SEGNATURA: Istituto Professionale di Stato "Giuseppe Medici" - Protocollo 0014067/2025 - Legnago, 25/10/2025

Vademecum Privacy

Personale ATA – Istituto Professionale di Stato "Giuseppe Medici"

1. Principi generali

Il personale ATA contribuisce in modo essenziale alla protezione dei dati personali trattati all'interno dell'Istituto.
Ogni operazione su dati di studenti, famiglie, docenti o colleghi deve rispettare i principi del **Regolamento (UE) 2016/679 (GDPR)** e del **D.Lgs. 196/2003**.

I principi da ricordare

- **Legalità** – i dati si trattano solo per compiti istituzionali e nel rispetto delle norme.
- **Trasparenza** – gli interessati (studenti, famiglie, personale) devono poter sapere come e perché i loro dati sono usati.
- **Minimizzazione** – si raccolgono solo i dati strettamente necessari.
- **Riservatezza e sicurezza** – i dati devono essere protetti da accessi non autorizzati, divulgazioni improprie o perdite.

2. Ruoli e responsabilità

- **Titolare del trattamento:** il Dirigente scolastico.
- **Responsabile della Protezione dei Dati (RPD):** figura di riferimento per chiarimenti, reclami e segnalazioni.
- **Personale ATA:** soggetti *autorizzati al trattamento*, che operano secondo le istruzioni ricevute dal Dirigente e nel rispetto delle procedure interne.

3. Comportamenti generali

Cosa fare	Cosa non fare
Proteggere la riservatezza dei dati trattati.	Parlare di questioni riservate (salute, famiglie, assenze, provvedimenti) con persone non autorizzate.
Utilizzare solo strumenti e canali ufficiali (PEC, email istituzionale, registro elettronico).	Usare chat personali, social o telefoni privati per divulgare dati scolastici.
Mantenere ordinati e custoditi fascicoli, registri e documenti.	Lasciare documenti o PC incustoditi, aperti o accessibili a terzi.
Segnalare immediatamente eventuali violazioni o smarrimenti di dati.	Tentare di risolvere autonomamente violazioni o problemi senza informare la Dirigenza.

Il pettegolezzo o la diffusione impropria di notizie costituisce violazione della normativa sulla protezione dei dati personali (GDPR e D.Lgs. 196/2003) e dei doveri del dipendente pubblico (D.P.R. 62/2013). Comporta sanzioni disciplinari e, nei casi più gravi, responsabilità penali.

4. Assistenti amministrativi

Gli assistenti amministrativi trattano dati particolarmente sensibili e devono agire con la massima prudenza.

Indicazioni pratiche

- Raccogliere e registrare **solo i dati previsti dalla normativa** (iscrizioni, contratti, graduatorie, certificazioni).

Documento informatico firmato digitalmente da STEFANO MINOZZI ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate

- **Limitare la conoscenza dei dati** al personale autorizzato e per il tempo necessario.
- Custodire fascicoli e archivi in **locali chiusi o protetti da password**.
- Pubblicare online **solo le informazioni previste per legge** (es. graduatorie con nome, cognome, punteggio e posizione).
- Non diffondere informazioni su salute, disabilità, condizioni economiche o disciplinari.
- Verificare sempre la **correttezza e la sicurezza** dei dati inseriti nel registro elettronico o nei software gestionali.

5. Assistenti tecnici

- Mantenere **la sicurezza dei sistemi informatici**, controllando accessi e aggiornamenti.
- Evitare l'installazione di software o dispositivi non autorizzati.
- Non accedere a dati o cartelle che non rientrano nelle proprie mansioni.
- Collaborare con il referente informatico e con il Dirigente per la **protezione dei dati digitali** e la gestione delle password.
- In caso di guasti o perdite di dati, **informare immediatamente** la Dirigenza.

6. Collaboratori scolastici

I collaboratori scolastici, in quanto personale che ha frequenti contatti con studenti e famiglie, svolgono un ruolo delicato nella tutela della privacy.

Cosa fare	Cosa non fare
Mantenere **riservate tutte le informazioni apprese** nello svolgimento del servizio (assenze, malattie, situazioni familiari, provvedimenti).	**Pettegolezzi o commenti**, anche informali, con studenti, genitori o estranei su fatti che riguardano persone della scuola o altre persone afferenti all'Istituto (studenti, famiglie ecc.).
In caso di domande da parte di studenti, genitori o esterni, **rinviare sempre agli uffici competenti** (Segreteria o Dirigenza).	Riferire notizie su assenze, problemi di salute o situazioni personali di studenti o docenti.
Segnalare con tempestività eventuali situazioni che possano riguardare la sicurezza o il benessere degli alunni.	**Diffondere e/o cercare informazioni senza autorizzazione o al di fuori delle proprie competenze.**

7. Sicurezza informatica e documentale

- Utilizzare **credenziali personali** e non condividerle.
- Bloccare il computer o la postazione quando ci si allontana.
- Archiviare e distruggere correttamente i documenti cartacei secondo le istruzioni dell'Istituto.
- Non copiare dati su dispositivi esterni non autorizzati (chiavette, dischi, cloud privati).
- Evitare di usare email personali per attività d'ufficio.

8. Questionari

- Per indagini o ricerche esterne (questionari, interviste) serve **l'autorizzazione della Dirigenza** e un'adeguata informativa per gli interessati.

9. In caso di dubbio

- Non fornire mai informazioni personali a chi non è chiaramente autorizzato.
- In caso di richiesta, errore, sospetta violazione o dubbio, **contattare subito il Dirigente scolastico o il RPD**.
- Ricorda: la collaborazione e la prudenza sono la migliore forma di tutela.

In sintesi

1. Tratta solo i dati indispensabili e per scopi istituzionali.
2. Proteggi la riservatezza di studenti, famiglie e colleghi.
3. Evita qualsiasi forma di diffusione non autorizzata o pettegolezzo.
4. Usa esclusivamente i canali e gli strumenti ufficiali della scuola.
5. Segnala immediatamente ogni violazione o problema.

IL DIRIGENTE
prof. Stefano Minozzi
Documento firmato digitalmente ai sensi del c.d.
Codice dell'Amministrazione digitale e normativa connessa