Ministero dell'Istruzione e del Merito
Ufficio Scolastico Regionale per il Lazio
Liceo Scientifico Statale "G. KEPLERO"
Cod. Mecc. RMPS19000T - C.F. 80230950588 - Distr. 23° - Sede centrale: Via Silvestro Gherardi, 87/89 - 00146 Roma
Via Avicenna, snc - 00146 Roma - Tel. 06121123925 - Succursale: Via delle Vigne, 156 - 00148 Roma – Tel. 06121126685
Sito web: www.liceokeplerororoma.edu.it - E-mail: rmps19000t@istruzione.it - succursale@liceokeplerororoma.edu.it

Circ. n. 97 a.s. 2025/26

Ai docenti
Al D.S.G.A.
Al personale A.T.A.
All'Albo online del Liceo "Keplero"

OGGETTO: Linee guida per il corretto trattamento dei dati personali particolari (ex dati sensibili).

Premessa

Si ritiene opportuno richiamare l'attenzione di tutto il personale scolastico sulle corrette procedure da seguire per il trattamento dei *dati personali particolari* degli alunni (ex dati sensibili), con particolare riferimento ai documenti come PEI, PDP, certificazioni sanitarie e altra documentazione contenente informazioni riservate.

Si ricorda che la protezione di questi dati è un obbligo normativo sancito dal Regolamento UE 2016/679 (GDPR) e dal D.lgs. 196/2003 (Codice Privacy), ma rappresenta soprattutto un dovere etico nei confronti degli alunni e delle loro famiglie.

Linee guida operative

1. Documenti cartacei

- I documenti cartacei contenenti dati particolari devono essere conservati in armadi chiusi a chiave, situati in locali ad accesso controllato.
- L'accesso a tali documenti è consentito solo al personale autorizzato per il tempo strettamente necessario all'espletamento delle proprie funzioni.
- Non lasciare mai incustoditi documenti contenenti dati particolari su scrivanie o in luoghi accessibili a persone non autorizzate.
- Quando non più necessari, i documenti devono essere riposti negli appositi archivi.

2. Documenti digitali

- I documenti digitali contenenti dati particolari devono essere salvati **prioritariamente** negli spazi di archiviazione ufficiali predisposti dall'Istituto.
- Si raccomanda di limitare l'utilizzo di dispositivi di memoria rimovibili (chiavette USB, hard disk esterni) per la conservazione di dati particolari.
- Nel caso sia necessario l'utilizzo di dispositivi rimovibili questi devono essere:
  - ✓ Dotati di password robusta o sistemi di crittografia
  - ✓ Utilizzati solo temporaneamente e mai come archivio permanente
  - ✓ Custoditi con la massima attenzione
  - ✓ Verificati periodicamente per la presenza di malware

3. Trasmissione dei dati

- La condivisione di documenti contenenti dati particolari deve avvenire esclusivamente attraverso i canali ufficiali dell'Istituto.

- È vietato l'invio di documenti contenenti dati particolari tramite e-mail personali o sistemi di messaggistica non ufficiali.
- Nell'invio di comunicazioni via e-mail contenenti dati particolari, utilizzare esclusivamente gli indirizzi istituzionali e, ove possibile, proteggere gli allegati con password da comunicare separatamente.

4. Stampa dei documenti

- Limitare la stampa dei documenti contenenti dati particolari allo stretto necessario.
- Ritirare immediatamente le stampe dalla stampante condivisa.
- Non lasciare incustoditi fogli stampati contenenti dati particolari.
- Distruggere i documenti stampati non più necessari, preferibilmente utilizzando gli appositi distruggi-documenti.

5. Riunioni e colloqui

- Durante le riunioni (GLO, consigli di classe, ecc.) nelle quali si discutono situazioni relative a dati particolari, assicurarsi che siano presenti solo le persone autorizzate.
- Non lasciare documentazione contenente dati particolari nelle sale riunioni al termine degli incontri.
- Nei colloqui con i genitori, assicurarsi di parlare in luoghi riservati, evitando corridoi o spazi aperti.

6. Utilizzo di dispositivi personali

- È consentito l'utilizzo di dispositivi personali (computer, tablet, smartphone, dispositivi di archiviazione) per il trattamento di dati particolari, purché vengano rispettate rigorose misure di sicurezza
- I dispositivi personali utilizzati devono essere:
  - ✓ Protetti da password robusta
  - ✓ Dotati di software antivirus aggiornato
  - ✓ Configurati in modo che i dati vengano salvati preferibilmente negli spazi cloud istituzionali
  - ✓ Mantenuti sotto costante controllo fisico
  - ✓ Configurati, se possibile, con funzionalità di backup e di cancellazione remota

Procedura in caso di violazione dei dati (data breach)

In caso di perdita, furto o accesso non autorizzato a dati particolari (ad esempio smarrimento di chiavette USB, documenti cartacei, dispositivi elettronici, accessi non autorizzati a documenti digitali), è obbligatorio:

1. Segnalare **immediatamente** l'episodio al Dirigente Scolastico.
2. Fornire tutte le informazioni disponibili sull'accaduto.
3. Non tentare di risolvere autonomamente la situazione.
4. Collaborare con il Dirigente Scolastico e il DPO per la gestione dell'incidente.

Si ricorda che la mancata o tardiva segnalazione di un data breach può comportare conseguenze gravi per l'Istituzione scolastica e per gli interessati.

Responsabilità

Si ricorda che ogni autorizzato al trattamento è responsabile della protezione dei dati personali trattati nell'esercizio delle proprie funzioni.

Tutti i destinatari della presente Circolare sono tenuti a conformare il proprio comportamento alle indicazioni ivi fornite.

Roma, 27/12/2025

IL DIRIGENTE SCOLASTICO
Prof. Roberto Toro
(Firma autografa sostituita a mezzo stampa, ai sensi dell'art. 3, comma 2, del D.lgs. 39/93)