E-Policy e Regolamento di Istituto per le Tecnologie Digitali e la Sicurezza Online

Delibera n 12 del Consiglio di Istituto del 18/11/2026

Preambolo Istituzionale e Quadro di Riferimento

La presente Policy di Istituto per le Tecnologie Digitali e la Sicurezza Online disciplina le modalità d'uso degli strumenti informatici, della rete telematica e dei dispositivi personali e d'istituto all'interno dell'Istituto d'Istruzione Superiore "E. Fermi". In conformità con le deliberazioni degli Organi Collegiali e integrando i principi stabiliti nel Regolamento d'Istituto per la Valutazione degli Apprendimenti e del Comportamento (approvato con Delibera n. 3 del Collegio dei Docenti del 22/10/2026), il presente regolamento intende promuovere la cultura della responsabilità, della sicurezza in rete e del rispetto formale tra tutte le componenti della comunità scolastica, famiglie ed eventuali soggetti esterni autorizzati ad operare negli spazi dell'Istituto o ad accedere alle sue risorse telematiche.

1. Oggetto, Principi Generali e Finalità Educative

Le Tecnologie dell'Informazione e della Comunicazione (TIC) costituiscono una risorsa essenziale per l'innovazione didattica, l'inclusione e lo sviluppo delle competenze digitali e civiche degli studenti. L'adozione dell'e-Policy risponde all'esigenza istituzionale di strutturare un ambiente educativo protetto, in cui l'accesso alle risorse digitali sia orientato all'apprendimento consapevole e alla prevenzione attiva dei rischi legati all'uso improprio della rete.

1.1 Finalità Strutturali dell'e-Policy

L'e-Policy d'Istituto si prefigge i seguenti obiettivi prioritari:**Promozione dell'uso positivo delle TIC:** Valorizzare le tecnologie digitali nella didattica curricolare ed extracurricolare per potenziare il successo formativo e l'autonomia dello studente.**Prevenzione dei rischi informatici e relazionali:** Strutturare presidi organizzativi per contrastare attivamente fenomeni di cyberbullismo, grooming, sexting e diffusione non consensuale di materiale privato.**Tutela dei dati e della riservatezza:** Garantire la protezione della privacy personale e la corretta gestione dei dati individuali in conformità alle normative vigenti.**Sviluppo della cittadinanza digitale:** Favorire l'interiorizzazione di regole di condotta etiche e formali nella comunicazione elettronica.**2.Quadro Normativo e Documenti d'Istituto**La presente e-Policy è parte integrante del Piano Triennale dell'Offerta Formativa (PTOF), del Regolamento d'Istituto, del Regolamento di Disciplina, del Patto Educativo di Corresponsabilità e del Regolamento per la Valutazione degli Apprendimenti e del Comportamento. Essa si inserisce nel seguente quadro normativo:

- **Tutela dei minori e contrasto al cyberbullismo:** Legge 71/2017, Legge 70/2024 e Linee di orientamento MIM vigenti per la prevenzione e il contrasto del bullismo e del cyberbullismo.
- **Valutazione del comportamento e uso dei dispositivi:** DPR 122/2009, Legge 150/2024 e disposizioni ministeriali sull'uso dei telefoni cellulari a scuola (inclusa la Circolare MIM 2025 sulle scuole secondarie di secondo grado).

- **Protezione dei dati e Intelligenza Artificiale:** Regolamento (UE) 2016/679 (GDPR), D.Lgs. 196/2003 (Codice Privacy) e Regolamento (UE) 2024/1689 (AI Act).
- **Competenze digitali e normativa penale/civile:** Legge 92/2019 (Educazione civica), quadro europeo DigComp 2.2 / DigCompEdu, nonché le disposizioni civili e penali in materia di diritto d'autore, diffamazione, privacy e reati informatici.

3. Ruoli e Responsabilità della Comunità Scolastica

Dirigente Scolastico: Garantisce la sicurezza fisica e digitale della comunità scolastica, nomina le figure di riferimento, promuove la formazione e attiva le procedure di legge e le segnalazioni alle autorità competenti nei casi gravi.

Animatore Digitale e Team per l'Innovazione: Coordinano la diffusione delle buone pratiche digitali, la scelta degli strumenti didattici, la formazione interna e la revisione periodica della e-Policy.

Referente per il Cyberbullismo e Team Antibullismo: Raccolgono e valutano le segnalazioni, attivano protocolli di tutela e supporto per le vittime e percorsi educativi per gli autori, mantenendo i raccordi con famiglie, servizi socio-sanitari e Polizia Postale.

Docenti: Integrano criticamente le TIC nella didattica, vigilano sul rispetto delle regole in classe, educano alla netiquette e alla verifica delle fonti, utilizzano esclusivamente piattaforme autorizzate e segnalano tempestivamente situazioni a rischio.

Personale ATA e Tecnico: Applica le misure di sicurezza dei dati con credenziali personali; il personale tecnico assicura manutenzione, aggiornamento dei sistemi e funzionamento dei filtri di rete.

Studentesse e Studenti: Rispettano la presente e-Policy, utilizzano i dispositivi e gli account esclusivamente per finalità didattiche, tutelano la privacy propria e altrui e segnalano episodi di disagio o prevaricazione online.

Famiglie: Collaborano nell'educazione digitale dei figli secondo il Patto di Corresponsabilità, utilizzano i canali ufficiali per le comunicazioni scuola-famiglia e si astengono dal diffondere online (inclusi gruppi di messaggistica di classe) immagini o dati relativi al contesto scolastico.

4. Curricolo Digitale, Formazione e Sensibilizzazione

L'Istituto inserisce l'educazione alla cittadinanza digitale nell'insegnamento trasversale dell'Educazione Civica in coerenza con il quadro DigComp 2.2 (alfabetizzazione ai dati e contrasto alle fake news, comunicazione e reputazione online, creazione di contenuti e diritto d'autore, sicurezza informatica e benessere digitale, problem solving). Sono previsti interventi mirati nel primo biennio (identità digitale, privacy, social network) e nel triennio (aspetti giuridici, reputazione professionale, uso critico dell'IA), affiancati da iniziative di peer education, corsi di aggiornamento per il personale e incontri informativi per le famiglie.

5. Gestione dell'Infrastruttura di Rete, Dispositivi Scolastici e Account Istituzionali

L'accesso e la fruizione delle risorse tecnologiche di proprietà dell'Istituto sono subordinati al rispetto di precisi vincoli operativi volti a preservare la sicurezza informatica, la continuità didattica e l'integrità dei beni scolastici.

5.1 Regolamentazione della Rete Wi-Fi d'Istituto

La connettività internet fornita dalla scuola è destinata esclusivamente al supporto delle attività formative e gestionali dell'Istituto ed è protetta da firewall
L'accesso alla rete Wi-Fi scolastica è controllato attraverso un monitor centralizzato ed è fatto esplicito divieto a studenti e utenti la visualizzazione e lo scarico di contenuti inappropriati, illegali o potenzialmente pericolosi

5.2 Uso dei Laboratori e dei Dispositivi Scolastici

Le postazioni informatiche fisiche, i computer portatili e i tablet di proprietà della scuola costituiscono beni pubblici assegnati per lo svolgimento delle attività didattiche.

1. **Destinazione d'uso:** Gli studenti devono utilizzare le apparecchiature dei laboratori e le dotazioni mobili esclusivamente per le mansioni e le esercitazioni indicate dai docenti.
2. **Integrità del sistema:** È severamente vietato installare software, applicativi o estensioni non espressamente autorizzati dal personale tecnico o dai docenti responsabili.
3. **Inviolabilità delle configurazioni:** È proibito modificare le impostazioni di sistema, i parametri di rete o le password operative residenti sui dispositivi scolastici.

5.3 Gestione degli Account Istituzionali (@istituto.edu.it)

A ciascuno studente viene assegnato un account personale con dominio istituzionale @istituto.edu.it, destinato all'accesso alle piattaforme per la didattica digitale (come Google Workspace)

L'account istituzionale è riservato a un uso strettamente scolastico. Ciascun titolare è unico e diretto responsabile della custodia e della riservatezza delle proprie credenziali di accesso. L'utilizzo dell'account per finalità estranee alla vita scolastica o la cessione delle credenziali a terzi costituisce una violazione delle norme di sicurezza d'Istituto.

6. Regolamentazione degli Smartphone e Politica BYOD

In conformità alle disposizioni ministeriali vigenti, l'uso dei telefoni cellulari e di analoghi dispositivi elettronici personali è vietato in via generale durante l'intero orario scolastico. L'integrazione didattica secondo il modello BYOD (Bring Your Own Device) è consentita esclusivamente secondo le condizioni operative riportate nella tabella seguente:

Ambito di Regolamentazione	**Disposizione e Requisito Operativo**
Eccezioni didattiche e inclusione	L'uso del dispositivo personale è ammesso solo su espressa richiesta e supervisione del docente per

	specifiche attività pedagogiche, oppure per esigenze documentate sanitarie, di studenti con BES, disabilità (PDP/PEI)
Custodia fuori dall'uso autorizzato	Durante le lezioni, i dispositivi devono rimanere spenti o in modalità silenziosa e riposti all'interno dello zaino (o negli appositi contenitori predisposti dall'Istituto).
Preparazione tecnica e ricarica	Gli studenti sono responsabili di portare il dispositivo carico; è vietato utilizzare le prese elettriche delle aule per ricaricare apparecchi personali. La scuola non risponde di furti, smarrimenti o danni.
Comunicazioni urgenti e verifiche	In caso di urgenze, i contatti tra studenti e famiglie avvengono tramite la segreteria scolastica. Durante verifiche scritte ed esami l'uso non autorizzato comporta l'annullamento della prova e le sanzioni disciplinari previste.

7. Tutela della Privacy, Diritto d'Autore, Proprietà Intellettuale , Netiquette e Intelligenza Artificiale

Il rispetto dei diritti individuali, della riservatezza e dell'onestà intellettuale costituisce un pilastro insostituibile dell'esperienza scolastica all'I.I.S. "E. Fermi".

7.1 Divieto di Registrazione e Diffusione Non Autorizzata

La protezione dell'immagine e della sfera privata di studenti, docenti e personale scolastico è tutelata da norme inderogabili all'interno e all'esterno dell'edificio scolastico.

È severamente vietato scattare fotografie, effettuare registrazioni audio o girare riprese video nei confronti di compagni, docenti o personale ATA all'interno degli spazi scolastici, nelle pertinenze dell'Istituto o durante le uscite didattiche e i viaggi d'istruzione. È altrettanto vietato diffondere tali materiali su social network, applicazioni di messaggistica istantanea, chat di gruppo o piattaforme web senza una formale e preventiva autorizzazione.

7.2 Diritto d'Autore e Prevenzione del Plagio

L'utilizzo delle risorse digitali per la ricerca e l'elaborazione di prodotti scolastici richiede il pieno rispetto delle normative sul diritto d'autore (*copyright*). Gli studenti sono tenuti a citare accuratamente le fonti bibliografiche e telematiche da cui traggono informazioni, dati o immagini, evitando qualsiasi forma di plagio o appropriazione indebita di contenuti altrui.

7.3 Netiquette nelle Comunicazioni Istituzionali

Tutte le interazioni digitali effettuate mediante l'account istituzionale o all'interno di ambienti scolastici (email, forum della classe, piattaforme collaborative) devono conformarsi alle regole della *Netiquette*. Si richiede l'adozione costante di un registro formale, corretto, educato e rispettoso delle opinioni e della dignità di ciascun interlocutore.

7.4 Intelligenza artificiale

L'impiego di sistemi di IA generativa è consentito esclusivamente con finalità didattiche e secondo le indicazioni del docente. Gli studenti hanno l'obbligo di dichiarare l'eventuale ricorso all'IA nella stesura o rielaborazione dei lavori, mantenendo l'originalità del proprio impegno. È vietato inserire nei prompt dati personali, sensibili o riservati propri o di terzi; i docenti esercitano sempre supervisione umana critica senza delegare decisioni valutative a sistemi automatizzati.

8. Protocollo di Prevenzione, Rilevazione e Gestione del Cyberbullismo e dei Rischi Digitali

L'Istituto contrasta in maniera sistemica e rigorosa ogni manifestazione di prevaricazione e disagio online, strutturando un sistema condiviso di segnalazione e presa in carico.

8.1 Assetto Organizzativo: Team per l'Innovazione e Referente per il Cyberbullismo

Per garantire una vigilanza efficace e un pronto intervento, l'Istituto individua al proprio interno:

- **Docente Referente per il Cyberbullismo:** Figura di riferimento a disposizione di studenti, famiglie e personale per la raccolta di segnalazioni relative ad atti di condotta lesiva, molestia o bullismo telematico.
- **Team per l'Innovazione Digitale:** Gruppo di lavoro scolastico incaricato di supportare la pianificazione di interventi educativi e la gestione dei protocolli di sicurezza.

- **Team di Emergenza** : Il Team Emergenza ha il compito di ricevere le segnalazioni di situazioni a rischio bullismo e di intervenire applicando il Protocollo.

8.2 Procedura Operativa di Intervento

La gestione degli eventi critici correlati ai rischi digitali si articola in fasi sequenziali formalmente definite.

1. **Rilevazione e Segnalazione:** Chiunque (studente, genitore, docente o personale ATA) venga a conoscenza di episodi di cyberbullismo, grooming, sexting o diffusione non consensuale di materiale privato aventi quale oggetto o soggetto studenti dell'Istituto è tenuto a darne tempestiva comunicazione al Referente per il Cyberbullismo o al Dirigente Scolastico.
2. **Valutazione e Presa in Carico:** Il Team scolastico preposto esamina la gravità dell'accaduto e predispone i protocolli immediati per la tutela e il supporto della vittima, avviando al contempo contestuali percorsi di rieducazione e responsabilizzazione per l'autore.
3. **Coinvolgimento della Famiglia e di Enti Esterni:** La dirigenza provvede a informare prontamente i genitori degli alunni coinvolti. Qualora gli atti configurino fattispecie di reato grave (reati

informatici, minacce gravi, materiale pedopornografico o episodi di *sextortion*), il Dirigente Scolastico inoltra immediata segnalazione alla Polizia Postale o ai Servizi Sociali competenti.

9. Quadro Sanzionatorio, Misure Riparatrici e Impatto sulla Valutazione del Comportamento

Le violazioni alla presente e-Policy costituiscono infrazioni disciplinari sanzionate secondo criteri di gradualità, proporzionalità e finalità rieducativa, in raccordo con il Regolamento di Disciplina e con la griglia di valutazione del comportamento deliberata dal Collegio dei Docenti ai sensi del DPR 122/2009 e della Legge 150/2024:

L'impostazione sanzionatoria dell'I.I.S. "E. Fermi", coordinata con il Regolamento per la Valutazione degli Apprendimenti e del Comportamento redatto ai sensi del DPR 122/2009 e della Legge 150/2024, persegue una finalità educativa e rieducativa, valorizzando il principio della responsabilità e della riparazione del danno.

9.1 Sanzioni Disciplinari

Le sanzioni applicabili in caso di violazione delle norme sull'uso delle tecnologie digitali e della sicurezza online sono così modulate:

- **Ritiro temporaneo del dispositivo personale:** In caso di utilizzo improprio o non autorizzato del cellulare in classe, il dispositivo viene ritirato dal docente e depositato presso la Presidenza, dove rimarrà in custodia fino alla formale riconsegna ai genitori o agli esercenti la responsabilità genitoriale.
- **Note disciplinari e allontanamento dalla comunità scolastica:** L'emissione di note disciplinari sul registro elettronico e l'adozione di provvedimenti di allontanamento fino a 15 giorni (o superiori a 15 giorni nei casi di eccezionale gravità) sono deliberate in caso di violazioni gravi (es. registrazioni abusive, cyberbullismo, danneggiamento intenzionale di sistemi o violazione degli account).
- **Percorsi educativi e riparatori:** È previsto l'obbligo di svolgere compiti operativi a favore della comunità scolastica e percorsi di sensibilizzazione sull'uso responsabile del web e di riparazione del danno.

9.2 Integrazione con la Griglia di Valutazione del Comportamento (Legge 150/2024 e DPR 122/2009)

In base ai criteri deliberati dal Collegio dei Docenti, la condotta digitale incide direttamente sull'attribuzione del voto di comportamento espresso in decimi in sede di scrutinio.

Voto di Condotta	Descrittori Disciplinari e Comportamentali legati al Digitale e alla Sicurezza
10 / 10	Rispetta in modo esemplare il Regolamento d'Istituto. Osserva scrupolosamente le procedure di sicurezza informatica. Condotta inappuntabile, assenza totale di provvedimenti disciplinari o ricorsi non autorizzati ai dispositivi.
9 / 10	Rispetta il regolamento e le norme di sicurezza. Non ha a carico richiami verbali o

	provvedimenti disciplinari legati all'uso improprio delle tecnologie.
8 / 10	Rispetta il regolamento, ma talvolta incorre in richiami verbali. Osserva le norme di sicurezza con qualche disattenzione non rischiosa. Massimo 1 nota disciplinare collettiva.
7 / 10	Utilizza in modo non adeguato il materiale o le attrezzature scolastiche. Dimentica le indicazioni base di sicurezza. Presenta frequenti richiami e note disciplinari (fino a 2 note) legate anche al mancato rispetto delle regole tecnologiche.
6 / 10	Episodi di inosservanza del regolamento con sanzioni (note disciplinari, sospensione fino a 15 giorni). Violazione di norme di sicurezza con potenziale rischio (senza danno). L'ammissione alla classe successiva è subordinata all'assegnazione e al superamento di uno specifico elaborato critico in materia di cittadinanza attiva e solidale.
5 / 10	Gravi e ripetute violazioni della sicurezza con rischio per sé o per gli altri, atti vandalici a locale o strutture, minacce, cyberbullismo grave o reati informatici con sospensione superiore a 15 giorni. Comporta la non ammissione all'anno successivo o all'Esame di Maturità.

L'applicazione rigorosa di tali criteri garantisce la trasparenza delle procedure e ribadisce la centralità del senso civico e del rispetto reciproco nell'era digitale.