Rete costituisce una responsabilità condivisa dell'intera comunità scolastica, la quale si impegna a realizzare interventi di sensibilizzazione, prevenzione e formazione per contrastare i rischi legati a fenomeni quali il cyberbullismo.

Tutto il personale scolastico è pertanto coinvolto nel monitoraggio dell'uso di Internet e nell'attuazione delle direttive per una navigazione sicura e responsabile.

Il presente documento costituisce parte integrante del *Regolamento di Disciplina degli Alunni* ed è portato a conoscenza dei genitori/tutori legali, degli studenti e di tutto il personale della scuola. Le prescrizioni qui contenute si applicano a tutti gli spazi, laboratori e ambienti di apprendimento dell'Istituto. Le regole d'accesso alla Rete sono esposte negli ambienti dotati di postazioni informatiche collegate e integrano il Regolamento d'Istituto.

2. FORMAZIONE E CURRICOLO

Per l'Istituzione Scolastica, l'uso consapevole delle tecnologie risponde a fondamentali esigenze formative e trasversali alle diverse discipline: realizzare ambienti di apprendimento multimediali efficaci in coerenza con precisi obiettivi educativi e valori sociali quali l'autonomia, il pensiero critico, la responsabilità e la partecipazione attiva. Non si tratta soltanto di consolidare le competenze tecnico-strumentali degli alunni, ma di guidarli a vivere l'esperienza digitale con adeguata consapevolezza dei processi affettivi, relazionali e di rappresentazione sociale coinvolti.
L'Istituto ha avviato da tempo un processo di innovazione tecnologica volto all'integrazione delle TIC nella didattica per l'evoluzione dei processi di apprendimento. Nel corso degli anni, la scuola ha aderito a differenti opportunità progettuali (tra cui le azioni dei Fondi Strutturali Europei PON/PNRR e i piani di investimento per la transizione digitale) finalizzate all'ammodernamento delle dotazioni infrastrutturali e tecnologiche:

- realizzazione e potenziamento delle reti di cablaggio e della connettività Wi-Fi/LAN nei plessi dell'Istituto, per consentire l'accesso sicuro alla Rete da parte di alunni e personale autorizzato;
- completamento della dotazione di Display Interattivi Touch / LIM e di postazioni informatiche nelle aule, nei laboratori e negli uffici amministrativi per la gestione dei dati e dei servizi digitali dell'Istituto;
- allestimento di ambienti didattici innovativi e *atelier creativi* destinati alle attività di *coding*, robotica educativa e *digital storytelling*.

La scuola aderisce alle iniziative nazionali e internazionali dedicate all'informatica e al pensiero computazionale (quali *"L'Ora del Codice"* e il progetto *"Programma il Futuro"*, promosso dal MIM in collaborazione con il CINI – Consorzio Interuniversitario Nazionale per l'Informatica). Tali attività mirano a fornire strumenti accessibili per introdurre i concetti fondamentali della programmazione e sviluppare le capacità logiche di *problem solving*.
Questi percorsi si integrano coerentemente con il progetto **Generazioni Connesse**, che costituisce un'occasione di riflessione sistemica sulle tematiche della sicurezza online e dell'impiego virtuoso del digitale nella didattica.
L'animatore digitale e il Team per l'Innovazione Digitale supportano e guidano il processo di digitalizzazione dell'Istituto, in attuazione delle linee guida per la transizione digitale e del Piano Nazionale Scuola Digitale (PNSD).

SENSIBILIZZAZIONE DELLE FAMIGLIE

La collaborazione tra scuola e famiglia è elemento determinante per la diffusione di un modello culturale fondato sull'uso critico della Rete, intesa come ambiente di vita in grado di strutturare esperienze cognitive, affettive e socio-relazionali (in conformità con le *Linee di orientamento per la prevenzione e il contrasto del bullismo e del cyberbullismo*).
La presenza di sportelli di ascolto e di supporto psicologico, unita alla collaborazione con gli Enti Locali, le Aziende Sanitarie Locali (ASL/ATS) e gli organi di Polizia di Stato (tra cui la Sezione Operativa per la Sicurezza Cibernetica - Polizia Postale), costituisce una risorsa strategica per la prevenzione e la gestione dei fenomeni di disagio, bullismo e cyberbullismo.
Al fine di condividere regole e responsabilità comuni nell'impiego sicuro dei dispositivi e della Rete sia nel contesto scolastico sia in quello domestico, si invitano i genitori e i tutori legali a prendere visione e ad attenersi alle prescrizioni contenute nel presente documento.

I genitori/tutori sono chiamati a promuovere il rispetto di tali norme anche a casa, affiancando i minori durante la navigazione e adottando adeguate misure di protezione (compresi i sistemi di controllo parentale/*parental control*) per ridurre l'esposizione a contenuti inappropriati o rischiosi.
Per consolidare tale alleanza educativa, l'Istituto promuove incontri informativi e formativi rivolti alle famiglie (con particolare attenzione alle classi terminali), focalizzati sulle finalità del progetto *Generazioni Connesse*, sulla sicurezza in Rete, sulla cittadinanza digitale e sulla prevenzione dei rischi informatici e del cyberbullismo.

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

L'Istituto mette a disposizione di docenti e alunni i seguenti servizi informatici e infrastrutture tecnologiche per fini didattici e istituzionali:

- aule dotate di Monitor Touch / LIM interattive e connessione di rete protetta (cablata e/o Wi-Fi);
- dispositivi mobili (tablet e PC portatili) con accesso controllato alla Rete;
- postazioni PC fisso in aula e nei laboratori informatici;
- account di posta elettronica istituzionale e liste di distribuzione professionali per il personale;
- ambienti di apprendimento online, piattaforme cloud dedicate (es. Google Workspace for Education / Microsoft 365) e blog/pagine di classe ad uso didattico;
- portale web istituzionale dell'Istituto per la consultazione di circolari, comunicazioni, normativa, modulistica e per l'accesso delle famiglie e del personale abilitato al Registro Elettronico;
- canali social istituzionali e informative ufficiali per la condivisione delle iniziative scolastiche e il dialogo con la comunità territoriale.

La scuola si impegna ad assicurare l'efficienza, la continuità e la sicurezza tecnologica di tali servizi, provvedendo al loro costante aggiornamento in un'ottica di miglioramento dell'offerta formativa.

PROTEZIONE DEI DATI PERSONALI (PRIVACY E GDPR)

In conformità al **Regolamento UE 2016/679 (GDPR)** e al **D.Lgs. 196/2003 e s.m.i.** (*Codice in materia di protezione dei dati personali*), all'atto dell'iscrizione o all'inizio dell'anno scolastico viene richiesta ai genitori/tutori legali l'informativa sulla privacy e l'eventualità del consenso espresso (liberatoria) per il trattamento e la pubblicazione di immagini o materiali audiovisivi prodotti per esclusive finalità didattiche e istituzionali. È diritto dei genitori/tutori manifestare il proprio diniego o revocare il consenso in qualsiasi momento.

4. USO DELLA STRUMENTAZIONE PERSONALE

- **Per gli studenti:** Durante l'orario scolastico non è consentito agli alunni l'uso di telefoni cellulari o smartphone personali, in conformità con le direttive ministeriali vigenti. L'impiego di dispositivi elettronici personali è ammesso esclusivamente qualora previsto dalle attività didattiche secondo il modello **BYOD** (*Bring Your Own Device*), regolamentato ed espressamente autorizzato dal docente.
- **Per i docenti:** Durante l'attività di insegnamento e di vigilanza non è consentito l'uso

personale del telefono cellulare. È ammesso l'utilizzo di dispositivi elettronici personali (PC, tablet) per esclusive finalità didattiche, amministrative e funzionali all'insegnamento (es. compilazione del Registro Elettronico), ad integrazione delle dotazioni scolastiche disponibili.

- **Per il personale ATA:** Durante l'orario di servizio, l'uso del telefono cellulare personale è limitato esclusivamente a comunicazioni di riconosciuta e indifferibile urgenza.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI
VALUTAZIONE DEI RISCHI

L'accesso alla Rete costituisce un diritto fondamentale della persona e una condizione per il suo pieno sviluppo individuale e sociale (art. 2, comma 1, *Dichiarazione dei diritti in Internet*). Ciononostante, la scuola ha il dovere di adottare tutte le misure preventive e di sicurezza per garantire agli studenti un ambiente di navigazione protetto, mitigando l'esposizione a possibili fattori di rischio quali:

- accesso accidentale o intenzionale a contenuti illegali, violenti, pornografici o comunque non appropriati all'età;
- utilizzo inadeguato di videogiochi o piattaforme di gioco online;
- carenza di senso critico nella valutazione dell'attendibilità, dell'accuratezza e della pertinenza delle fonti informative in Rete;
- download improprio o riproduzione non autorizzata di materiale coperto da diritto d'autore (*copyright*);
- violazione delle licenze software mediante installazione di programmi non autorizzati;
- **Cyberbullismo:** qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, furto d'identità o alterazione di dati personali effettuata per via telematica a danno di minori. Come il bullismo tradizionale, si configura come una condotta di prevaricazione e oppressione intenzionale e reiterata;
- **Sexting:** l'invio, la ricezione o la condivisione di messaggi, testi, immagini o video digitali a carattere sessualmente esplicito o autoprodotto tramite telefonia mobile, messaggistica istantanea o social network;
- **Grooming (adescamento online):** la tecnica di manipolazione psicologica messa in atto da soggetti adulti per instaurare un rapporto di fiducia e intimità con bambini o adolescenti attraverso la Rete (chat, messaggistica, reti sociali, piattaforme di gaming), al fine di abbatterne le resistenze emotive.

STRATEGIE DI SICUREZZA INFORMATICA E PREVENZIONE

Per garantire la tutela degli utenti e la sicurezza della rete d'Istituto, la scuola adotta le seguenti misure organizzative e tecnologiche:

1. promozione di percorsi di aggiornamento e formazione continua rivolti al personale docente sull'uso consapevole e sicuro delle TIC;
2. coinvolgimento attivo delle famiglie nelle iniziative legate alla sicurezza in Rete (es. Progetto *Generazioni Connesse*);
3. collocazione dei server, degli apparati di rete e delle infrastrutture Wi-Fi in ambienti protetti e ad accesso riservato;
4. manutenzione e verifica periodica dei sistemi informatici a cura degli incaricati dell'assistenza tecnica/amministratori di sistema;

5. divieto assoluto per gli utenti di installare software o modificare le configurazioni di sistema sulle macchine della scuola;
6. divieto di utilizzo della Rete e delle dotazioni dell'Istituto per scopi personali estranei alle attività didattiche e istituzionali;
7. implementazione di sistemi di protezione perimetrale della rete (*firewall*) e applicazione di filtri sui contenuti (*content filtering*) per inibire l'accesso a siti non idonei alle finalità educative;
8. aggiornamento costante dei sistemi di protezione antivirus/antimalware e scansione periodica dei dispositivi;
9. restrizione dell'uso di supporti di memoria rimovibili esterni (es. chiavette USB), ammessi solo previa verifica di sicurezza.

NORME E LINEE GUIDA DI BUONA CONDOTTA (NETIQUETTE)

IL PERSONALE DOCENTE È TENUTO A:

- impiegare le risorse di rete esclusivamente per scopi didattici, formativi e di ricerca professionale;
- esplicitare agli alunni le regole di condotta per la navigazione in Rete, informandoli che la fruizione del servizio può essere oggetto di monitoraggio di sicurezza;
- vigilare costantemente sulle attività online svolte dagli studenti durante le lezioni;
- custodire la strumentazione affidata, segnalando tempestivamente eventuali guasti, anomalie o malfunzionamenti;
- mantenere la massima riservatezza sulle proprie credenziali d'accesso (username e password) e non cederle a terzi;
- effettuare il *logout* dai propri account al termine dell'utilizzo della postazione di classe prima di allontanarsi;
- non memorizzare file contenenti dati personali non necessari o non autorizzati sulle memorie locali dei dispositivi ad uso promiscuo;
- guidare le ricerche online degli studenti fornendo indirizzi di siti o parole chiave preventivamente verificate dal docente sotto il profilo della sicurezza e della tutela della proprietà intellettuale.

GLI ALUNNI SONO TENUTI A:

- utilizzare le apparecchiature tecnologiche dell'Istituto (Monitor Touch, PC, tablet) esclusivamente sotto la guida e la supervisione del docente;
- astenersi dall'usare la strumentazione scolastica per scopi personali, di svago o di gioco non previsti dall'attività didattica;
- non accedere ai social network o a piattaforme esterne, salvo espressa autorizzazione del docente per specifiche attività formative;
- salvare i propri elaborati unicamente nelle cartelle personali o di classe indicate, evitando di ingombrare il desktop o le directory di sistema;
- custodire con riservatezza le proprie credenziali d'accesso e non rivelare dati personali propri o altrui;
- non diffondere o inviare immagini o materiali fotografici personali o dei propri compagni;
- segnalare immediatamente al docente la ricezione o il reperimento casuale di messaggi, immagini o contenuti inappropriati, offensivi o molesti, astenendosi da qualsiasi risposta;
- richiedere l'autorizzazione dell'insegnante prima di effettuare il download di qualsiasi

risorsa dalla Rete;
- rispettare la dignità e la sensibilità altrui, evitando di pubblicare o condividere commenti, contenuti o immagini lesivi della reputazione individuale;
- acquisire consapevolezza sui rischi legati alla permanenza dei dati e delle immagini diffuse in Rete e sulle difficoltà connesse alla loro rimozione dai social media.

Le presenti regole vengono condivise con gli alunni attraverso la redazione di appositi decaloghi e codici di condotta rielaborati in formato accessibile e affissi negli ambienti di apprendimento.

RILEVAZIONE E GESTIONE DEI CASI DI BULLISMO E CYBERBULLISMO

L'intera comunità scolastica è costantemente sensibilizzata sulla prevenzione e sul contrasto del bullismo e del cyberbullismo. Riconoscere tempestivamente i segnali di disagio o le condotte prevaricatorie è essenziale per attivare interventi immediati a tutela dei minori coinvolti e prevenire conseguenze negative sullo sviluppo psicofisico degli studenti.

In conformità con la normativa vigente (**L. 71/2017**, **L. 70/2024** e Linee di Orientamento MIM), qualora si riscontrino o si segnalino episodi di bullismo o cyberbullismo, la procedura di intervento si articola nei seguenti punti:

1. **Segnalazione interna:** Il docente che viene a conoscenza di un presunto caso ne dà immediata comunicazione al Dirigente Scolastico e al Referente d'Istituto per il Cyberbullismo.
2. **Coinvolgimento delle famiglie:** Il Dirigente Scolastico o un suo delegato provvede a convocare tempestivamente i genitori/tutori legali dei minori coinvolti.
3. **Approfondimento dei fatti:** I docenti/referenti conducono colloqui d'ascolto separati e riservati con gli studenti coinvolti (vittima, presunti autori, testimoni) al fine di ricostruire accuratamente la dinamica dei fatti.
4. **Verbalizzazione:** Le informazioni raccolte vengono formalizzate mediante compilazione dell'apposita scheda di rilevazione/incidente predisposta dall'Istituto.
5. **Attivazione della rete territoriale:** Nei casi previsti, e in relazione alla gravità dei fatti, l'Istituto raccorda le proprie azioni con i Servizi Sociali territoriali, la ASL/ATS competente e/o la Sezione Operativa della Polizia Postale.
6. **Comunicazione alle Autorità:** Qualora i fatti configurino fattispecie di reato o rivestano carattere di particolare gravità, il Dirigente Scolastico adempie agli obblighi di legge inoltrando segnalazione alla Procura della Repubblica presso il Tribunale per i Minorenni o alle Autorità di Pubblica Sicurezza.
7. **Intervento educativo e ripristinatorio:** Gli studenti responsabili delle condotte sanzionate sono guidati alla maturazione di una piena consapevolezza della gravità degli atti compiuti. Eventuali sanzioni disciplinari integrano percorsi riparatori e di utilità sociale a carattere formativo ed educativo.
8. **Azioni pedagogiche e di classe:** Il Consiglio di Classe trasforma l'evento in un'occasione di riflessione collettiva, integrando la tematica all'interno della programmazione didattica e delle attività di **Educazione alla Cittadinanza Digitale**.

APPROVAZIONE E REVISIONE DEL DOCUMENTO

La presente Policy è stata adottata ed approvata dagli Organi Collegiali dell'Istituto.

Il documento è soggetto a revisione e aggiornamento periodico (almeno annuale) da parte del Team dell'Innovazione Digitale e del Referente per il Cyberbullismo, in presenza di innovazioni tecnologiche o normative, e sottoposto all'approvazione del Collegio dei Docenti e del Consiglio di Circolo/Istituto.

AGGIORNATO CON DELIBERA N.34 DEL CONSIGLIO DI CIRCOLO DEL 17/09/2026