MINISTERO DELL'ISTRUZIONE E DEL MERITO
ISTITUTO COMPRENSIVO STATALE *PRATOLA SERRA*
Scuola dell'Infanzia – Scuola Primaria – Scuola Secondaria di Primo Grado
Via G. Picardo, 37 - 83039 PRATOLA SERRA (AV)
Sedi/plessi Comuni di Pratola Serra, Prata di Principato Ultra e Santa Paolina
Tel. 0825967816 - C.F.80008530646- Codice Meccanografico AVIC857002
E-MAIL avic857002@istruzione.it - PEC avic857002@pec.istruzione.it - SITO WEB www.icpratolaserra.edu.it

ISTITUTO COMPRENSIVO - -PRATOLA SERRA
Prot. 0006380 del 30/06/2025
I-1 (Uscita)

Regolamento di Politica di Uso Accettabile (PUA) delle Tecnologie Digitali e della Rete Internet

Articolo 1 – Finalità e Ambito di Applicazione

Il presente Regolamento ha lo scopo di promuovere un uso corretto, sicuro e responsabile delle tecnologie digitali e della rete Internet nell'Istituto Comprensivo, tenendo conto dell'età delle/gli alunne/i della scuola primaria e secondaria di primo grado. Esso definisce le regole che alunni, personale scolastico e genitori devono rispettare nell'utilizzo degli strumenti informatici e dei servizi online della scuola, al fine di garantire un ambiente educativo sereno, protetto e produttivo.
Ambito di applicazione: le disposizioni si applicano a tutte/i le/gli alunne/i dell'Istituto Comprensivo (dalla scuola primaria alla secondaria di I grado), alle/ai docenti e al personale che utilizza le risorse ICT scolastiche, nonché, per quanto compatibile, ai genitori/tutori nel supportare le/i proprie/i figlie/i. Il regolamento riguarda l'uso di computer, tablet, LIM, dispositivi mobili, rete Internet e piattaforme digitali messi a disposizione dalla scuola, sia in aula che in altri spazi scolastici, oltre all'utilizzo eventualmente autorizzato di dispositivi personali per fini didattici. Vengono inoltre fornite linee guida per l'uso della rete scolastica anche durante attività a distanza o extrascolastiche organizzate dall'Istituto.

Articolo 2 – Principi Generali e Comportamenti Attesi

L'Istituto Comprensivo incentiva l'utilizzo delle TIC come strumento per arricchire la didattica e le competenze digitali fin dalla giovane età, nel rispetto di valori educativi e della sicurezza delle/dei minori. A tal fine, tutti gli utenti sono tenuti ad adottare comportamenti improntati a legalità, buon senso e rispetto reciproco, in linea con i seguenti principi generali:

- Uso educativo e appropriato: le tecnologie digitali e Internet devono essere utilizzate esclusivamente a scopi didattici o di approfondimento culturale, sotto la guida delle/i docenti. Alle/gli alunne/i è richiesto di seguire le indicazioni degli insegnanti e di non usare i dispositivi per scopi estranei alle attività scolastiche.
- Sicurezza e benessere: la scuola assume un ruolo di tutela dei minori online. Verranno adottate misure preventive (filtri, controllo dei contenuti) per evitare che le/gli alunne/i accedano a materiali inappropriati o pericolosi. Le/gli alunne/alunni devono collaborare attivamente a mantenere un ambiente digitale sicuro, segnalando subito alle/i docenti eventuali contenuti o comportamenti online che li mettano a disagio.
- Responsabilità condivisa: l'educazione digitale è un percorso condiviso tra scuola e famiglia. I genitori/tutori sono incoraggiati a partecipare attivamente, monitorando l'uso della tecnologia da parte delle/i figlie/i a casa, dialogando con loro sulle esperienze online e rispettando a loro volta le regole di questo regolamento quando interagiscono con gli strumenti scolastici (es. registro elettronico, piattaforme didattiche).
- Rispetto e correttezza: nel contesto digitale valgono le stesse regole di convivenza civile presenti nella vita scolastica offline. Si richiede rispetto verso persone e dati altrui, linguaggio appropriato nelle comunicazioni online, e osservanza delle norme di "netiquette" (comportamento educato in rete). Ogni forma di cyberbullismo, offesa, discriminazione o violazione della dignità di altri utenti è severamente vietata e contraria ai valori della comunità scolastica.
- Uso consapevole e formativo: alle/gli alunne/i, in base alla loro età, viene insegnato ad essere cittadine/i digitali consapevoli, imparando gradualmente a utilizzare Internet e le tecnologie in modo critico e sicuro. Ciò include comprendere che l'accesso alle risorse informatiche della scuola è un privilegio legato a responsabilità: un uso mirato e responsabile aiuta a garantire le migliori opportunità di apprendimento per tutti.

Articolo 3 – Norme Specifiche sull'Utilizzo delle TIC

Nel quotidiano utilizzo di computer, dispositivi e Internet a scuola, tutti gli utenti dovranno attenersi alle seguenti regole specifiche:

- Supervisione e autorizzazione: Le/gli alunne/i possono accedere a Internet solo sotto la supervisione di una/un docente. In particolare, nella scuola primaria e nei primi anni della secondaria di I grado, l'uso di qualsiasi dispositivo o applicazione online deve avvenire alla presenza o con il permesso dell'insegnante. I siti web, i video e i software verranno selezionati dalla/dal docente o previamente approvati dalla/o stessa/o, in modo da essere adeguati all'età e agli obiettivi educativi.
- Navigazione sicura: È vietato alle/gli alunne/alunni cercare intenzionalmente o accedere a contenuti inappropriati, osceni, violenti, offensivi o illegali. I sistemi informatici della scuola sono dotati di filtri per limitare l'accesso a siti non adatti; è altresì vietato tentare di aggirare tali filtri o misure di sicurezza (ad esempio mediante proxy o VPN non autorizzati).
- Credenziali e account: Qualora vengano forniti alle/gli alunne/alunni account personali (ad es. account per piattaforme didattiche, email scolastica), questi devono essere utilizzati solo dal titolare e non vanno condivisi con

nessuno. Ogni studentessa/studente è responsabile dell'attività svolta tramite le proprie credenziali; perciò, deve custodirle con cura, usare password robuste e non consentire accessi non autorizzati.

- Divieto di installazione e modifiche: le/gli alunne/alunni non devono installare software, app o modificare le configurazioni dei dispositivi scolastici. Qualsiasi necessità di installare programmi didattici verrà valutata e gestita dal personale tecnico o docente autorizzato. È anche vietato collegare alla rete o ai computer della scuola dispositivi esterni (chiavette USB, hard disk, etc.) senza preventiva autorizzazione, per evitare virus o intrusioni.
- Uso appropriato delle risorse: le risorse informatiche comuni (laboratori, tablet condivisi, LIM) vanno utilizzate con cura e rispetto dei beni comuni. È severamente proibito danneggiare, scollegare cavi, manomettere attrezzature o alterare il funzionamento di dispositivi e rete. Le/gli alunne/alunni sono tenuti a segnalare immediatamente alle/i docenti eventuali guasti o malfunzionamenti riscontrati, senza tentare riparazioni autonome.
- Comunicazioni online interne: nell'utilizzare strumenti come email scolastiche, chat didattiche o forum interni, le/gli alunne/i devono mantenere un tono educato e rispettoso. Messaggi offensivi, linguaggio volgare, diffusione di pettegolezzi o contenuti che possano ledere qualcuno non saranno tollerati. La comunicazione deve riguardare temi scolastici; è vietato usare i canali scolastici per spam, catene di Sant'Antonio, pubblicità o attività personali non pertinenti.
- Privacy e dati personali: non è consentito rivelare online informazioni personali proprie o di altri (come indirizzo, numero di telefono, password, foto private) su siti pubblici o chat non controllate dalla scuola. Le/gli alunne/alunni devono comprendere l'importanza di proteggere la propria privacy: ad esempio, non dovrebbero mai condividere il proprio nome completo o altre informazioni identificative su forum pubblici senza supervisione. Inoltre, è fatto divieto di scattare foto o registrare video/audio a scuola senza permesso (vedi anche Art. 8 sul tema social media e privacy).
- Rispetto della legalità: l'uso delle tecnologie deve avvenire nel rispetto delle leggi in vigore. In particolare, è vietato utilizzare i dispositivi della scuola per attività illegali (ad es. scaricare materiale pirata o coperto da copyright senza autorizzazione, accedere a sistemi informatici protetti, commettere frodi, plagiare contenuti altrui spacciandoli per propri nelle attività scolastiche, ecc.). Alle/gli alunne/i è richiesto di rispettare le normative sul diritto d'autore: non si possono copiare testi o risorse digitali senza citare le fonti, e non si devono installare o usare software non regolarmente concessi dalla scuola.

Le/gli alunne/i più giovani, compatibilmente con la loro età, verranno guidati in modo graduale a comprendere queste norme. Le/i docenti della scuola primaria dedicheranno del tempo a spiegare con esempi concreti cosa è consentito e cosa no, affinché anche le/i bambine/i interiorizzino le regole base (come chiedere sempre prima di navigare, non toccare dispositivi senza permesso, fermarsi se incontrano qualcosa di strano online, ecc.). Nella scuola secondaria di primo grado, via via che cresce l'alfabetizzazione digitale, alle/gli alunne/alunni è richiesto di mostrare maggiore autonomia responsabile, pur restando la supervisione del personale un elemento fondamentale.

Articolo 4 – Trattamento dei Dati Personali e Tutela della Privacy

Nel trattamento dei dati personali di alunne/alunni, famiglie e personale, l'Istituto opera nel pieno rispetto della normativa vigente in materia di privacy, in particolare del Regolamento (UE) 2016/679 (GDPR), del D.Lgs. 30 giugno 2003 n.196 ("Codice in materia di protezione dei dati personali", come modificato dal D.Lgs. 101/2018). I dati personali raccolti e trattati attraverso i sistemi informatici scolastici (es. registri elettronici, piattaforme educative, elenchi di utenti, fotografie o video didattici) saranno utilizzati esclusivamente per finalità istituzionali e didattiche, connesse al percorso educativo delle/gli alunne/alunni.

Modalità e tutele: Il trattamento dei dati avverrà secondo principi di correttezza, liceità, trasparenza e tutela della riservatezza. La scuola adotta misure tecniche e organizzative adeguate a proteggere i dati da accessi non autorizzati, divulgazione indebita, alterazione o perdita (ad esempio: sistemi di autenticazione per l'accesso alle piattaforme, backup periodici, antivirus e firewall aggiornati). L'accesso ai dati è consentito solo a personale autorizzato e per scopi legittimi legati all'attività scolastica.

Consenso e informativa: Per le/gli alunne/i minorenni, eventuali servizi digitali che richiedano consenso al trattamento dei dati personali (ad es. iscrizione a specifiche piattaforme online extrascolastiche) saranno attivati previa acquisizione del consenso dei genitori o tutori, come previsto dalla normativa. All'inizio di ogni anno scolastico, i genitori riceveranno l'informativa sul trattamento dei dati personali (ai sensi degli artt. 13-14 GDPR) da parte dell'Istituto, che dettaglia le tipologie di dati trattati, le finalità, i diritti degli interessati e i riferimenti del Responsabile Protezione Dati (RPD/DPO) dell'Istituto. I genitori sono tenuti a leggere tale informativa e a restituire il modulo di presa visione/firma per consenso quando necessario.

Uso di immagini e contenuti multimediali: Particolare attenzione è dedicata all'utilizzo di foto, video o altri materiali multimediali riguardanti le/gli alunne/alunni:

- La pubblicazione di immagini o video di minori riconoscibili, sul sito web della scuola o su canali ufficiali, avverrà solo con il consenso scritto dei genitori delle/gli alunne/i interessati. In assenza di tale liberatoria, non saranno diffuse immagini identificative del minore.
- Le/gli alunne/alunni e i loro familiari, dal canto loro, non devono pubblicare su spazi online pubblici foto o video che ritraggono compagni di classe, insegnanti o altri membri della comunità scolastica durante attività scolastiche, senza aver ottenuto il permesso delle persone coinvolte (e dei genitori, se si tratta di minorenni). Questo per tutelare la privacy e la sicurezza di tutti.

Diritti degli interessati: in qualsiasi momento, genitori/tutori (o le/gli alunne/alunni maggiori di 14 anni, in relazione ai servizi della società dell'informazione) possono esercitare i diritti previsti dal GDPR (accesso, rettifica, cancellazione, limitazione del trattamento, opposizione, portabilità dei dati ove applicabile) rivolgendosi al Titolare del trattamento (Dirigente Scolastica) o al Responsabile della protezione dei dati.

Articolo 5 – Sicurezza Informatica e Responsabilità degli Utenti

La sicurezza informatica è fondamentale per proteggere sia i dati che il regolare svolgimento delle attività didattiche. Tutti gli utenti sono pertanto tenuti a contribuire attivamente a mantenere sicura la rete e le attrezzature scolastiche, osservando le seguenti disposizioni:

- Credenziali sicure: come già indicato, ogni utente ha proprie credenziali di accesso alle piattaforme digitali scolastiche. Queste vanno conservate in modo sicuro. Non scrivere le password in chiaro su quaderni accessibili ad altri, non comunicarle a compagne/i o colleghe/i, e modificarle immediatamente in caso di sospetto che qualcun altro le conosca. Le password devono rispettare eventuali criteri di complessità indicati dall'Istituto (lunghezza minima, uso di numeri/simboli, ecc.).
- Blocco dei dispositivi e protezione fisica: Quando si termina di usare un computer condiviso o un tablet della scuola, occorre effettuare il logout dall'account e chiudere la sessione, in modo che il prossimo utente non possa accedere a dati altrui. Le/i docenti vigileranno affinché le/gli alunne/i più piccoli ricordino di disconnettersi correttamente. Inoltre, non lasciare incustoditi dispositivi scolastici in luoghi accessibili senza controllo; dopo l'uso, riporli secondo le indicazioni (es. riconsegnare il tablet alla/al docente, chiudere a chiave il laboratorio informatico se non utilizzato, ecc.).
- Uso della rete e divieto di intrusioni: è proibito effettuare attività che possano compromettere la sicurezza della rete scolastica o di altri sistemi. In particolare, è vietato tentare di accedere a risorse informatiche senza autorizzazione (ad es. entrare in account di altri, esplorare cartelle di sistema protette, violare reti Wi-Fi interne), così come è vietato provare a introdurre virus, malware o usare strumenti di hacking di qualsiasi tipo. Gli utenti che, anche accidentalmente, si imbattano in una vulnerabilità del sistema sono tenuti a segnalarlo immediatamente al personale tecnico o alla Dirigente e non devono sfruttarla in alcun modo.
- Aggiornamenti e antivirus: i dispositivi scolastici verranno mantenuti aggiornati e dotati di software di sicurezza (antivirus, anti-malware) dall'Istituto. Gli utenti non devono disabilitare né interferire con questi strumenti di protezione. Nel caso di dispositivi personali autorizzati all'uso (BYOD, vedi Art. 7), le/gli alunne/alunni dovranno assicurarsi che tali dispositivi abbiano antivirus aggiornato e che il sistema operativo sia protetto da password o PIN, per ridurre rischi alla rete scolastica.
- Responsabilità individuale: ogni utente è responsabile delle azioni che compie utilizzando le risorse informatiche della scuola. Le attività effettuate sulla rete scolastica potrebbero essere tracciate e registrate (log di accesso, cronologia di navigazione sui dispositivi istituzionali) in conformità con le normative vigenti e al solo fine di sicurezza/prevenzione. Tali log potranno essere consultati dall'amministratore di sistema o dalla Dirigente *in caso di violazioni sospette* e, se necessario, condivisi con le Autorità competenti per accertare comportamenti illeciti. La scuola garantisce comunque che il monitoraggio avviene nel rispetto della privacy e solo per motivi giustificati di sicurezza.

Il personale scolastico (docenti e ATA) ha il dovere di vigilare sull'uso delle tecnologie da parte delle/gli alunne/i, e contestualmente deve anch'esso attenersi a regole di sicurezza: ad esempio, le/i docenti non lasceranno i registri elettronici aperti su schermo alla portata delle/gli alunne/alunni, non utilizzeranno software non autorizzati sui PC della scuola e contribuiranno a diffondere la cultura della sicurezza digitale tra le/gli alunne/i.

Articolo 6 – Didattica Digitale e Utilizzo delle Piattaforme Online

L'Istituto Comprensivo mette a disposizione piattaforme digitali e servizi online per supportare la didattica (ad es. registro elettronico, ambienti per la didattica digitale integrata, applicativi per esercizi interattivi, aule virtuali o strumenti di condivisione materiali). L'uso di tali piattaforme è regolato come segue:

- Accesso alle piattaforme: ad ogni studentessa/studente (soprattutto nella scuola secondaria di I grado, e talvolta nelle ultime classi della primaria) potrà essere assegnato un account sulle piattaforme didattiche utilizzate dalla scuola. L'accesso avviene con credenziali fornite dall'Istituto. Come già previsto, tali credenziali sono personali. I genitori delle/i bambine/i più piccoli potranno affiancarli nell'accesso e nel monitoraggio delle attività online, soprattutto per quanto riguarda la scuola primaria, dove spesso l'utilizzo delle piattaforme avviene insieme all'adulto.
- Comportamento nelle aule virtuali: qualora si utilizzino strumenti di classe virtuale, videoconferenza (es. per didattica a distanza o progetti online) o forum, alle/gli alunne/alunni è richiesto di mantenere lo stesso comportamento rispettoso e disciplinato che terrebbero in una classe fisica. Ciò implica: partecipare con attenzione, non disturbare le sessioni con interventi inopportuni, non aprire microfono o webcam se non richiesto, utilizzare chat o forum per scopi attinenti alla lezione. Durante eventuali videolezioni, l'alunna/o deve presentarsi in modo decoroso (abbigliamento adeguato) e con un nickname identificabile (nome e cognome reali), evitando sfondi o immagini del profilo non appropriati.
- Uso del registro elettronico e compiti online: genitori e alunne/i devono consultare regolarmente il registro elettronico per tenersi aggiornati su compiti, comunicazioni e voti. Le giustificazioni di assenze o le comunicazioni scuola-famiglia via registro devono essere effettuate in modo veritiero e tempestivo. Nel caso di consegna di compiti in formato digitale tramite piattaforme (es. caricamento di elaborati, questionari online), alle/gli alunne/alunni è richiesto di svolgere in autonomia il proprio lavoro, rispettando le scadenze e le indicazioni delle/i docenti, e di non violare le regole (ad esempio evitando di farsi inviare soluzioni via chat durante un compito online, che costituirebbe una forma di plagio/copia non consentita).
- Rispetto della privacy e divieto di registrazione: Né alunne/alunni né docenti devono condividere all'esterno contenuti riservati delle piattaforme. Ad esempio, è vietato fare screenshot non autorizzati di conversazioni su piattaforme didattiche o registrare senza permesso le videolezioni o audio delle lezioni online. I materiali (slide, video, dispense) forniti dalle/gli insegnanti sulle piattaforme sono da intendersi per uso esclusivamente interno e didattico: le/gli alunne/alunni non possono redistribuirli o pubblicarli altrove senza autorizzazione, soprattutto se contengono informazioni personali (nomi di alunne/alunni, immagini di attività di classe, ecc.).

- Supporto tecnico e segnalazioni: In caso di difficoltà tecniche nell'uso delle piattaforme (password smarrita, problemi di accesso, bug del sistema), la/o studentessa/studente o la famiglia è tenuto a informare la/il docente referente o il personale tecnico incaricato, evitando di risolvere autonomamente con metodi non ufficiali. La scuola garantirà supporto per un corretto utilizzo degli strumenti digitali, anche attraverso guide o momenti formativi rivolti sia alle/gli alunne/i che ai genitori, specialmente all'inizio di nuove iniziative di didattica digitale.

Nota per le famiglie: È importante che le famiglie dei più piccoli partecipino attivamente alla familiarizzazione con gli strumenti digitali scolastici. Ad esempio, per le piattaforme usate nella scuola primaria, si invita il genitore a sedersi con la/ila bambina/o durante le prime volte di utilizzo a casa, spiegando in modo semplice le regole (ad es. "scrivi solo cose gentili", "chiedi alla maestra se non sai cosa fare sul computer"). Questo rafforza l'efficacia educativa della piattaforma e crea continuità tra l'uso della tecnologia a scuola e a casa.

Articolo 7 – Sezione sul BYOD (Bring Your Own Device)

Bring Your Own Device (Porta il tuo dispositivo) si riferisce alla possibilità per le/gli alunne/alunni di utilizzare dispositivi digitali personali (tablet, notebook o, in casi specifici, smartphone) a scuola per finalità didattiche. Data la giovane età delle/gli alunne/i dell'Istituto Comprensivo, l'approccio al BYOD sarà graduale e attentamente controllato:

- Scuola Primaria: di norma, non è consentito alle/gli alunne/i della primaria portare dispositivi personali a scuola. L'attività didattica in questa fascia d'età si svolge con strumenti forniti dalla scuola (tablet condivisi, computer del laboratorio, etc.) o in presenza dell'insegnante. Eventuali progetti speciali che prevedano l'uso di un dispositivo personale (ad esempio un progetto di coding con tablet in quinta primaria) dovranno essere espressamente autorizzati dal Consiglio di Classe e comunicati ai genitori, i quali dovranno dare il loro assenso e collaborare perché il dispositivo sia utilizzato secondo le indicazioni date.
- Scuola Secondaria di I grado: per le/gli alunne/alunni delle medie, l'Istituto può consentire il BYOD in forme controllate. In particolare, solo su esplicita indicazione della/del docente e per specifiche attività didattiche (come ricerche online in classe, utilizzo di applicazioni educative, laboratori digitali), le/gli alunne/alunni potranno essere invitati a utilizzare un proprio dispositivo (ad esempio un tablet o un computer portatile; l'uso del cellulare sarà invece limitato, si veda oltre). In ogni caso, l'impiego di dispositivi personali richiede l'autorizzazione preventiva dei genitori interessati, i quali devono essere informati sull'attività e sulle regole d'uso.

Quando il BYOD è autorizzato, si applicano le seguenti regole generali:

- Uso limitato al contesto didattico: il dispositivo personale può essere utilizzato esclusivamente durante le ore di lezione e solo per lo scopo indicato dall'insegnante. Al di fuori di tale contesto (ad esempio intervallo, spostamenti, prima e dopo le lezioni), i dispositivi personali devono rimanere spenti o comunque non utilizzati dalle/gli alunne/alunni. Rimane in vigore il divieto generale di utilizzo non autorizzato dei telefoni cellulari in orario scolastico, in linea con le disposizioni ministeriali: il cellulare non deve distrarre né l'alunna/o né le/i compagne/i, e può essere accesso solo se richiesto per un esercizio didattico specifico.
- Connessione alla rete scolastica: se è necessario accedere a Internet, la/o studentessa/studente dovrà collegare il proprio dispositivo esclusivamente alla rete Wi-Fi scolastica (se disponibile e fornita per le/gli alunne/alunni) che ha filtri di sicurezza, e non usare reti dati proprie che eludano i controlli. L'accesso alla Wi-Fi scolastica con dispositivi esterni potrà richiedere credenziali temporanee o una registrazione del dispositivo secondo le procedure tecniche dell'Istituto.
- Divieto di contenuti non consentiti: sul dispositivo personale, durante l'attività scolastica, non devono essere presenti o utilizzati contenuti o applicazioni non adatti o estranei all'argomento (giochi, social network, messaggistica privata, etc.). La/o studentessa/studente è tenuto a chiudere o rimuovere eventuali applicazioni non pertinenti prima dell'uso a scuola. La/il docente e/o i referenti tecnici potranno richiedere in qualsiasi momento di visionare lo schermo del dispositivo per verificare che si stia seguendo l'attività assegnata.
- Responsabilità e cura del dispositivo: la/o studentessa/studente e la sua famiglia sono responsabili del proprio dispositivo portato a scuola. La scuola mette in atto misure di sorveglianza di base durante le attività (ad esempio la/il docente presente vigila), ma non risponde di furti, smarrimenti o danni eventualmente subiti dal dispositivo personale in ambiente scolastico. Si consiglia pertanto di contrassegnare chiaramente il dispositivo, tenerlo sempre sotto controllo e, se non utilizzato, tenerlo spento nello zaino.
- Rispetto della privacy altrui: anche usando dispositivi propri, valgono le regole generali: è vietato registrare audio, foto o video di compagni, insegnanti o altre persone durante l'orario scolastico senza autorizzazione. Un dispositivo personale non autorizza comportamenti difformi: se uno studente viola la privacy altrui con il suo telefono o tablet (ad esempio filmando di nascosto un compagno o accedendo a dati riservati), sarà soggetto alle medesime sanzioni disciplinari come se avesse usato un dispositivo della scuola.
- Configurazione di sicurezza: al momento dell'adesione a un progetto BYOD, potranno essere fornite indicazioni tecniche ai genitori su come preparare il dispositivo (es.: installare un antivirus aggiornato, assicurarsi che l'account utilizzato sul tablet non abbia accesso illimitato a store di app non controllate, etc.). Lo scopo è garantire un ambiente sicuro sia per la/o studentessa/studente che per la rete scolastica. Il mancato rispetto di tali requisiti di sicurezza potrà comportare l'esclusione temporanea del dispositivo dall'attività (fino a messa in regola).
- L'Istituto si riserva la facoltà di interrompere o limitare il progetto BYOD in qualsiasi momento se si riscontrano utilizzi impropri diffusi o rischi per la sicurezza, comunicando tale decisione alle famiglie. In ogni caso, l'introduzione del BYOD sarà accompagnata da momenti formativi per docenti e genitori, affinché tutti comprendano finalità e limiti di tale pratica.

Articolo 8 – Regole sull'Uso dei Social Media in Ambito Scolastico

L'uso dei social network e dei media digitali di comunicazione pone sfide particolari in ambito scolastico, specie considerando che le/gli alunne/i dell'Istituto Comprensivo sono in gran parte minori di 14 anni (età generalmente sotto il limite di iscrizione autonoma ai principali social network). Di conseguenza:

- Divieto di accesso ai social durante la scuola: alle/gli alunne/alunni non è permesso accedere ai propri profili social(Facebook, Instagram, TikTok, WhatsApp, YouTube con account personale, ecc.) durante l'orario scolastico o tramite i dispositivi della scuola, a meno che ciò non faccia parte di un'attività didattica autorizzata dal docente. I siti o le app di social media saranno bloccati dai filtri della rete d'Istituto. Se uno studente dovesse comunque accedervi (ad esempio usando la propria connessione dati di nascosto), verrebbe considerata una violazione del presente Regolamento.
- Uso didattico e progetti digitali: nel caso in cui la scuola decida di utilizzare strumenti di condivisione che hanno caratteristiche di social media per progetti educativi (ad esempio un blog di classe, un gruppo chiuso supervisionato su una piattaforma dedicata all'istruzione, caricamento di video didattici su YouTube con canale scolastico privato), tali attività saranno strettamente mediate dalle/i docenti. I contenuti pubblicati dalle/gli alunne/i in questi contesti saranno vagliati dall'insegnante prima della pubblicazione. Inoltre, verranno adottati accorgimenti per la tutela dell'identità: ad esempio, si potrebbe usare solo il nome di battesimo delle/gli alunne/i o un nickname nei contenuti esterni, e non saranno pubblicati volti o dati identificativi senza consenso dei genitori (come già specificato nell'Art. 4).
- Comportamento delle/gli alunne/alunni sui social (anche extra-scuola): Anche se l'uso privato dei social media avviene fuori dall'ambiente scolastico, la scuola richiama alunni e famiglie a un senso di responsabilità: qualunque comportamento gravemente offensivo, molesto o lesivo dell'immagine altrui tenuto *online* dalla/o studentessa/studente, se riguarda membri della comunità scolastica o episodi di vita scolastica, potrà attivare interventi educativi o disciplinari da parte della scuola. In particolare, bullismo e cyberbullismo commessi attraverso i social o le chat (ad es. creare gruppi per deridere un compagno, diffondere foto imbarazzanti di un coetaneo, insultare un docente sui social) sono *condotte gravissime*: l'Istituto, venutone a conoscenza, attiverà le procedure previste dalla Legge 71/2017 per il contrasto al cyberbullismo, informando tempestivamente le famiglie coinvolte e, se necessario, le autorità competenti. Le/gli alunne/i sono educati a capire che le regole di rispetto valgono anche nel mondo virtuale: prima di postare o condividere qualcosa su qualcuno, occorre riflettere sulle conseguenze.
- Uso dei social da parte del personale: le/i docenti e il personale scolastico dovrebbero astenersi dall'utilizzare i social media per comunicare individualmente con le/gli alunne/i al di fuori degli strumenti ufficiali (registro elettronico, piattaforma istituzionale). Eventuali gruppi classe gestiti dai genitori su applicazioni di messaggistica (es. gruppo WhatsApp dei genitori rappresentanti) non sono sotto la responsabilità diretta della scuola; tuttavia, si invitano i genitori a usare tali mezzi in modo costruttivo e nel rispetto di tutti, evitando di diffondere informazioni non verificate o dati sensibili relativi ad altri minori.
- Immagine dell'Istituto online: alle/gli alunne/alunni e alle famiglie è richiesto di non pubblicare contenuti sui social che possano ledere il decoro e l'immagine della comunità scolastica. Critiche o segnalazioni riguardanti la scuola dovrebbero preferibilmente essere affrontate tramite i canali ufficiali di dialogo scuola-famiglia, anziché esposte sui social in modo inappropriato. Allo stesso modo, non è consentito utilizzare senza permesso il nome, il logo o altri simboli identificativi dell'Istituto per creare pagine, profili o gruppi sui social. L'Istituto ha canali ufficiali gestiti dalla dirigenza per finalità informative e progettuali, e ogni altra presenza online che sembri riferibile alla scuola ma creata da terzi potrà essere segnalata per gli opportuni provvedimenti.

In sintesi, la regola d'oro è che il rispetto della persona e delle norme vale anche su Internet: la comunità scolastica si impegna a formare alunni che siano utenti consapevoli e responsabili, capaci di utilizzare i social media in modo positivo, ma allo stesso tempo tutela i minori dagli aspetti pericolosi o nocivi di tali strumenti.

Articolo 9 – Sanzioni Disciplinari (alunne/alunni) e Responsabilità del Personale Scolastico

Per le/gli alunne/alunni: la violazione delle norme stabilite nel presente Regolamento comporterà provvedimenti disciplinari proporzionati alla gravità e alla reiterazione dell'infrazione, in coerenza con il Regolamento di Istituto e lo Statuto delle Alunne e delle/gli alunne/alunni. A titolo di esempio:

- *Infrazioni lievi* (es. uso occasionale del dispositivo per scopi non autorizzati, lieve negligenza nel seguire le istruzioni del docente online): potranno determinare un richiamo verbale immediato da parte della/del docente e l'eventuale temporanea sospensione dall'uso dello strumento digitale (es. la/il docente può far spegnere il dispositivo o far allontanare la/o studentessa/studente dal computer per il resto dell'ora). La/il docente informerà comunque l'alunna/o sul motivo del richiamo, in ottica educativa.
- *Infrazioni di media gravità* (es. reiterato utilizzo scorretto del dispositivo nonostante i richiami, accesso a contenuti non consoni, linguaggio inappropriato in chat di classe, condivisione di piccole quantità di materiale non autorizzato): possono portare a una nota disciplinare sul registro di classe e alla comunicazione dell'episodio ai genitori. In aggiunta, potrà essere revocato per un periodo definito il privilegio di utilizzare gli strumenti informatici della scuola (ad esempio divieto di accedere al laboratorio o alla piattaforma per un certo numero di giorni), salvo necessità didattiche, e/o assegnati compiti educativi (come riflettere per iscritto sull'uso responsabile della tecnologia).
- *Infrazioni gravi* (es. cyberbullismo verso compagni o personale, diffusione intenzionale di materiale offensivo o privato, danneggiamento di apparecchiature, accesso fraudolento a dati riservati, uso del dispositivo per copiare durante verifiche, violazioni di legge quali installazione di materiale pirata, ecc.): comporteranno l'intervento della Dirigenza scolastica. Le sanzioni possibili, in base al regolamento disciplinare, includono il richiamo scritto ufficiale (nota sul registro ufficiale o lettera alla famiglia), la sospensione dalle lezioni (anche con eventuale esclusione dallo scrutinio o non ammissione a gite, se previsto dal Regolamento d'Istituto, a seconda della

gravità) e la revoca dell'accesso alle risorse digitali della scuola per un periodo prolungato. Nel caso di atti configurabili come reati (ad esempio accessi abusivi a sistemi informatici, diffamazione online grave, pornografia minorile, minacce via web), la scuola, oltre a applicare sanzioni interne, coinvolgerà le Forze dell'Ordine per gli accertamenti del caso, secondo quanto previsto dalla legge.

- In tutti i casi di infrazioni disciplinari, alla/o studentessa/studente è sempre garantito il diritto di difesa e di spiegare le proprie ragioni. Le sanzioni, specialmente quelle più gravi, saranno irrogate seguendo le procedure formali (contestazione, eventuale istruttoria da parte di un organo disciplinare, comunicazione scritta ai genitori, possibilità di conversione in attività riparative se previsto dallo Statuto Alunni/Alunne). L'obiettivo infatti è principalmente educativo: far comprendere l'errore e prevenirne il ripetersi, più che punitivo fine a sé stesso. A tal fine, potranno essere previste attività di recupero, come brevi corsi sulla cittadinanza digitale o colloqui di riflessione con lo psicologo scolastico (se presente), per aiutare la/o studentessa/studente a migliorare il proprio comportamento online.

Si sottolinea inoltre che la famiglia è civilmente responsabile dei danni cagionati dai figli minori a persone o cose (art. 2048 C.C.). Pertanto, in caso di danni materiali intenzionali alle attrezzature informatiche o alle infrastrutture di rete della scuola, sarà richiesto ai genitori il risarcimento dei costi di riparazione o sostituzione, ferme restando le sanzioni educative verso la/o studentessa/studente autore dell'atto.

Per il personale scolastico: docenti e personale ATA hanno l'obbligo professionale di attenersi a questo Regolamento e di farlo rispettare alle/gli alunne/alunni. Un mancato adempimento grave da parte del personale (ad esempio: utilizzo indebito di dati personali delle/gli alunne/i, negligenza ripetuta nella sorveglianza che conduca a incidenti online, uso di strumenti scolastici per fini privati non consentiti durante l'orario di lavoro, violazione della privacy o della sicurezza informatica dell'Istituto) può configurare un illecito disciplinare. In tal caso, verranno attivate le procedure previste dal contratto collettivo di lavoro e dal D.Lgs. 165/2001 (Testo Unico del Pubblico Impiego) per il personale della scuola: la Dirigente potrà emettere rilievi scritti, richiami formali o segnalazioni all'Ufficio competente per i procedimenti disciplinari, a seconda della gravità. Anche per il personale, condotte di particolare gravità sul piano penale (es. accesso abusivo a sistemi, divulgazione di dati riservati, adescamento di minori online, etc.) saranno oggetto di denuncia alle Autorità.

In generale, però, l'Istituto intende puntare sulla formazione e la prevenzione: verranno organizzati momenti di aggiornamento per il personale sulle tematiche della sicurezza digitale, della privacy e dell'uso consapevole delle TIC, affinché le/i docenti siano preparati ad educare e guidare le/gli alunne/alunni dando essi stessi il buon esempio. La collaborazione tra tutte le componenti (alunni, docenti, ATA, genitori) è fondamentale per creare un clima di fiducia e responsabilità condivisa nell'uso della tecnologia.

Articolo 10 – Approvazione, Diffusione e Aggiornamento del Regolamento

Il presente Regolamento di Politica di Uso Accettabile (PUA) è stato elaborato tenendo conto delle linee guida ministeriali e della normativa vigente. Esso è approvato dal Consiglio di Istituto, ai sensi dell'art. 10 comma 3 lettera a) del D.P.R. 275/1999 (potere deliberante in materia di regolamenti interni), in data 27/06/2025 con delibera n.48. Prima dell'approvazione finale, il documento è stato condiviso con il Collegio dei docenti per un parere pedagogico, al fine di assicurare che le disposizioni siano chiare e adeguatamente calibrate sull'età delle/gli alunne/i.

Pubblicazione e presa visione: Dopo l'approvazione, il Regolamento PUA è pubblicato sul sito web istituzionale e sul Registro Elettronico di Istituto, in area accessibile alle famiglie, affinché tutti possano prenderne visione. All'inizio di ogni anno scolastico, o al momento dell'iscrizione di nuovi alunni, i genitori (e per conoscenza le/gli alunne/alunni stessi, specie se della scuola secondaria) sono tenuti a firmare per presa visione il presente Regolamento, confermando il proprio impegno a rispettarne e a farne rispettare i contenuti. La firma avverrà preferibilmente tramite le funzionalità del registro elettronico, oppure in modalità cartacea qualora necessario.

Aggiornamenti: Il Regolamento verrà riesaminato periodicamente (almeno una volta all'anno scolastico) dalla Dirigente Scolastica e dagli organi collegiali competenti, per valutare se sia necessario aggiornarlo in base all'evoluzione tecnologica, a nuove normative o a eventuali problematiche emerse nella sua applicazione pratica. Eventuali modifiche o integrazioni devono essere approvate dal Consiglio di Istituto con apposita delibera. Ogni versione aggiornata del Regolamento verrà tempestivamente comunicata a tutta la comunità scolastica con le stesse modalità (pubblicazione su sito e registro, circolare informativa) e sostituirà le disposizioni precedenti dalla data di entrata in vigore stabilita. Con l'obiettivo di mantenere alta l'attenzione su questi temi, l'Istituto promuoverà anche attività di informazione periodica: ad esempio, incontri annuali con genitori e alunni per discutere della cittadinanza digitale e delle eventuali novità normative, in modo che il Regolamento non resti una mera formalità ma sia veramente compreso e interiorizzato da tutti.