



Istituto Comprensivo Grosseto 1 “Alberto Manzi”
Via Corelli, 3 – 58100 Grosseto Tel. 0564 413622 Fax. 0564 427112
Cod. Meccanografico: gric830005 - Codice Fiscale: 80003460534 - C.U.U.: UF83XE
E-mail: gric830005@istruzione.it PEC: gric830005@pec.istruzione.it
www.icgrosseto1.edu.it

DESIGNAZIONE A PERSONALE AUTORIZZATO
AL TRATTAMENTO DEI DATI PERSONALI
(art. 29 Reg. UE 2016/679 – art. 2-quaterdecies D.lgs. 196/2003)

ISTRUZIONI OPERATIVE PER LE PERSONE AUTORIZZATE
AL TRATTAMENTO DEI DATI PERSONALI
(ai sensi dell’art. 29 Reg. UE 2016/679 e art. 2-quaterdecies D.lgs. 196/2003)

Versione 1.1 – in vigore dal 01/09/2026

1. Finalità e ambito di applicazione

Il presente documento contiene le **istruzioni operative** che le persone autorizzate al trattamento dei dati personali dell’Istituzione scolastica sono tenute a rispettare nello svolgimento delle proprie mansioni.

Le istruzioni si applicano a tutti i trattamenti di dati personali, **in forma cartacea e digitale**, effettuati per finalità istituzionali.

2. Principi generali di trattamento

(art. 5 Reg. UE 2016/679)

La persona autorizzata è tenuta a trattare i dati personali nel rispetto dei seguenti principi:

- liceità, correttezza e trasparenza;
- minimizzazione dei dati;
- esattezza e aggiornamento;
- limitazione della conservazione;
- integrità e riservatezza.

I dati personali devono essere trattati **esclusivamente per finalità istituzionali** e nei limiti delle mansioni assegnate.

3. Accesso ai dati e sostituibilità

(art. 29 Reg. UE 2016/679 – art. 2-quaterdecies D.lgs. 196/2003)

La persona autorizzata opera sotto l’autorità del Titolare del trattamento e nel rispetto delle istruzioni impartite.

Considerata l’organizzazione del servizio amministrativo, l’accesso alle banche dati e agli archivi è **condiviso tra il personale autorizzato**, al fine di garantire la continuità del servizio e la sostituzione reciproca degli operatori.

In ogni caso:

- l’accesso deve essere **pertinente e giustificato** dalle attività svolte;
- è vietata ogni consultazione di dati **non necessaria** o per finalità personali.

4. Trattamento di dati particolari e giudiziari

(artt. 9 e 10 Reg. UE 2016/679)

I dati appartenenti a categorie particolari (es. salute, disabilità, BES) e i dati giudiziari devono essere trattati con **particolare attenzione** e nel rispetto delle specifiche istruzioni impartite dal Titolare del trattamento.

È vietata qualsiasi forma di comunicazione o diffusione non autorizzata.

5. Documenti cartacei e archivi fisici

(art. 32 Reg. UE 2016/679)

La persona autorizzata è tenuta a:

- custodire i documenti contenenti dati personali in luoghi non accessibili a soggetti non autorizzati;
- non lasciare incustoditi documenti o fascicoli;
- riconsegnare la documentazione consultata agli uffici competenti;
- procedere alla distruzione dei documenti non più necessari secondo le modalità stabilite dall'Istituzione scolastica.

6. Strumenti informatici e credenziali

(art. 32 Reg. UE 2016/679)

Le credenziali di accesso ai sistemi informativi:

- sono **personali e non cedibili**.
- devono essere custodite con cura e riservatezza;
- non devono essere annotate o comunicate a terzi.

In caso di smarrimento, furto o sospetto utilizzo improprio delle credenziali, la persona autorizzata deve informare **immediatamente** il Titolare del trattamento o il soggetto delegato.

7. Comunicazioni e trasmissione dei dati

(art. 5 e art. 32 Reg. UE 2016/679)

La comunicazione di dati personali a soggetti interni o esterni è consentita solo nei casi previsti dalla legge o su espressa autorizzazione del Titolare del trattamento.

Le comunicazioni devono avvenire:

- con modalità riservate;
- tramite strumenti istituzionali;
- evitando la diffusione di dati a soggetti non legittimati.

8. Supporti rimovibili

(art. 32 Reg. UE 2016/679)

L'utilizzo di supporti rimovibili (chiavette USB, hard disk esterni, ecc.) è consentito solo se strettamente necessario.

Tali supporti devono:

- essere custoditi con particolare attenzione;
- non essere lasciati incustoditi;
- essere resi inutilizzabili o distrutti quando non più necessari, soprattutto se contenenti dati particolari o giudiziari.

9. Lavoro fuori sede e modalità agile

(art. 32 Reg. UE 2016/679)

In caso di attività svolta fuori dalla sede scolastica, la persona autorizzata deve:

- evitare che persone non autorizzate possano accedere ai dati;

- utilizzare esclusivamente **account e strumenti istituzionali**;
- evitare il collegamento a reti non sicure;
- non salvare dati personali su dispositivi o cloud personali;
- adottare misure di sicurezza (blocco schermo, antivirus aggiornati, ecc.).

Eventuale documentazione cartacea deve essere custodita in contenitori chiusi e sicuri.

10. Segnalazione di incidenti e violazioni

(artt. 33 e 34 Reg. UE 2016/679)

Ogni evento che possa comportare:

- perdita,
- distruzione,
- accesso non autorizzato,
- diffusione indebita di dati personali

deve essere **segnalato tempestivamente** al Titolare del trattamento o al Responsabile della Protezione dei Dati (RPD/DPO), secondo le procedure interne.

11. Obbligo di riservatezza

(art. 5 Reg. UE 2016/679)

L'obbligo di riservatezza riguarda tutte le informazioni e i dati personali trattati e **permane anche dopo la cessazione del rapporto di lavoro**, senza limiti temporali.

12. Aggiornamento delle istruzioni e responsabilità

(art. 29 Reg. UE 2016/679)

Le presenti istruzioni possono essere aggiornate dal Titolare del trattamento.

Le presenti Istruzioni operative sono adottate nella versione indicata in intestazione. Eventuali aggiornamenti o integrazioni saranno comunicati dal Titolare del trattamento e diventeranno vincolanti dalla data di adozione della nuova versione.

Il mancato rispetto delle istruzioni e della normativa vigente può comportare responsabilità disciplinari, civili e penali, secondo quanto previsto dalla legge.

13. Disposizioni specifiche per il Direttore dei Servizi Generali e Amministrativi (DSGA)

(artt. 5, 29 e 32 Reg. UE 2016/679)

Il Direttore dei Servizi Generali e Amministrativi (DSGA), in ragione delle funzioni di coordinamento, supervisione e continuità dei servizi amministrativi, è autorizzato ad accedere ai dati personali, anche appartenenti a categorie particolari e giudiziari, trattati dagli uffici amministrativi dell'Istituzione scolastica, nei limiti delle finalità istituzionali e delle attività assegnate.

In caso di necessità organizzative, assenza del personale o esigenze di continuità del servizio, l'accesso ai sistemi informativi e ai dati avviene mediante credenziali personali, procedure di reset o account istituzionali di servizio, secondo le modalità definite dall'Istituzione scolastica, senza utilizzo delle password personali di altri utenti.

Il DSGA sovrintende alla gestione dei profili di accesso ai sistemi informativi dell'Istituzione scolastica e può richiedere la creazione, la modifica, la sospensione o la disattivazione delle credenziali di accesso del personale amministrativo, nel rispetto delle misure di sicurezza adottate.

Resta fermo l'obbligo di riservatezza e il rispetto dei principi di liceità, correttezza, minimizzazione, integrità e sicurezza del trattamento dei dati personali.