REGOLAMENTO INTERNO PRIVACY – UFFICI DI SEGRETERIA

Regole di riservatezza e sicurezza

Non è consentito:

- Portare fuori dai locali scolastici documenti, su qualsiasi supporto, che consentano l'identificazione di soggetti attraverso dati personali, tranne che per le operazioni espressamente autorizzate;
- comunicare i dati personali oggetto di trattamento a soggetti che non risultano essere incaricati;
- utilizzare a proprio vantaggio le informazioni di cui viene a conoscenza nello svolgimento delle sue mansioni;
- fornire informazioni, anche verbali, a terzi senza aver verificato la legittimità della loro richiesta;
- fornire a terzi, non incaricati, elaborazioni di dati personali di sua competenza.

Evitare, inoltre, di discutere, anche con colleghi, di informazioni relative a dati personali.

Regole generali per la sicurezza del trattamento dei dati

- Nessun incaricato può cominciare a trattare dati personali senza un'appropriata formazione;
- assicurarsi che durante le comunicazioni verbali o telefoniche, il cui oggetto siano dati o situazioni che possono consentire l'identificazione di un soggetto, non siano presenti soggetti non incaricati dello stesso trattamento;
- verificare che l'invio via fax di documenti contenenti dati personali, anche sensibili, vada immediatamente a buon fine. Nel dubbio, evitare di utilizzare tale modalità attenendosi alle istruzioni impartite;
- nel caso di custodia di documenti in luoghi accessibili anche da parte di soggetti non incaricati utilizzare le procedure di sicurezza, quali la chiusura chiave di cassetti, armadi, etc.;
- in caso di richiesta verbale, telefonica o scritta di dati personali, accertarsi dell'autorizzazione del richiedente o degli obblighi previsti per legge;
- prima di comunicare via telefono dati personali, accertarsi di non essere ascoltati da terzi estranei;
- qualora ci si trovi a gestire una situazione di rischio non regolamentata nella scuola, occorre rivolgersi al responsabile competente e chiedere ulteriori istruzioni.

Archivi con trattamento manuale.

- Per quanto riguarda i dati personali ordinari e i dati sensibili, la loro classificazione, collocazione, procedure e modalità per l'organizzazione degli archivi occorre far

riferimento all'inventario degli armadi come da **Allegato 1** (UFFICI SEGRETERIA - ARCHIVIAZIONE TRATTAMENTO MANUALE); a tali armadi si accede con chiave in quanto i locali sono praticabili anche dal personale di pulizia.

- Ogni incaricato al trattamento dati è autorizzato ad accedere solo agli archivi di competenza (come da tabella: STRUTTURE PREPOSTE AL TRATTAMENTO E RIPARTO DELLE RESPONSABILITA') e per il tempo necessario al trattamento stesso, avendo cura di riporre i materiali sempre nel luogo della loro conservazione secondo i criteri stabiliti. Durante il trattamento i documenti non dovranno mai essere lasciati incustoditi; durante momenti di pausa riportarli sempre nel luogo della loro conservazione o eventualmente custodirli nei cassetti chiusi con chiave delle proprie scrivanie.
- Per trattare documenti contenenti dati sensibili occorre esplicita autorizzazione del Dirigente Scolastico.
- Documenti con dati sensibili degli alunni (es. diagnosi funzionali, ecc…) possono essere consultati dal personale docente di competenza nell'ufficio della Presidenza o del/la Dirigente dei Servizi Generali e Amministrativi (Segretaria) in sua presenza, sempre e solo previa autorizzazione del Dirigente Scolastico e dopo la compilazione di un modello di richiesta di consultazione nel quale venga esplicitato il fine per il quale i dati verranno consultati. Al termine della consultazione l'addetto di segreteria verificherà che via sia la data, l'ora e firma di riconsegna sul modello precompilato e riporrà la documentazione nell'archivio preposto.
- Fuori dall'orario di servizio del personale di segreteria non è permesso ad alcuno di accedere ai locali ove sono ubicati gli archivi (per l'orario di servizio del personale di segreteria si veda l' **Allegato 2** "ORGANIZZAZIONE DEI SERVIZI AMMINISTRATIVI – RIPARTIZIONE DELLE FUNZIONI E MANSIONI DEL PERSONALE AMMINISTRATIVO ED ORARI).
- In caso di trasferimento ad altro luogo di documenti con dati personali e/o sensibili (su supporto sia cartaceo che digitale), assicurarsi che il trasporto avvenga in regime di sicurezza.
- Eventuali dati personali ordinari affidati dall'incaricato ai docenti per la compilazione dei documenti dovranno essere conservati con cura e restituiti al termine delle operazioni affidate con controfirma su apposito modello.

Archivi con trattamento con elaboratori in rete.

- L'incaricato del trattamento di dati personali con elaboratori elettronici dispone di credenziali di autenticazione (nome utente) che permettono l'identificazione dell'incaricato stesso. Egli deve consegnare, al custode delle password, una busta chiusa contenente la nuova parola chiave elaborata e che ha provveduto a sostituire autonomamente con la prevista periodicità (**trimestrale in caso di trattamento di dati sensibili, semestrale negli altri casi)**;
- il custode delle password deve custodire in cassaforte le buste con le stesse;
- non lasciare visualizzati sullo schermo, in assenza dell'incaricato, dei dati personali, ma utilizzare il sistema di sicurezza della password;
- accertarsi che estranei non possano osservare i dati sullo schermo;
- cancellare sempre tutti i dati residui presenti nel computer, quando non più utilizzati;

- se ci si accorge di aver accesso a dati e programmi di trattamento non di propria competenza, informare subito il titolare o l'amministratore di rete;
- Non utilizzare dischetti, pen drive, cd rom con dati e programmi di provenienza ignota, per evitare infezioni da virus e di danneggiare dati;
- Effettuare con regolarità l'aggiornamento dell'antivirus, meglio se tutti i giorni;
- Al termine del trattamento chiudere sempre i programmi secondo procedura;
- Proteggere i computer, gli apparati terminali ed i supporti di registrazione da condizioni climatiche sfavorevoli;
- Predisporre copie di riserva dei dati (copie di back up) e conservarle in aree sicure; in caso di dati sensibili, le copie di back up devono avere una scadenza almeno settimanale;
- Per quanto riguarda il trasporto di dati personali su supporto informatico occorre che i file vengano preventivamente cifrati con algoritmo crittografico o quantomeno compressi con password; indipendentemente dallo strumento di protezione dei dati, è indispensabile che l'incaricato che li trasporta non li abbandoni, ma si accerti che essi non siano in alcun modo accessibili ad estranei;
- Provvedere almeno annualmente a richiamare gli aggiornamenti periodici dei programmi per elaboratore (es. Windows) per prevenire la vulnerabilità dei sistemi elettronici ("patches"). Almeno ogni sei mesi se si trattano dati sensibili;
- Rispetto all'accesso ad Internet, di cui si deve usufruire solo nei limiti necessari per lo svolgimento dell'attività lavorativa, è tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti d'autore; prima di procedere allo scarico di qualsiasi file e programma, anche a titolo gratuito, si dovrà inoltre chiedere l'autorizzazione all'amministratore di rete.