LINEE GUIDA IN MATERIA DI SICUREZZA PER IL PERSONALE AMMINISTRATIVO AUTORIZZATO AL TRATTAMENTO

Vengono di seguito riportate le norme cui dovrà attenersi il personale amministrativo autorizzato al trattamento dei dati personali, ai sensi del Regolamento UE 2016/679 e del D.Lgs. 196/2003 (come novellato dal D.Lgs. 101/2018). Ulteriori informazioni sulle modalità del trattamento e sulle misure di sicurezza adottate sono contenute nel registro dei trattamenti. Le presenti indicazioni sono coerenti con le "Misure minime di sicurezza ICT per le pubbliche amministrazioni" adottate da AgID.

1. Regole generali di comportamento

- controllare e custodire gli atti e i documenti contenenti dati personali in modo da assicurarne l'integrità e la riservatezza;
- conservare sempre i dati del cui trattamento si è autorizzati nell'apposito armadio assegnato, accertandosi della corretta funzionalità dei meccanismi di chiusura e segnalando tempestivamente eventuali anomalie;
- rendere disponibile all'interessato l'informativa predisposta dal titolare del trattamento (artt. 13 e 14 del Regolamento); si ricorda che l'informativa è un adempimento del titolare e non va redatta caso per caso dall'operatore;
- i trattamenti connessi alle finalità istituzionali della scuola si fondano sull'esecuzione di compiti di interesse pubblico (art. 6, par. 1, lett. e, e art. 9, par. 2, lett. g, del Regolamento; artt. 2-sexies e 2-octies del Codice) e non sul consenso degli interessati; il modulo di consenso va quindi raccolto esclusivamente nei casi residuali in cui il consenso costituisce l'effettiva base giuridica (ad esempio taluni servizi facoltativi o la diffusione di immagini), secondo le indicazioni fornite dal titolare;
- procedere alla raccolta dei dati con la massima cura, verificandone l'esattezza;
- accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per lo svolgimento delle funzioni e dei compiti affidati e per le finalità dell'incarico ricevuto;
- conservare i documenti e gli atti che contengono categorie particolari di dati o dati relativi a condanne penali e reati in archivi (stanze, armadi, schedari, contenitori) chiusi a chiave;
- non fornire telefonicamente o con altri mezzi dati e informazioni relativi a terzi senza una specifica autorizzazione del titolare;

- qualora giungano richieste telefoniche di categorie particolari di dati da parte dell'Autorità Giudiziaria o degli organi di polizia, richiedere l'identità del chiamante e provvedere quindi a richiamare, avendo così certezza sull'identità del richiedente;
- non fornire, anche telefonicamente o per posta elettronica, dati e informazioni ai diretti interessati senza avere la certezza della loro identità;
- nella comunicazione di categorie particolari di dati adottare sempre procedure che garantiscano la sicurezza e la riservatezza delle informazioni, anche mediante tecniche di anonimizzazione e pseudonimizzazione;
- distruggere o rendere comunque illeggibili i documenti cartacei non più utilizzati, specie se contenenti categorie particolari di dati, prima di eliminarli;
- non consentire l'accesso di estranei e di soggetti non autorizzati alle aree in cui sono conservati dati personali su supporto cartaceo o informatico;
- conservare i documenti ricevuti da genitori, studenti o personale in apposite cartelline non trasparenti e consegnare la documentazione in buste non trasparenti;
- effettuare esclusivamente copie (fotostatiche o su supporto informatico) dei documenti per i quali si è autorizzati e non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete, accertandosi che vengano sempre distrutte;
- non lasciare incustodito il registro contenente indirizzi e recapiti del personale e degli studenti e non annotarne il contenuto sui fogli di lavoro;
- non abbandonare la postazione di lavoro senza aver provveduto a custodire in luogo sicuro i documenti trattati, e segnalare tempestivamente al responsabile la presenza di documenti incustoditi provvedendo temporaneamente alla loro custodia;
- attenersi alle direttive ricevute e non effettuare operazioni per le quali non si è stati espressamente autorizzati dal titolare.

2. Trattamento di categorie particolari di dati e di dati relativi a condanne penali e reati

Gli assistenti amministrativi, nello svolgimento delle proprie funzioni, possono venire a conoscenza di dati appartenenti a categorie particolari ai sensi dell'art. 9 del Regolamento (UE) 2016/679 e di dati relativi a condanne penali e reati ai sensi dell'art. 10, quali:

- dati relativi alla salute degli alunni o del personale (certificati medici, documentazione su disabilità, DSA, BES, allergie o intolleranze alimentari, infortuni);
- dati che rivelano convinzioni religiose o filosofiche (ad esempio per esoneri da determinate attività o per richieste particolari delle famiglie);
- dati che rivelano opinioni sindacali o altre informazioni tutelate dalla normativa.

Il trattamento di tali dati:

- è consentito solo nei limiti strettamente indispensabili allo svolgimento dei compiti istituzionali e trova la propria base di liceità negli artt. 2-sexies e 2-octies del Codice (motivi di interesse pubblico rilevante);
- deve avvenire secondo il principio di minimizzazione, evitando raccolte superflue o eccedenti rispetto alla finalità;
- richiede l'adozione di particolari cautele di custodia (armadi chiusi a chiave, archivi informatici protetti da credenziali personali);

- non può comportare la diffusione dei dati né la comunicazione a terzi non autorizzati;
- deve avvenire esclusivamente nell'ambito delle procedure autorizzate dall'Istituto, sotto la responsabilità del Dirigente scolastico.

È fatto assoluto divieto di condividere categorie particolari di dati attraverso canali informali (chat, posta elettronica personale, social network). Eventuali comunicazioni a soggetti esterni (ASL, enti locali, Autorità Giudiziaria) devono sempre essere autorizzate dal Dirigente scolastico e avvenire con canali sicuri.

3. Utilizzo di strumenti di intelligenza artificiale

Nell'utilizzo di strumenti basati sull'Intelligenza Artificiale per attività amministrative, quali la redazione, riformulazione o sintesi di documenti, il personale autorizzato al trattamento deve attenersi alle seguenti indicazioni:

- non utilizzare strumenti di Intelligenza Artificiale non espressamente autorizzati dall'Istituto per lo svolgimento di attività amministrative;
- non inserire dati personali, a maggior ragione se relativi a minori o appartenenti a categorie particolari, nei prompt forniti a strumenti di Intelligenza Artificiale non autorizzati dall'Istituto;
- utilizzare esclusivamente gli eventuali strumenti di Intelligenza Artificiale individuati e autorizzati dall'Istituto, nell'ambito delle finalità e dei casi d'uso espressamente consentiti e nel rispetto delle relative istruzioni;
- qualora l'utilizzo dello strumento sia stato autorizzato, sottoporre sempre il contenuto prodotto dall'Intelligenza Artificiale a rilettura, verifica e validazione da parte dell'operatore, prima del suo utilizzo nell'attività amministrativa;
- verificare che il contenuto prodotto sia corretto, pertinente e coerente con la finalità perseguita e che non contenga dati personali eccedenti o non necessari rispetto alla comunicazione o al procedimento;
- non considerare l'output dell'Intelligenza Artificiale come automaticamente attendibile, mantenendo in capo all'operatore la responsabilità della verifica e della decisione finale.

Nelle more dell'eventuale autorizzazione di specifici strumenti o casi d'uso da parte dell'Istituto, resta fermo il divieto di utilizzare strumenti di Intelligenza Artificiale nello svolgimento delle attività amministrative.

4. Trattamenti eseguiti con strumenti informatici

- utilizzare, per l'accesso ai sistemi informatici, esclusivamente le credenziali di accesso ricevute;
- adottare le necessarie cautele per assicurare la segretezza delle credenziali e la diligente custodia di ogni altro dispositivo di autenticazione (badge, schede, chiavi di sicurezza, ecc.); è fatto divieto di comunicare ad altri le proprie credenziali di accesso;
- utilizzare, ove disponibile, l'autenticazione a più fattori (MFA) messa a disposizione dall'Istituto;
- ogni volta che si abbandoni la postazione di lavoro, porre i PC e i terminali in condizione di non essere utilizzati da estranei, chiudendo le applicazioni in uso e attivando il blocco del sistema mediante password; spegnere sempre il PC alla fine della giornata lavorativa o in caso di assenze prolungate;
- in caso di difformità dei dati trattati o di malfunzionamento degli elaboratori, darne immediata comunicazione al titolare del trattamento e all'amministratore di sistema;

- mantenere attive e aggiornate le soluzioni di protezione (endpoint) fornite dall'Istituto e verificare i file provenienti da fonti esterne secondo le indicazioni dell'amministratore di sistema;
- utilizzare esclusivamente le piattaforme individuate dalla scuola come sicure e da questa nominate responsabili del trattamento, in particolare qualora si rendano necessarie attività lavorative a distanza, secondo le modalità organizzative dell'Istituto e la normativa vigente;
- verificare sempre la corretta modifica e/o cancellazione di dati su documenti, cartelle o informazioni condivise cui si abbia accesso (double check), al fine di evitare modifiche o cancellazioni indesiderate che possano arrecare danno agli interessati o limitare il lavoro dei colleghi;
- nelle comunicazioni via posta elettronica non usare impropriamente il campo CC, che porterebbe indebitamente a conoscenza di tutti i destinatari i relativi indirizzi; utilizzare il campo CCN quando è necessario mantenere riservati gli indirizzi dei destinatari.

5. Scelta e gestione delle parole chiave

- usare una parola chiave di almeno dodici caratteri;
- non inserire nella parola chiave riferimenti facilmente riconducibili all'utente (nome, cognome, data di nascita, numeri di telefono, propri o dei familiari);
- usare una combinazione di caratteri alfabetici e numerici, preferibilmente con almeno un segno di interpunzione o un carattere speciale;
- non riutilizzare la stessa parola chiave su servizi diversi;
- modificare la parola chiave 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 e le buone pratiche vigenti;
- conservare con cura la parola chiave, evitando di trascriverla su fogli posti in vista in prossimità del PC o sulla rubrica dell'ufficio.

6. Segnalazione delle violazioni dei dati personali (data breach)

Qualunque violazione dei dati personali – perdita, sottrazione, accesso non autorizzato, distruzione o divulgazione accidentale o illecita di dati – o anche il semplice sospetto di essa, deve essere segnalata senza ritardo al Dirigente Scolastico e, per il suo tramite, al Responsabile della Protezione dei Dati (DPO), al fine di consentire le valutazioni e gli adempimenti previsti dagli artt. 33 e 34 del Regolamento (eventuale notifica al Garante entro 72 ore e comunicazione agli interessati). La tempestività della segnalazione è essenziale per il rispetto dei termini di legge.

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 dal titolare e/o dai responsabili possono riguardare anche i soggetti autorizzati che non rispettino o non adottino le misure necessarie.

La documentazione relativa alla privacy è disponibile nell'Area privacy del sito istituzionale.ù

Pisa,

Il Dirigente scolastico

Prof. Ssa Francesca Napolitano

Firma autografa sostituita a mezzo stampa ai sensi
e per gli effetti dell'art. 3, c. 2 del D. L.g.s. n. 39/93