POLICY BYOD (Bring Your Own Device) PER L'UTILIZZO DI STRUMENTI DI INTELLIGENZA ARTIFICIALE

1. Premessa

La presente Policy disciplina l'utilizzo di dispositivi personali (BYOD – Bring Your Own Device) nell'ambito delle attività scolastiche che prevedono l'utilizzo di sistemi di Intelligenza Artificiale (IA), nel rispetto del Regolamento (UE) 2024/1689 ("AI Act"); del GDPR; delle norme in materia di sicurezza informatica; delle disposizioni interne dell'Istituto.

La Policy è finalizzata a: garantire un utilizzo sicuro e consapevole degli strumenti IA; tutelare i dati personali; proteggere gli studenti e il personale scolastico; ridurre i rischi derivanti dall'utilizzo di dispositivi personali.

---

2. Ambito di applicazione

La presente Policy si applica: ai docenti; agli studenti; al personale ATA; che utilizzano dispositivi personali per accedere: alle piattaforme scolastiche; ai servizi cloud; ai sistemi di Intelligenza Artificiale; agli account istituzionali dell'Istituto.

---

3. Definizioni

3.1 BYOD

Utilizzo di dispositivi personali per attività scolastiche o istituzionali.

3.2 Sistemi IA

Piattaforme e strumenti basati su Intelligenza Artificiale, inclusi: chatbot; sistemi generativi; assistenti virtuali; strumenti di supporto didattico; piattaforme di produttività con funzionalità IA.

---

4. Principi generali

L'utilizzo di dispositivi personali deve avvenire nel rispetto dei principi di: sicurezza; minimizzazione dei dati; protezione dei minori; supervisione umana; utilizzo consapevole delle tecnologie IA.

---

5. Utilizzo consentito

L'utilizzo di dispositivi personali è consentito esclusivamente: per finalità didattiche; per attività istituzionali autorizzate; nel rispetto delle indicazioni dell'Istituto; mediante strumenti e piattaforme autorizzati.

---

6. Utilizzo di account istituzionali

L'accesso ai sistemi IA e alle piattaforme scolastiche deve avvenire preferibilmente tramite: account istituzionali; credenziali assegnate dall'Istituto.

È sconsigliato l'utilizzo di account personali per attività connesse al servizio scolastico.

---

7. Misure minime di sicurezza

I dispositivi personali utilizzati devono garantire: aggiornamento del sistema operativo; utilizzo di password robuste; blocco automatico del dispositivo; antivirus/strumenti di protezione aggiornati; browser aggiornati; protezione delle credenziali di accesso.

---

8. Protezione dei dati personali

È vietato caricare nei sistemi IA mediante dispositivi personali: PEI, PDP, dati sanitari; dati disciplinari; documenti riservati; immagini o video degli studenti; dati rientranti nell'art. 9 GDPR, salvo espressa autorizzazione e utilizzo di piattaforme conformi alle disposizioni dell'Istituto.

---

9. Utilizzo corretto degli strumenti IA

Gli utenti devono: verificare criticamente gli output IA; evitare utilizzi impropri o illeciti; rispettare le indicazioni dei docenti e dell'Istituto; non utilizzare strumenti IA per attività fraudolente o scorrette.

---

10. Divieti

È vietato: utilizzare strumenti IA non autorizzati dall'Istituto; condividere credenziali istituzionali; utilizzare account di altri utenti; effettuare upload di dati eccedenti o riservati; utilizzare IA per cyberbullismo, deepfake o contenuti offensivi; aggirare i sistemi di sicurezza o i filtri di rete dell'Istituto.

---

11. Sicurezza della rete

L'Istituto può adottare: filtri DNS/web; sistemi di logging; monitoraggio amministrativo; limitazioni di accesso,

al fine di garantire sicurezza, continuità operativa e protezione dei dati.

---

12. Responsabilità degli utenti

Ogni utente è responsabile: del corretto utilizzo del proprio dispositivo; della custodia delle credenziali; dei dati trattati; delle attività effettuate tramite il proprio account.

---

13. Incidenti e violazioni

Eventuali: anomalie; accessi abusivi; smarrimenti del dispositivo; utilizzi impropri; incidenti relativi ai sistemi IA, devono essere tempestivamente segnalati all'Istituto.

---

14. Controlli e monitoraggio

L'Istituto può effettuare verifiche: sulla sicurezza degli accessi; sull'utilizzo degli account istituzionali; sul rispetto della presente Policy, nel rispetto dei principi di: proporzionalità; minimizzazione; tutela della riservatezza.

---

15. Formazione e AI Literacy

L'Istituto promuove attività di: alfabetizzazione all'Intelligenza Artificiale; sicurezza informatica; utilizzo consapevole delle tecnologie digitali; protezione dei dati personali.

---

16. Violazioni della Policy

Il mancato rispetto della presente Policy può comportare: sospensione degli accessi; limitazioni all'utilizzo delle piattaforme; provvedimenti disciplinari; eventuali responsabilità civili o penali.

---

17. Aggiornamento della Policy

La presente Policy potrà essere aggiornata: in relazione all'evoluzione normativa; all'evoluzione tecnologica dei sistemi IA; alle indicazioni del Ministero dell'Istruzione e del Merito; ai provvedimenti del Garante per la protezione dei dati personali.