Ministero dell'Istruzione e del Merito

ISTITUTO COMPRENSIVO "CAVOUR – MAZZINI"
annesso al CONVITTO AUDIOFONOLESI

Piazza F. Pizzo n. 10 – 91025 Marsala (TP) - Tel. 0923/714186
Cod.Fisc. 91042910819 Convitto - C.F. 91042920818 I.C. Cavour-Mazzini
Cod.Mecc. TPVC050004
e-mail tpvc050004@istruzione.it - Pec tpvc050004@pec.istruzione.it

Sede OSSERVATORIO per la lotta alla DISPERSIONE SCOLASTICA

Prot. e data vds. segnatura

LINEE GUIDA PER IL TRATTAMENTO E LA PROTEZIONE DEI DATI PERSONALI
INCARICATI DEL TRATTAMENTO
ASSISTENTI TECNICI

Le presenti Linee Guida contengono la descrizione delle misure operative che gli assistenti tecnici sono chiamati ad adottare per garantire la sicurezza dei dati personali dei soggetti interessati.

Definizioni

Trattamento: qualunque operazione, svolta con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati (art. 4 GDPR).

Incaricato del trattamento: chiunque agisca sotto l'autorità del Titolare del trattamento o del Responsabile del trattamento (art. 29 GDPR).

***Violazione dei dati personali:** la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art. 4, 12, GDPR)

Misure operative generiche

Nello svolgimento delle sue mansioni l'assistente tecnico, in qualità di incaricato del trattamento, dovrà:

- Trattare i dati personali in modo lecito e secondo correttezza, per scopi determinati, espliciti e legittimi e per finalità compatibili con quelle relative al profilo di appartenenza
- Verificare che i dati siano esatti e, se necessario, aggiornarli;
- Verificare che i dati siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- Conservare i dati in forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
- Comunicare o eventualmente diffondere o trasferire all'esterno i dati personali relativi a terzi esclusivamenteai soggetti autorizzati, ed in ogni caso nel rispetto delle istruzioni ricevute;
- Al di fuori dell'ambito lavorativo, l'incaricato dovrà astenersi dal comunicare a terzi qualsivoglia dato personale;
- Informare prontamente il Titolare, il Referente Privacy, o il Responsabile per la Protezioni dei Dati dell'Istituto (RPD), di ogni circostanza idonea a determinare una violazione dei dati personali (*).
- Non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Titolare ed in ogni caso senza il previo accertamento dell'identità del richiedente;
- Non lasciare a disposizione di estranei documenti o supporti di memorizzazione (cd, dvd, pen drive) contenenti dati personali, e/o dati personali appartenenti a categorie particolari e/o dati personali relativi a condanne penali e reati;
- Non abbandonare la postazione di lavoro senza aver previamente provveduto a custodire in luogo sicuro i documenti o supporti di memorizzazione (cd, dvd, pen drive) contenenti dati personali e/o dati personali

appartenenti a categorie particolari e/o dati personali relativi a condanne penali e reati;

- Nel caso di utilizzo di registri cartacei, al termine delle attività didattiche giornaliere provvedere personalmente a riporli in apposito armadio o cassetto dotato di serratura nel locale dell'edificio scolastico adibito alla loro custodia, o in alternativa consegnarli al collaboratore scolastico incaricato.
- Nel caso in cui l'incaricato entri in possesso di documenti, che contengono dati personali, particolari, e giudiziari e/o penali inutilizzati o superflui (es. doppia copia non necessaria di un documento, appunti provvisori, copia non autorizzata, etc…) dovrà accertarsi della loro corretta distruzione (tramite il "distruggi-documenti");
- Effettuare copie fotostatiche di documenti contenenti dati personali, particolari, e giudiziari e/o penali, esclusivamente previa autorizzazione;
- Al fine di garantire la protezione, l'integrità e la riservatezza dei dati all'atto di duplicazione di documenti attraverso fotocopie e del trasporto degli stessi, l'incaricato dovrà comportarsi in maniera lecita prevenendone la perdita, la distruzione, o eventuali danni accidentali;
- Procedere alla chiusura dei locali non utilizzati in caso di assenza del personale;
- Verificare la corretta funzionalità dei meccanismi di chiusura di armadi che custodiscono dati personali, segnalando tempestivamente al responsabile di sede eventuali anomalie.

Misure operative specifiche all'utilizzo di tecnologie informatiche

- Per un'adeguata protezione dei diversi software gestionali, dispositivi informatici, o piattaforme software, scegliere una password alfanumerica, composta da almeno otto caratteri di cui una lettera in maiuscolo e un carattere speciale, non facilmente intuibile, evitando che contenga riferimenti alla propria persona (es. proprio nome o di congiunti, date di nascita, ecc.).
- Conservare accuratamente la propria password di accesso a software gestionali, dispositivi informatici, o piattaforme software ed astenersi dal comunicarla a soggetti terzi per qualsiasi motivo.
- Cambiare periodicamente (almeno una volta ogni tre mesi) la propria password dei software gestionali, dispositivi informatici, o piattaforme software;
- Prima di abbandonare la postazione di lavoro anche temporaneamente, effettuare il log-off, dai diversi software gestionali, dispositivi informatici, o piattaforme software, e, laddove presenti, da sistemi di autenticazione di rete, o quantomeno impostare uno screen- saver protetto da password.
- Al termine di ogni sessione di lavoro, procedere allo spegnimento dei dispositivi informatici.
- Nella comunicazione multimediale con alunni e genitori utilizzare esclusivamente le piattaforme informatiche messe a disposizione dall'Istituto; è fatto divieto di utilizzare social network.
- Nell'utilizzo della posta elettronica non aprire allegati di cui non sia certa la provenienza, e controllare accuratamente l'indirizzo dei destinatari prima di inviare e-mail contenenti in allegato o nel corpo del messaggio dati personali.
- Nel caso di creazione, lettura o modifica di documenti informatici residenti in locale (cioè non accessibili da WEB o in cloud) contenenti dati personali di alunni o genitori, utilizzare esclusivamente le apparecchiature informatiche fornite dalla scuola, presenti nelle aule, laboratori e sale docenti, in quanto in linea con le misure minime di sicurezza ICT emanate dall'AGID.

Disposizioni specifiche per la gestione degli apparati

In relazione alla gestione degli apparati l'assistente tecnico è tenuto ad osservare le presenti disposizioni specifiche:

1. Trattamento dei dati personali
   - L'assistente tecnico incaricato della gestione degli apparati informatici è autorizzato al trattamento dei dati personali limitatamente alle operazioni necessarie per garantire il corretto funzionamento delle infrastrutture digitali.
   - Il trattamento deve avvenire nel rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione e integrità previsti dal Regolamento (UE) 2016/679 (GDPR).
2. Accesso ai sistemi
   - L'accesso ai sistemi informatici contenenti dati personali (es. registro elettronico, piattaforme didattiche, archivi digitali) è consentito solo se strettamente necessario per interventi tecnici, manutentivi o di ripristino.
   - Ogni accesso deve essere specificamente autorizzato dal titolare, tracciato e documentato, ove tecnicamente possibile, per garantire la responsabilità e la verifica delle operazioni svolte.
3. Riservatezza e obblighi di non divulgazione
   - L'assistente tecnico è vincolato da un obbligo di riservatezza assoluta sui dati personali trattati, anche dopo la cessazione dell'incarico.

- È vietata qualsiasi forma di divulgazione, comunicazione o utilizzo improprio dei dati a cui si accede durante l'attività lavorativa.

4. Sicurezza dei dati e degli apparati
   - È responsabilità del gestore adottare misure tecniche e organizzative adeguate per prevenire accessi non autorizzati, perdite, alterazioni o distruzioni dei dati.
   - Deve garantire che gli apparati informatici siano configurati in modo da limitare l'accesso ai soli utenti autorizzati, con credenziali sicure e aggiornate.
5. Supporto al DPO e al Titolare del trattamento
   - L'assistente tecnico collabora con il Responsabile della Protezione dei Dati (DPO) e con il Dirigente Scolastico, fornendo informazioni utili per la valutazione dei rischi e per la gestione di eventuali incidenti di sicurezza.
   - È tenuto a segnalare tempestivamente qualsiasi anomalia, violazione o sospetto di data breach.

Si precisa che il titolare è sempre e comunque responsabile della mancata esecuzione degli adempimenti previsti dal D.lgs. n.196/2003 e del Regolamento UE 2016/679. Tuttavia le responsabilità, per l'inosservanza delle istruzioni impartite dal Titolare e/o dai responsabili, possono riguardare anche gli incaricati, che non rispettino o non adottino le misure necessarie.

LA RETTRICE DIRIGENTE SCOLASTICA
Prof.ssa *Annalisa Giacalone*

_____

Per presa visione e accettazione

_____

Firmato da:
GIACALONE ANNALISA
Ministero dell'Istruzione e del Merito
22/09/2025 21:44:20