Viale F.Turati 1/R 52011 Bibbiena (Ar) Tel : 0575-955716 c.f. 94004080514 cod. mecc.ARIC82800R
Ambito territoriale AR3 - USR Toscana - UST Arezzo - Sito ufficiale https://icdovizibibbiena.edu.it/
indirizzi e mail : aric82800r@istruzione.it - aric82800r@pec.istruzione.it

Prot. n. (si veda intestazione) Bibbiena, (si veda intestazione)

LINEE GUIDA IN MATERIA DI SICUREZZA PER IL TRATTAMENTO DEI DATI PERSONALI
ASSISTENTI TECNICI AUTORIZZATI AL TRATTAMENTO

Le presenti linee guida descrivono le misure operative che gli assistenti tecnici, in qualità di soggetti autorizzati al trattamento, sono chiamati ad adottare per garantire la sicurezza dei dati personali degli interessati, ai sensi del Regolamento UE 2016/679 e del D.Lgs. 196/2003 (novellato dal D.Lgs. 101/2018).

Definizioni

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

Persona autorizzata al trattamento: chiunque agisca sotto l'autorità del titolare o del responsabile del trattamento (art. 29 del Regolamento; art. 2-quaterdecies del Codice). È la figura che il previgente Codice definiva "incaricato".

Violazione dei dati personali (data breach): 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 del Regolamento).

Misure operative generali

Nello svolgimento delle proprie mansioni l'assistente tecnico, in qualità di soggetto autorizzato al trattamento, dovrà:

- trattare i dati personali in modo lecito e corretto, per scopi determinati, espliciti e legittimi e per finalità compatibili con quelle del proprio profilo, verificando che siano esatti, aggiornati, pertinenti, completi e non eccedenti;
- conservare i dati in forma che consenta l'identificazione dell'interessato per un tempo non superiore a quello necessario agli scopi del trattamento;

- comunicare, diffondere o trasferire all'esterno dati personali relativi a terzi esclusivamente ai soggetti autorizzati e nel rispetto delle istruzioni ricevute; al di fuori dell'ambito lavorativo astenersi dal comunicare a terzi qualsivoglia dato personale;
- segnalare senza ritardo al Dirigente Scolastico e, per il suo tramite, al Responsabile della Protezione dei Dati (nonché all'eventuale referente privacy) ogni circostanza idonea a determinare una violazione dei dati personali, ai fini degli adempimenti di cui agli artt. 33 e 34 del Regolamento;
- non fornire telefonicamente o con altri mezzi dati e informazioni relativi a terzi senza una specifica autorizzazione del titolare e senza il previo accertamento dell'identità del richiedente;
- non lasciare a disposizione di estranei, e non abbandonare la postazione senza aver custodito in luogo sicuro, documenti o supporti di memorizzazione contenenti dati personali, categorie particolari di dati o dati relativi a condanne penali e reati;
- nel caso di registri cartacei, al termine delle attività giornaliere riporli in armadio o cassetto dotato di serratura nel locale adibito alla loro custodia, o consegnarli al collaboratore scolastico incaricato;
- accertarsi della corretta distruzione (tramite distruggi-documenti) dei documenti contenenti dati personali, particolari o giudiziari non più utilizzati o superflui, ed effettuare copie fotostatiche di tali documenti esclusivamente previa autorizzazione, prevenendone perdita, distruzione o danni durante duplicazione e trasporto;
- provvedere alla chiusura dei locali non utilizzati in caso di assenza del personale e verificare la corretta funzionalità dei meccanismi di chiusura degli armadi che custodiscono dati personali, segnalando tempestivamente al responsabile di sede eventuali anomalie.

Misure operative specifiche per l'uso delle tecnologie informatiche

- utilizzare password di almeno dodici caratteri (maiuscole, minuscole, numeri e caratteri speciali), non facilmente intuibili, non riconducibili alla propria persona e non riutilizzate su altri servizi; utilizzare, ove disponibile, l'autenticazione a più fattori (MFA);
- conservare accuratamente le proprie password e non comunicarle a terzi per alcun motivo; modificare la password in caso di sospetta compromissione o su indicazione dell'amministratore di sistema (non è richiesta una rotazione periodica prefissata, in coerenza con le indicazioni AgID);
- prima di abbandonare la postazione, anche temporaneamente, effettuare il log-off dai sistemi e dalle piattaforme o attivare il blocco schermo protetto da password; al termine della sessione di lavoro spegnere i dispositivi;
- non immettere in strumenti di intelligenza artificiale generalisti non contrattualizzati dalla scuola dati personali eventualmente incontrati nel corso dell'attività (a maggior ragione se relativi a categorie particolari o a minori) e utilizzare esclusivamente gli strumenti di IA individuati e autorizzati dall'Istituto;
- nella comunicazione con alunni e genitori utilizzare esclusivamente le piattaforme informatiche messe a disposizione dall'Istituto; è vietato l'uso dei social network;
- nell'uso della posta elettronica non aprire allegati di provenienza incerta e controllare accuratamente gli indirizzi dei destinatari prima di inviare messaggi contenenti dati personali;
- per la creazione, lettura o modifica di documenti in locale contenenti dati personali di alunni o genitori, utilizzare esclusivamente le apparecchiature informatiche fornite dalla scuola, in linea con le Misure minime di sicurezza ICT emanate da AgID.

Disposizioni per la gestione degli apparati (ove assegnato l'incarico di gestore dei sistemi)

All'assistente tecnico cui sia assegnato l'incarico di gestore dei sistemi informatici di un laboratorio o dell'intero istituto si applicano, in aggiunta, le seguenti misure:

- gestire le utenze e i profili di accesso secondo il principio del minimo privilegio, attivandoli e disattivandoli tempestivamente in raccordo con la segreteria;
- assicurare l'aggiornamento dei sistemi operativi e degli applicativi (patch di sicurezza) e il corretto funzionamento delle soluzioni di protezione (endpoint);
- effettuare e verificare periodicamente i backup dei dati e testarne il ripristino;
- mantenere un inventario aggiornato dei dispositivi e curare la cancellazione sicura dei dati sui dispositivi dismessi;
- segnalare tempestivamente al Dirigente e al DPO ogni incidente di sicurezza o anomalia rilevata sui sistemi.

Si precisa che il titolare è sempre e comunque responsabile della corretta esecuzione degli adempimenti previsti dal D.Lgs. 196/2003 e dal Regolamento UE 2016/679. Tuttavia, le responsabilità per l'inosservanza delle istruzioni impartite possono riguardare anche i soggetti autorizzati che non rispettino o non adottino le misure necessarie.

IL DIRIGENTE SCOLASTICO
PROF.SSA ALESSANDRA MUCCI
(documento firmato digitalmente ai sensi del CAD)