ALLEGATO 1

Istruzioni operative per la protezione dei dati personali, la sicurezza delle informazioni e il corretto utilizzo delle tecnologie digitali
Regolamento (UE) 2016/679 - GDPR, D.Lgs. 30 giugno 2003, n. 196, come modificato dal D.Lgs. 10 agosto 2018, n. 101, Regolamento (UE) 2024/1689 (AI Act), Direttiva (UE) 2022/2555 (NIS2), nonché normativa europea e nazionale vigente in materia di protezione dei dati personali, sicurezza delle informazioni, cybersicurezza e utilizzo dell'Intelligenza Artificiale.

1. Premessa

La protezione dei dati personali costituisce uno degli elementi essenziali per il corretto funzionamento dell'Istituzione scolastica e rappresenta un preciso dovere di tutto il personale.

Le istituzioni scolastiche trattano quotidianamente un'ingente quantità di informazioni riferite ad alunni, famiglie, personale dipendente, fornitori, professionisti ed altri soggetti che, per loro natura, richiedono elevati livelli di riservatezza, integrità, disponibilità e sicurezza.

Il personale ATA, nello svolgimento delle proprie attività istituzionali, è autorizzato al trattamento dei dati personali esclusivamente nei limiti delle mansioni assegnate e secondo le istruzioni impartite dal Titolare del trattamento, dal Dirigente Scolastico e dai soggetti formalmente autorizzati.

Le presenti istruzioni costituiscono parte integrante del Piano delle Attività del personale ATA e definiscono le principali misure organizzative, tecniche e comportamentali finalizzate a garantire il corretto trattamento dei dati personali, la sicurezza delle informazioni e la prevenzione degli incidenti informatici.

Il rispetto delle presenti disposizioni costituisce obbligo di servizio.

---

2. Principi generali

Ogni trattamento di dati personali deve essere effettuato nel rispetto dei principi previsti dal Regolamento (UE) 2016/679.

In particolare tutto il personale ATA è tenuto ad operare affinché i dati personali siano trattati:

- esclusivamente per finalità istituzionali;
- nel rispetto della normativa vigente;
- limitatamente ai dati realmente necessari allo svolgimento delle attività affidate;
- con modalità tali da garantirne riservatezza, integrità, disponibilità e correttezza;
- adottando ogni misura idonea ad impedirne la perdita, l'accesso non autorizzato, la divulgazione o l'utilizzo improprio.

Ogni dipendente è personalmente responsabile della corretta gestione delle informazioni alle quali accede nello svolgimento della propria attività lavorativa.

Le informazioni acquisite durante il servizio sono coperte da obbligo di riservatezza anche dopo la cessazione del rapporto di lavoro o il mutamento delle mansioni.

---

3. Regole generali di comportamento

Il personale ATA è tenuto ad osservare le seguenti disposizioni.

3.1 Riservatezza

È vietato comunicare o divulgare dati personali a soggetti non autorizzati.

Le informazioni acquisite durante il servizio non possono essere utilizzate per finalità estranee all'attività istituzionale né essere oggetto di conversazioni in luoghi aperti al pubblico o comunque accessibili a persone non autorizzate.

Particolare attenzione dovrà essere prestata durante i colloqui telefonici, allo sportello e negli ambienti comuni dell'Istituzione scolastica.

3.2 Principio di minimizzazione

Devono essere trattati esclusivamente i dati strettamente necessari allo svolgimento della specifica attività amministrativa.

È vietata la consultazione di fascicoli, registri, banche dati o documenti per finalità diverse da quelle connesse alle mansioni assegnate.

3.3 Custodia della documentazione

I documenti cartacei contenenti dati personali devono essere custoditi con la massima diligenza.

È fatto divieto di:

- lasciare fascicoli incustoditi su scrivanie, banconi o fotocopiatrici;
- abbandonare documenti nelle stampanti;
- lasciare aperti armadi o archivi contenenti documentazione riservata;
- consentire la consultazione di documenti da parte di soggetti non autorizzati.

Al termine dell'attività lavorativa la documentazione deve essere riposta negli archivi, negli armadi o nei cassetti destinati alla conservazione.

3.4 Accesso agli uffici

L'accesso agli uffici amministrativi è consentito esclusivamente al personale autorizzato.

L'eventuale presenza di utenti, fornitori o altri soggetti esterni deve avvenire esclusivamente per il tempo necessario allo svolgimento delle attività di competenza e sotto la vigilanza del personale dell'Istituzione scolastica.

---

4. Utilizzo degli strumenti informatici e sicurezza delle informazioni

L'utilizzo delle dotazioni informatiche e dei servizi digitali dell'Istituzione scolastica costituisce parte integrante dell'attività lavorativa del personale ATA e deve avvenire nel rispetto della normativa vigente, delle misure di sicurezza adottate dall'Amministrazione e delle presenti istruzioni operative.

Tutti gli strumenti informatici assegnati (computer, notebook, tablet, telefoni di servizio, stampanti multifunzione, dispositivi di autenticazione e altri apparati digitali) sono destinati esclusivamente allo svolgimento delle attività istituzionali.

Il personale è tenuto ad utilizzare tali strumenti con diligenza, evitando comportamenti che possano compromettere la sicurezza delle informazioni, l'integrità dei sistemi informatici o la continuità dei servizi amministrativi.

4.1 Credenziali di autenticazione

Le credenziali di accesso ai sistemi informativi costituiscono strumenti strettamente personali.

Il personale è tenuto a:

- custodire con la massima cura le proprie credenziali di autenticazione;
- utilizzare esclusivamente le credenziali personali assegnate;
- evitare qualsiasi forma di comunicazione, cessione o condivisione delle proprie password o dei dispositivi di autenticazione;
- adottare password robuste, conformi alle politiche di sicurezza dell'Istituzione scolastica;
- modificare tempestivamente le credenziali qualora vi sia il sospetto che possano essere state conosciute da soggetti non autorizzati;
- utilizzare, ove prevista, l'autenticazione a più fattori (MFA).

È vietato utilizzare le credenziali di altri utenti, anche con il loro consenso.

4.2 Utilizzo delle postazioni di lavoro

Le postazioni informatiche devono essere utilizzate esclusivamente per finalità istituzionali.

Durante l'attività lavorativa il personale deve:

- verificare che lo schermo non sia visibile a soggetti estranei;
- bloccare la sessione di lavoro in caso di allontanamento, anche temporaneo;
- effettuare il logout dai servizi utilizzati al termine delle attività;
- evitare il salvataggio non necessario di documenti contenenti dati personali sul desktop o in cartelle locali prive di adeguate misure di protezione;
- utilizzare esclusivamente gli spazi di archiviazione e le risorse digitali individuate dall'Istituzione scolastica.

Al termine della giornata lavorativa la postazione deve essere lasciata in condizioni tali da impedire l'accesso ai dati da parte di soggetti non autorizzati.

4.3 Posta elettronica istituzionale

La casella di posta elettronica istituzionale costituisce uno strumento ufficiale di lavoro.

Il personale è tenuto a:

- utilizzare esclusivamente l'indirizzo istituzionale per le comunicazioni inerenti al servizio;
- verificare attentamente l'identità dei destinatari prima dell'invio di documenti contenenti dati personali;
- limitare l'invio dei dati personali a quanto strettamente necessario;
- utilizzare modalità di trasmissione idonee a garantire la riservatezza delle informazioni;
- attenersi alle procedure interne per l'utilizzo della posta elettronica certificata (PEC).

L'invio accidentale di dati personali a destinatari errati deve essere immediatamente segnalato secondo le procedure previste dall'Istituzione scolastica.

4.4 Navigazione Internet

L'accesso ad Internet è consentito esclusivamente per finalità connesse allo svolgimento delle attività istituzionali.

Il personale deve prestare particolare attenzione ai siti visitati, evitando l'accesso a pagine web non pertinenti all'attività lavorativa o potenzialmente idonee a compromettere la sicurezza dei sistemi informatici.

È vietato installare autonomamente programmi, estensioni del browser, applicazioni o software non autorizzati.

4.5 Supporti di memorizzazione

L'utilizzo di dispositivi esterni di memorizzazione (chiavette USB, hard disk esterni, schede di memoria o altri supporti analoghi) deve essere limitato ai casi di effettiva necessità operativa e secondo le procedure adottate dall'Istituzione scolastica.

Qualora tali dispositivi contengano dati personali o informazioni riservate, devono essere custoditi con particolare diligenza e protetti mediante adeguate misure di sicurezza.

In caso di smarrimento o furto del dispositivo, il personale è tenuto a darne immediata comunicazione al Dirigente Scolastico e al Direttore dei Servizi Generali e Amministrativi.

4.6 Servizi cloud e condivisione dei documenti

L'archiviazione e la condivisione dei documenti devono avvenire esclusivamente mediante piattaforme, applicazioni e servizi autorizzati dall'Istituzione scolastica.

È vietato trasferire documenti contenenti dati personali su servizi cloud privati o su piattaforme non autorizzate.

La condivisione dei documenti deve avvenire nel rispetto del principio di necessità, consentendo l'accesso esclusivamente ai soggetti che ne abbiano effettiva esigenza per ragioni di servizio.

4.7 Minacce informatiche

Il personale ATA costituisce il primo presidio di sicurezza dell'Istituzione scolastica.

Particolare attenzione deve essere prestata ai tentativi di:

- phishing;
- smishing;
- vishing;
- social engineering;
- malware;
- ransomware;
- falsificazione dell'identità digitale;
- accessi fraudolenti ai sistemi informativi.

Il personale deve diffidare di messaggi di posta elettronica, SMS, telefonate, QR Code o siti Internet che richiedano l'inserimento di credenziali, dati personali o informazioni riservate senza adeguate garanzie di autenticità.

Qualsiasi anomalia o sospetto tentativo di frode deve essere immediatamente segnalato all'Amministratore di sistema, al Direttore dei Servizi Generali e Amministrativi e al Dirigente Scolastico, evitando qualsiasi iniziativa autonoma che possa aggravare l'incidente.

4.8 Aggiornamenti e sicurezza dei dispositivi

Il personale non può modificare autonomamente le configurazioni di sicurezza delle postazioni di lavoro, disattivare i sistemi antivirus o eludere le misure di protezione predisposte dall'Istituzione scolastica.

Gli aggiornamenti software, gli interventi di manutenzione e le attività di assistenza tecnica devono essere effettuati esclusivamente dal personale autorizzato.

---

5. Utilizzo dei sistemi di Intelligenza Artificiale

L'Intelligenza Artificiale costituisce uno strumento di supporto alle attività amministrative che, se utilizzato correttamente, può contribuire a migliorare l'efficienza dei processi, la qualità dei documenti prodotti e l'organizzazione del lavoro.

Il suo utilizzo deve avvenire nel rispetto della normativa europea e nazionale vigente, dei principi di protezione dei dati personali, sicurezza delle informazioni, trasparenza, riservatezza, segreto d'ufficio, proprietà intellettuale e buon andamento dell'azione amministrativa, nonché delle eventuali disposizioni organizzative adottate dall'Istituzione scolastica.

Le presenti disposizioni costituiscono istruzioni operative rivolte al personale ATA e disciplinano le modalità di utilizzo dei sistemi di Intelligenza Artificiale nell'ambito delle attività istituzionali.

L'impiego di tali sistemi non sostituisce in alcun modo la responsabilità del personale nello svolgimento delle attività istruttorie, nella predisposizione degli atti, nella verifica delle informazioni e nell'adozione delle decisioni di competenza.

In caso di dubbio circa la liceità dell'utilizzo di un sistema di Intelligenza Artificiale o delle modalità del suo impiego, il personale è tenuto ad astenersi dal relativo utilizzo e a richiedere preventivamente indicazioni al Dirigente scolastico o al Direttore dei Servizi Generali e Amministrativi.

5.1 Ambiti di utilizzo consentiti

I sistemi di Intelligenza Artificiale possono essere utilizzati esclusivamente per finalità istituzionali e secondo le modalità eventualmente individuate dall'Istituzione scolastica.

Nel rispetto di tali condizioni, essi possono essere impiegati, a titolo esemplificativo, quale supporto per:

- predisposizione di schemi o bozze di documenti amministrativi;
- revisione linguistica, formale e redazionale dei testi;
- sintesi di documentazione normativa o tecnica;
- elaborazione di schemi, tabelle e prospetti;
- supporto alla progettazione organizzativa;
- attività di formazione e aggiornamento professionale;
- ricerca, raccolta e sistematizzazione di informazioni di carattere generale.

L'utilizzo dell'Intelligenza Artificiale ha carattere esclusivamente ausiliario e non può sostituire l'attività istruttoria, valutativa o decisionale rimessa al personale dell'Istituzione scolastica.

5.2 Utilizzi vietati

È vietato inserire, comunicare, caricare o comunque rendere disponibili in sistemi di Intelligenza Artificiale non autorizzati:

- dati personali relativi ad alunni, famiglie, personale, fornitori, professionisti o altri soggetti;
- categorie particolari di dati personali;
- dati relativi alla salute;
- dati relativi a condanne penali e reati;
- documenti amministrativi riservati o non destinati alla pubblicazione;
- fascicoli personali o parti di essi;
- verbali, relazioni, comunicazioni interne o bozze di provvedimenti contenenti dati identificativi;
- informazioni soggette a segreto d'ufficio o ad obblighi di riservatezza;
- credenziali di autenticazione, codici di accesso o informazioni relative alla sicurezza dei sistemi;
- documenti contrattuali, contabili o gestionali contenenti informazioni riservate;
- ogni altra informazione la cui divulgazione possa arrecare pregiudizio agli interessati o all'Istituzione scolastica.

È inoltre vietato utilizzare sistemi di Intelligenza Artificiale:

- per assumere decisioni amministrative esclusivamente automatizzate;
- per sostituire attività istruttorie, valutative o decisionali attribuite al personale;
- per formulare valutazioni definitive su persone o situazioni individuali;
- per generare o diffondere contenuti falsi, ingannevoli, discriminatori o lesivi della dignità delle persone;
- in violazione della normativa sulla protezione dei dati personali, del diritto d'autore o della proprietà intellettuale;
- mediante account personali o piattaforme private per lo svolgimento di attività istituzionali, salvo diversa autorizzazione dell'Istituzione scolastica.

5.3 Verifica delle informazioni

I contenuti prodotti dai sistemi di Intelligenza Artificiale devono essere sempre sottoposti a verifica da parte dell'operatore prima del loro utilizzo.

Il personale è tenuto ad accertarne:

- l'esattezza delle informazioni;
- la correttezza dei riferimenti normativi;
- l'attualità delle disposizioni richiamate;
- la coerenza con la normativa vigente;
- la conformità alle procedure adottate dall'Istituzione scolastica.

Nessun documento può essere sottoscritto, trasmesso o pubblicato senza una preventiva verifica umana del contenuto generato dal sistema.

5.4 Principio della supervisione umana

L'Intelligenza Artificiale costituisce esclusivamente uno strumento di supporto all'attività lavorativa.

Le decisioni amministrative, le valutazioni discrezionali, l'adozione e la sottoscrizione degli atti restano di esclusiva competenza dei soggetti individuati dalla normativa vigente.

Il personale conserva in ogni caso la piena responsabilità della correttezza, della completezza e della legittimità degli atti e delle attività svolte con il supporto dell'Intelligenza Artificiale.

5.5 Formazione e utilizzo consapevole

L'Istituzione scolastica promuove un utilizzo responsabile, consapevole e sicuro dei sistemi di Intelligenza Artificiale attraverso attività di informazione e formazione rivolte al personale.

Ogni dipendente è tenuto ad utilizzare tali strumenti con spirito critico, consapevolezza dei loro limiti tecnologici e particolare attenzione alla tutela dei dati personali, alla sicurezza delle informazioni e alla qualità dei contenuti prodotti.

Le cinque regole fondamentali

1. Non inserire mai dati personali, informazioni riservate, credenziali o documenti interni in sistemi di Intelligenza Artificiale non autorizzati.
2. Verificare sempre l'esattezza delle informazioni e dei riferimenti normativi prima del loro utilizzo.
3. Mantenere il controllo umano su ogni attività amministrativa e su ogni decisione.
4. Utilizzare esclusivamente gli strumenti eventualmente autorizzati dall'Istituzione scolastica e nel rispetto delle relative disposizioni.
5. Segnalare tempestivamente al Direttore dei Servizi Generali e Amministrativi e al Dirigente scolastico eventuali anomalie, utilizzi impropri o incidenti di sicurezza.

Principio generale: l'Intelligenza Artificiale assiste il personale nello svolgimento delle attività amministrative, ma non ne sostituisce mai la responsabilità. Ogni contenuto prodotto deve essere compreso, verificato e validato dall'operatore prima del suo utilizzo.

---

6. Gestione degli incidenti di sicurezza e delle violazioni dei dati personali (Data Breach)

La tutela dei dati personali e la sicurezza delle informazioni richiedono che ogni evento idoneo a compromettere la riservatezza, l'integrità o la disponibilità dei dati sia tempestivamente individuato e gestito.

Costituisce incidente di sicurezza qualsiasi evento, volontario o accidentale, che possa determinare la perdita, la distruzione, l'alterazione, la divulgazione non autorizzata o l'accesso illecito a dati personali o informazioni riservate trattate dall'Istituzione scolastica.

Il personale ATA è tenuto a collaborare attivamente nella prevenzione, nell'individuazione e nella tempestiva segnalazione di tali eventi.

6.1 Eventi che devono essere immediatamente segnalati

Fermo restando l'obbligo di comunicare qualsiasi situazione anomala, devono essere segnalati senza ritardo, a titolo esemplificativo:

- smarrimento, furto o sottrazione di documenti contenenti dati personali;
- perdita o furto di computer portatili, tablet, telefoni di servizio, supporti di memorizzazione o altri dispositivi utilizzati per finalità istituzionali;
- invio di documenti o messaggi di posta elettronica a destinatari errati;
- accesso accidentale o non autorizzato a fascicoli, archivi o sistemi informativi;
- divulgazione involontaria di dati personali;
- ricezione di messaggi sospetti riconducibili a tentativi di phishing, smishing, vishing o altre forme di frode informatica;
- infezioni da malware, ransomware o altri software malevoli;
- cancellazione accidentale di documenti o banche dati;
- malfunzionamenti che possano compromettere la disponibilità o l'integrità delle informazioni;
- qualsiasi altro evento suscettibile di arrecare pregiudizio ai diritti e alle libertà degli interessati o al corretto funzionamento dell'Istituzione scolastica.

L'elencazione ha carattere esemplificativo e non esaustivo.

6.2 Obbligo di segnalazione

Il personale che venga a conoscenza di un incidente di sicurezza o sospetti il verificarsi di una violazione dei dati personali è tenuto a darne immediata comunicazione al Direttore dei Servizi Generali e Amministrativi e al Dirigente Scolastico ed eventualmente al DPO [Inserire link alla pagina internet con i contatti del DPO: Ing. Sandro Falivene, fornendo tutte le informazioni utili alla valutazione dell'accaduto.

La tempestività della segnalazione costituisce elemento essenziale per consentire all'Istituzione scolastica di adottare le misure tecniche ed organizzative necessarie a limitare le conseguenze dell'evento e ad adempiere agli eventuali obblighi previsti dalla normativa vigente.

L'obbligo di segnalazione sussiste anche qualora il dipendente ritenga che l'evento possa essere stato già comunicato da altri soggetti.

6.3 Comportamenti da adottare

In presenza di un incidente di sicurezza il personale deve:

- interrompere, ove possibile, l'attività che ha determinato o aggravato l'evento;
- preservare documenti, dispositivi e ogni altro elemento utile alla ricostruzione dei fatti;
- evitare iniziative autonome che possano compromettere ulteriormente i sistemi informativi o alterare le evidenze disponibili;
- attenersi esclusivamente alle istruzioni impartite dal Dirigente Scolastico, dal Direttore dei Servizi Generali e Amministrativi e dagli altri soggetti competenti.

È fatto divieto di occultare, minimizzare o omettere la comunicazione di eventi suscettibili di integrare una violazione dei dati personali.

6.4 Valutazione dell'evento

La valutazione circa la natura dell'incidente, la sua qualificazione come violazione dei dati personali (*Data Breach*), l'eventuale notifica al Garante per la protezione dei dati personali e le ulteriori misure da adottare competono esclusivamente al Titolare del trattamento, con il supporto del Responsabile della Protezione dei Dati (RPD/DPO) e degli altri soggetti competenti.

Il personale ATA non è tenuto ad effettuare valutazioni giuridiche sull'evento, ma esclusivamente a garantire la tempestiva segnalazione e la piena collaborazione nelle attività di gestione dell'incidente.

6.5 Cultura della prevenzione

La sicurezza delle informazioni costituisce una responsabilità condivisa da tutto il personale dell'Istituzione scolastica.

Ogni dipendente è tenuto ad operare con diligenza, prudenza e senso di responsabilità, contribuendo alla diffusione di una cultura organizzativa orientata alla prevenzione dei rischi, alla tutela dei dati personali e al continuo miglioramento delle misure di sicurezza adottate dall'Amministrazione.