ISTITUTO COMPRENSIVO STATALE
CARRARESE EUGANEO

Via Roma, 69 35020 DUE CARRARE - PD -Tel. 049/525451
http://www.iccarrareseeuganeo.edu.it
e-mail: pdic853006@istruzione.it – C.F. 80016220289

REGOLAMENTO PER L'USO POSITIVO DELLE TECNOLOGIE DIGITALI

PROTOCOLLO INFORMATIVO E ACCETTAZIONE

L'informazione degli studenti sui contenuti delle Linee Guida per l'uso positivo delle tecnologie digitali è compito dei docenti che utilizzano i vari supporti informatici della scuola. Tale attività deve essere svolta tenendo conto dell'età degli studenti ed evidenziando sia le opportunità che i rischi connessi all'uso della comunicazione tecnologica.

Si specifica che, allo stato attuale, l'Istituto non mette a disposizione degli utenti (alunni e personale) le funzionalità di Intelligenza Artificiale generativa integrate nelle proprie piattaforme didattiche, come Google Workspace, in attesa di un pieno consolidamento delle procedure di sicurezza e di una completa integrazione pedagogica.
Nonostante tali funzioni non siano attive all'interno degli strumenti istituzionali, la scuola riconosce la necessità di fornire indicazioni generali ai docenti e agli studenti sui comportamenti corretti da adottare nel panorama digitale odierno. In particolare, l'istituto pone l'accento sulla distinzione tra i vari livelli di criticità tecnologica, esplicitando il divieto tassativo di utilizzare sistemi di IA in modalità ad alto rischio che possano compromettere la privacy, la sicurezza o l'integrità psicofisica della comunità scolastica. L'obiettivo è favorire un approccio critico che permetta agli alunni di riconoscere opportunità e rischi della rete e dell'uso delle nuove tecnologie digitali.

Il regolamento intende dunque educare alla cittadinanza digitale e all'onestà intellettuale, garantendo la sicurezza e la tutela dei minori e dei loro dati personali in ogni attività didattica mediata dalle tecnologie.

L'informazione dei genitori e dei docenti viene attuata tramite la pubblicazione del documento sul sito web della scuola, come allegato al Regolamento di Istituto.
Questo regolamento viene formalmente accettato dai genitori attraverso la sottoscrizione del **Patto di Corresponsabilità Educativa**.

1. FINALITÀ E QUADRO NORMATIVO

Il presente documento mira a promuovere un utilizzo corretto, consapevole e responsabile di tutte le apparecchiature informatiche, in piena conformità con il Regolamento UE 2024/1689 (AI Act) e le disposizioni nazionali della L. 132/2025 e del DM 166/2025.
Gli obiettivi principali sono:

- Innovazione e Valore Didattico: Assicurare un valore aggiunto alla didattica corrente attraverso l'integrazione delle tecnologie, utilizzandole come strumenti per potenziare l'apprendimento nel rispetto delle linee guida ministeriali.
- Cittadinanza Digitale e Approccio Critico: Favorire un approccio critico, in linea con la Dichiarazione dei diritti in internet (Artt. 3.4 e 3.5), permettendo agli alunni di riconoscere opportunità e rischi della rete e dell'IA, distinguendo tra contenuti generati dall'uomo e quelli prodotti da algoritmi.
- Sicurezza e Tutela dei Minori: Garantire il diritto dei minori a una navigazione sicura e alla protezione dei propri dati personali, agendo nel rigoroso rispetto del Regolamento UE 2016/679 (GDPR) per prevenire rischi legati alla privacy e alla profilazione.

- Onestà Intellettuale: Promuovere il rispetto delle norme sul copyright e sull'originalità del lavoro scolastico, educando gli studenti a dichiarare con trasparenza l'eventuale supporto ricevuto da sistemi di IA.

2. DEFINIZIONI ESSENZIALI

- IA (Intelligenza Artificiale): Sistema di machine learning che genera testi, immagini o decisioni con vari livelli di autonomia.
- IA ad alto rischio: secondo l'AI Act dell'Unione Europea, un sistema qualsiasi di Intelligenza Artificiale è classificato come ad alto rischio se il suo utilizzo può impattare significativamente sulla sicurezza o sui diritti fondamentali delle persone.
- Strumenti Integrati: Piattaforme già adottate dall'Istituto (es. Google Workspace).
- Strumenti Esterni: sono qualsiasi risorsa digitale, applicazione, dispositivo o servizio online non fornito, gestito o controllato direttamente dall'istituto scolastico.

3. LINEE GUIDA DELLA GESTIONE DELLE TIC CON GLI ALUNNI (DISTINZIONE PER ETÀ)

L'accesso alle tecnologie deve essere sempre guidato da un docente attraverso un approccio che tenga conto dello sviluppo cognitivo e delle restrizioni legali per i minori di 13 anni.
Data l'età degli utenti e le restrizioni d'uso delle applicazioni web, si applicano le seguenti prescrizioni.

3.1. Per tutti gli alunni

- Supervisione costante: Ogni attività digitale deve essere sempre guidata e controllata da un docente. È sempre vietato l'utilizzo di strumenti non certificati per la fascia d'età o non inseriti nel Piano dell'Offerta Formativa e l'uso di IA o software non espressamente autorizzati.
- Sicurezza Fisica e Digitale: È vietato toccare cavi o parti elettriche, modificare le impostazioni dei dispositivi o installare software. Qualora l'alunno si imbatta in contenuti offensivi o inappropriati, deve riferirlo immediatamente al docente o a un adulto.
- Gestione Account e Privacy: Gli alunni devono utilizzare esclusivamente l'account istituzionale (attivato dalla quarta classe della SP), mantenendo segreta la propria password. È severamente vietato inviare foto proprie, dei compagni o del personale scolastico e riferire dati personali (nomi, indirizzi, numeri di telefono) a terzi o all'interno di prompt per l'IA.
- Uso Etico dell'IA e Copyright: Gli studenti devono dichiarare se un lavoro è stato realizzato con il supporto dell'IA tramite applicativi utilizzati a casa. Ogni contenuto scaricato o utilizzato deve rispettare il copyright e citare correttamente gli autori.
- Salvataggio e Risorse: I lavori devono essere salvati esclusivamente nello spazio Google Drive associato all'account istituzionale o nelle cartelle di classe indicate, evitando il desktop dei PC o supporti rimovibili non autorizzati.

3.2. Scuola dell'Infanzia (3-6 anni): approccio dimostrativo

Modalità: L'uso delle tecnologie è di tipo esperienziale e guidato. Non è previsto l'uso autonomo di dispositivi collegati alla rete o di sistemi di IA generativa.
Cosa poter far fare (Sì):

- Interazione diretta con strumenti didattici specifici, come robot per il coding (robotica educativa) o tavoli/tappeti interattivi, sempre all'interno di un progetto educativo e sotto la supervisione costante del docente.
- Utilizzo di schermi interattivi per attività collettive di ascolto, visione o gioco cooperativo mediato dall'insegnante.

Cosa NON far fare (No):

- Uso individuale e non supervisionato di tablet, computer o smartphone.
- Creazione di account o inserimento di dati personali.
- Accedere a internet o a sistemi di IA in modo autonomo o individuale.
- Non superare in ogni caso 30' continuativi di utilizzo attivo.

3.3. Scuola Primaria - Classi I, II, III (6-8 anni): la scoperta guidata

Per questa fascia "ponte", l'uso è collettivo e mediato, finalizzato a una prima comprensione dei meccanismi tecnologici.

Cosa poter far fare (Sì):

- Utilizzare monitor interattivi (LIM) e tablet dell'Istituto per attività individuali/di piccolo gruppo coordinate dal docente.
- Utilizzare software didattici scelti dal docente che non richiedano la creazione di profili individuali o l'inserimento di dati.

Cosa NON far fare (No):

- Accedere a internet o a sistemi di IA in modo autonomo o individuale.
- Uso individuale e non supervisionato di tablet o computer.
- Creazione di account o inserimento di dati personali.
- Non superare in ogni caso 40' continuativi di utilizzo attivo.

3.4. Scuola Primaria - Classi IV e V (9-11 anni): L'alfabetizzazione operativa

In questo biennio inizia la transizione verso un uso più attivo e consapevole degli strumenti digitali di istituto.

Cosa poter far fare (Sì):

- Gestione Account: Utilizzare l'account istituzionale Google Workspace esclusivamente sotto la stretta vigilanza del docente.
- Sicurezza: Imparare a generare password efficaci e mantenerle segrete.
- Salvataggio e Archiviazione: Salvare i propri lavori scolastici esclusivamente nello spazio Google Drive associato all'account istituzionale del docente o nelle specifiche cartelle di classe.
- Partecipare ad attività guidate dal docente per esplorare il funzionamento degli algoritmi.

Cosa NON far fare (No):

- Privacy: Inviare foto proprie, dei compagni o del personale scolastico, o riferire dati personali (nomi, indirizzi, numeri di telefono) all'interno di prompt per l'IA o a terzi.
- Autonomia non autorizzata: Utilizzare software che non siano stati espressamente autorizzati e supervisionati dal docente.
- Gestione file errata: Salvare documenti sul desktop dei PC o su supporti rimovibili (chiavette USB) non autorizzati.
- Rispetto del Copyright: Utilizzare contenuti scaricati dalla rete citando correttamente gli autori e rispettando le norme sul diritto d'autore.
- Non superare in ogni caso 40' continuativi di utilizzo attivo.

3.5. Scuola Secondaria di Primo Grado (11-13 anni): l'uso critico e l'etica

L'approccio per questa fascia d'età è focalizzato sulla ricerca, il brainstorming e lo sviluppo di un senso etico digitale.

Cosa poter far fare (Sì):

- Supporto allo studio: Utilizzare le app autorizzate in modo guidato e limitato per attività di brainstorming, ricezione di feedback e supporto alla ricerca.
- Onestà Intellettuale: Dichiarare sempre e con trasparenza se un lavoro è stato realizzato con il supporto dell'IA in ambiente domestico.
- Rispetto del Copyright: Utilizzare contenuti scaricati dalla rete citando correttamente gli autori e rispettando le norme sul diritto d'autore.
- Comunicazione: Utilizzare gli strumenti ufficiali (Gmail istituzionale, Classroom) per lo scambio di materiali didattici con i docenti. Per lo scambio di informazioni con dati sensibili, utilizzare esclusivamente il registro elettronico.

Cosa NON far fare (No):

- Privacy: Inviare foto proprie, dei compagni o del personale scolastico, o riferire dati personali (nomi, indirizzi, numeri di telefono) all'interno di prompt per l'IA o a terzi.
- Plagio: Presentare come propri lavori interamente generati dall'intelligenza artificiale.

- Finalità Valutative: Utilizzare sistemi di IA per attività destinate alla valutazione (compiti, verifiche, ecc…).
- Uso Personale: Accedere ad account personali (email private, social network) o utilizzare gli strumenti digitali per scopi privati, finanziari o pubblicitari durante le lezioni.
- Manomissione: Modificare le impostazioni dei dispositivi, installare software non autorizzati o toccare cavi e parti elettriche.

4. NORME PER I DOCENTI E IL PERSONALE ATA

I docenti sono i mediatori responsabili della "cittadinanza digitale". I docenti agiscono come amministratori e mediatori responsabili delle attività digitali in classe:
Mediazione e Controllo: il docente ha il dovere di illustrare agli alunni i contenuti del seguente regolamento, monitorando costantemente le navigazioni per prevenire rischi derivanti da accessi a siti non idonei.
Comunicazioni Ufficiali: lo scambio di materiali privi di dati sensibili tra docenti e studenti deve avvenire esclusivamente tramite gli strumenti di Google Workspace (es. Classroom, Gmail istituzionale). Per i materiali contenenti dati sensibili va utilizzato esclusivamente il registro elettronico.
Supervisione Umana: la responsabilità finale delle decisioni (soprattutto valutative) resta sempre in capo alla persona fisica; è vietato usare l'IA per generare valutazioni e giudizi automatizzati senza la supervisione finale del docente.
Divieti: i docenti NON possono inserire dati sensibili degli alunni (esempio dati anagrafici, voti, PEI, PDP, ecc…) o foto identificative all'interno di sistemi di IA.
Istruzioni Operative: i docenti devono fornire indicazioni chiare sull'accensione/spegnimento dei dispositivi e sulle modalità di interazione con i software didattici.
Chiusura Sessioni: al termine delle attività, i docenti devono assicurarsi che gli alunni effettuino correttamente il logout dai propri account istituzionali e che i dispositivi siano spenti e riposti correttamente.

5. SICUREZZA E FIGURE DI RIFERIMENTO

Per garantire la protezione dei dati e la sicurezza digitale, l'Istituto si avvale di:

- DPO (Responsabile Protezione Dati): per la consulenza sulla privacy e la gestione dei *data breach*.
- RTD (Responsabile Transizione Digitale, per la scuola il Dirigente scolastico): per il coordinamento della sicurezza informatica.

Ogni incidente digitale o violazione della privacy deve essere tempestivamente segnalato a tali figure tramite la segreteria.

6. SANZIONI E RESPONSABILITÀ

La violazione consapevole delle regole contenute in questo regolamento comporta l'avviso dei genitori tramite nota didattica/disciplinare e/o le seguenti sanzioni:

- Sospensione temporanea: in base alla gravità, può essere sospeso l'accesso ai mezzi informatici. La durata dell'esclusione dai mezzi informatici è commisurata alla gravità dell'infrazione commessa.
- Valutazione della condotta: il mancato rispetto delle norme influirà sul giudizio relativo alla condotta.
- Responsabilità: per violazioni gravi o danni materiali, la scuola si riserva di richiedere il risarcimento e di informare le autorità competenti nei casi di potenziale reato.

Le sanzioni all'interno dell'Istituto hanno finalità educativa e sono graduate in base alla gravità.

(vedi pagina seguente)

Categoria di Infrazione	**Esempi di Utilizzo Scorretto**
Plagio e Onestà Intellettuale	Presentare lavori interamente generati dall'IA come propri; non citare gli autori dei materiali consultati.
Privacy e Protezione Dati	Inviare foto proprie, dei compagni o del personale scolastico, o riferire dati personali (nomi, indirizzi, numeri di telefono) all'interno di prompt per l'IA o a terzi.
Sicurezza Informatica	Tentare intenzionalmente di superare i filtri di protezione o alterare i parametri di sicurezza del sistema. Accedere e utilizzare sistemi di Intelligenza Artificiale tramite i dispositivi digitali scolastici.
Cyberbullismo e Netiquette	Utilizzare le tecnologie per atti di bullismo, razzismo o diffusione di materiale inappropriato/offensivo.
Integrità Hardware e Software	Installare software non autorizzati; modificare configurazioni; danneggiare fisicamente i dispositivi (cavi, tastiere, ecc.).
Uso non Didattico	Utilizzare account personali (email, social) o strumenti digitali per fini privati, finanziari o pubblicitari durante le lezioni.