PROCEDURE PRIVACY PER IL PERSONALE AUTORIZZATO AL TRATTAMENTO DATI

L'autorizzato al trattamento è tenuto a conformarsi alle indicazioni fornite dal Titolare ed alle procedure operative contenute nelle istruzioni e nei documenti privacy consegnati all'incaricato.

A titolo esemplificativo ma non esaustivo si elencano di seguito le procedure da seguire, le misure di sicurezza da adottare ed i divieti da rispettare nel trattamento dei dati personali.

PROCEDURE PER IL TRATTAMENTO DATI:
- fornire sempre l'informativa all'interessato e raccogliere il consenso se previsto, prima di procedere alla raccolta dei dati personali;
-raccogliere i dati con gli strumenti autorizzati dal Titolare e con le modalità indicate;
-verificare l'esattezza, completezza e pertinenza dei dati, salvo espresse deroghe, ed esclusivamente per l'adempimento delle proprie mansioni;
-accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni e conservarli per il periodo di tempo necessario agli scopi per i quali essi sono stati raccolti;
-attenersi scrupolosamente alle policy di cybersecurity contenute nelle istruzioni generali ed operative riguardanti ad esempio la sostituzione della password di accesso con cadenza periodica, il blocco automatico (screen saver) dei pc in assenza dell'operatore della postazione, la crittografia dei dispositivi mobili ecc..;
- adottare le necessarie cautele per assicurare la segretezza della parola chiave per l'accesso alla rete o alle piattaforme;
-custodire diligentemente ogni dispositivo di autenticazione informatica (badge, schede magnetiche, chiavi USB, etc.);
-conservare con cura la password evitando di trascriverla su fogli posti a vista in prossimità del PC o sulla rubrica dell'ufficio;
- effettuare la disconnessione dal proprio account al termine di qualsiasi lavoro tramite un terminale o un dispositivo digitale (log - out);
- controllare e custodire gli atti e i documenti contenenti dati personali in modo da assicurarne l'integrità e la riservatezza e seguire scrupolosamente le procedure inerenti i documenti cartacei per prevenire i data breach, come ad esempio le procedure clean desk e la corretta gestione degli archivi;
-in caso di malfunzionamento dei sistemi informatici compresa la presenza di file malevoli, avvisare tempestivamente il Titolare, il DSGA ed il DPO, seguendo il vademecum per il data breach;
-segnalare tempestivamente la presenza di documenti incustoditi o di supporti di memorizzazione (cd, dvd, pen drive), provvedendo temporaneamente alla loro custodia e alla chiusura dei locali in cui sono conservati;
-procedere alla cancellazione e distruzione degli atti e documenti contenenti dati personali nel rispetto della policy di data retention e del principio di minimizzazione , in modo che i dati personali non siano più visibili o utilizzabili;
-trattare solamente i dati strettamente necessari all'espletamento della mansione;
-effettuare copie cartacee o copie digitali soltanto qualora sia strettamente necessario avendo cura di adottare tutte le misure necessarie previste per la custodia degli originali;
-effettuare copie fotostatiche di documenti con dati particolari nel numero limitato allo scopo, usando le fotocopiatrici posizionate nei locali accessibili ai soli addetti ai lavori;
- aprire gli allegati delle email solo dopo averne accertato la provenienza;
-controllare accuratamente l'indirizzo dei destinatari prima di inviare email contenenti dati personali;
- usare la funzione di invio CCN per le mail collettive, per evitare di evidenziare chi siano gli altri destinatari e quale sia il loro indirizzo di posta elettronica;
- visualizzare la documentazione chiusa a chiave nell'armadio del locale dedicato alla custodia dei documenti contenenti dati particolari riservato agli addetti ai lavori, dopo avere firmato il registro di accesso allo stesso, in presenza del personale di segreteria. A consultazione conclusa gli stessi docenti sono tenuti a restituire la documentazione al personale di segreteria e a firmare nuovamente il registro per l'avvenuta riconsegna della documentazione.

Misure di sicurezza:
-gestire e custodire atti e documenti contenenti dati personali con diligenza durante tutta la sessione lavorativa, avendo cura di riporli in luoghi adatti ad evitare che terzi non autorizzati possano accedervi durante la momentanea assenza dell'autorizzato;
-riporre i documenti in archivi al termine della sessione lavorativa avendo cura di chiuderli a chiave limitando così l'accesso alle sole persone autorizzate;
-custodire le chiavi dei locali, degli armadi e/o degli archivi evitando di cederle a terzi, farne copia, e comunicando tempestivamente l'eventuale smarrimento o il furto al Titolare;
- chiudere a chiave la porta di accesso agli uffici durante la pausa pranzo e sempre a conclusione dell'ultimo turno di lavoro di segreteria;
-utilizzare con diligenza le credenziali di accesso alla rete e /o alla piattaforma fornite dal Titolare, evitando di lasciare incustodito il dispositivo (PC, laptop, Ipad ecc..), considerando che il tempo di attivazione automatica del blocco per inattività è di circa 3/5 minuti;
-custodire le proprie credenziali in luogo sicuro e inaccessibile a terzi;
-notiziare immediatamente il Titolare in caso di perdita, sottrazione di credenziali di accesso o in qualunque caso di attività sospetta ;
-crittografare (es. bitlocker) il contenuto dei supporti di memorizzazione qualora autorizzati per il trattamento dati o supporti di archiviazione (chiavette USB, Hard disk esterni, CD ecc..)
-sostituire la password ogni volta che il sistema ne richieda la modifica o periodicamente secondo le istruzioni di cambio fornite nei documenti privacy (nomina ad incaricato);
-provvedere ad adottare le misure di pulizia dei dati (data wiping) prima del reimpiego dei supporti re-scrivibili, previsti dalla policies per evitare il recupero dei dati da parte di terzi non autorizzati;
-monitorare l'aggiornamento dei software e del sistema operativo delle apparecchiature informatiche , già impostati di default, così da segnalare immediatamente eventuali problemi al Titolare;
-attenersi scrupolosamente alla policy relativa alla sicurezza informatica evitando di aprire email o allegati dall'incerta o pericolosa provenienza, anche se non segnalate automaticamente dall'antivirus;
-accertarsi che al termine delle lezioni o del turno di lavoro, o comunque in caso di assenze prolungate dalla postazione di lavoro i computer siano spenti e che i documenti contenenti dati personali siano stati ricollocati negli appositi armadi e chiusi a chiave.
- conservare i registri cartacei negli armadietti provvisti di serratura;

DIVIETO a tutti gli autorizzati:
-divieto di comunicare a terzi o divulgare qualsiasi dato personale di cui si è venuti a conoscenza durante lo svolgimento della prestazione lavorativa, salvo diversa indicazione del Titolare;
- divieto di fornire telefonicamente o a mezzo elettronico dati personali e informazioni a terzi, senza una specifica autorizzazione del Titolare e, comunque, senza avere la certezza dell' identità dell'interlocutore. Nel caso di richiesta telefonica da parte delle Autorità è necessario richiedere l'identità dell'interlocutore, e la formalizzazione della richiesta tramite pec.
- divieto di comunicare a terzi e/o qualunque altro incaricato le proprie credenziali di autenticazione alla piattaforma;
- divieto di custodire le proprie credenziali in luoghi in luoghi poco sicuri, o accessibili a terzi (es. post it su schermo, o zone comuni);
- divieto di sottrarre o estrarre qualunque dato personale allocandolo in spazi diversi da quelli autorizzati dal Titolare;
- divieto di effettuare operazioni di trattamento non autorizzate;
- divieto di comunicare dati personali salvo espressa previsione di legge o di regolamento;

- divieto di diffondere dati personali, ivi comprese immagini o video, salvo specifica autorizzazione scritta di chi esercita la potestà genitoriale e del Dirigente Scolastico;
- divieto di lasciare a disposizione di estranei documenti o supporti di memorizzazione (cd, dvd, pen drive) che contengono dati personali e/o particolari;
- divieto di lasciare incustoditi registri o fogli contenenti gli indirizzi ed i recapiti telefonici del personale e dei genitori;
- divieto di utilizzare social network quali Facebook, Whatsapp o altri per la pubblicazione e/o la diffusione di dati inerenti gli studenti o per comunicare con le famiglie;
- divieto di inviare via mail messaggi contenenti il nome per esteso di alunni o di qualsiasi persona nei casi di trattamento di dati particolari (alunni con BES, persone seguite dai servizi sanitari, assistenziali, giudiziari, ecc.), avendo cura di indicarli solo con le iniziali;
- divieto di allegare documenti, anche se proveniente da terzi, in cui siano trattati i dati particolari (ad es. i certificati medici) consegnandoli al personale di segreteria incaricato o al Dirigente scolastico in busta chiusa, mettendo in campo tutte le attenzioni necessarie, come ad es. la crittografia.
- divieto di istallare programmi di natura incerta senza essere preventivamente autorizzati dal Titolare;
- divieto di trasportare fuori dal luogo di lavoro atti e documenti contenenti dati personali, salvo il caso di estrema necessità e su autorizzazione del titolare;
- divieto di forzare la disattivazione degli applicativi di sicurezza che consentono una attivazione automatica di un blocco o di altre forme di protezione;
- divieto di utilizzare le stesse password per più account oppure password utilizzate in precedenza;
- divieto di permettere agli alunni l'accesso presso l'aula docenti.

* * *

Si ricorda all'incaricato che l'art 33 del Regolamento UE 2016/679 prevede l'obbligo di notificare al Garante per la protezione dei dati entro 72 ore la "violazione dei dati personali" (data breach), ovvero la distruzione, la modifica o la divulgazione non autorizzata, l'accesso abusivo ai dati e lo smarrimento o il furto di documentazione o di un supporto di memorizzazione contenente dati personali.

Si precisa che l'Istituto Scolastico è sempre e comunque responsabile della mancata esecuzione degli adempimenti previsti dal D.Lgs. n.196/2003 integrato e modificato dal D. Lgl n.101/2018 e dal Regolamento UE 2016/679. Tuttavia, le responsabilità, per l'inosservanza delle istruzioni impartite dal Titolare, possono riguardare anche il personale che non rispetta le istruzioni ricevute o non adotti le misure necessarie per la salvaguardia dei dati personali.

Si chiede pertanto di porre la massima attenzione nel monitorare e rilevare tempestivamente tutte le potenziali e reali violazioni dei dati e di comunicarle immediatamente al Dirigente Scolastico. Si ricorda che la tardiva o omessa notificazione al Garante di una "violazione dei dati personali" è punita con sanzioni pecuniarie di rilevante entità".