I.S.I.S.S. "L. EINAUDI – R. MOLARI"
Sede Molari: Via F. Orsini, 19 - 47822 - Santarcangelo di R. (RN)
Sede Einaudi: Via E. Morri, 8 – 47922 – Viserba di Rimini (RN)
Tel. Molari 0541-624658/625051 - Tel. Einaudi 0541-736168
C.F. 91161340400 - Cod. Min. RNIS 006001
E-mail: RNIS006001@istruzione.it
PEC: RNIS006001@pec.istruzione.it
Codice Unico Ufficio: UF92XH

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. Ulteriori informazioni sulla modalità del trattamento dei dati e sulle misure di sicurezza adottate sono contenute nel registro dei trattamenti.

- 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 incaricati in apposito armadio assegnato
- accertarsi della corretta funzionalità dei meccanismi di chiusura dell'armadio, segnalando tempestivamente eventuali anomalie;
- prima di procedere alla raccolta e al trattamento dei dati fornire sempre l'informativa all'interessato o alla persona presso cui si raccolgono i dati;
- consegnare, quando necessario, il modulo per il consenso da parte dell'interessato. Ricevere quindi il modello opportunamente firmato da parte dell'interessato o di chi lo rappresenti;
- occorre procedere alla raccolta dei dati con la massima cura verificando l'esattezza dei dati stessi;
- si può accedere ai soli dati personali, oggetto di trattamento, la cui conoscenza sia strettamente necessaria per lo svolgimento delle funzioni e dei compiti affidati e per le finalità di cui al provvedimento di incarico;
- i documenti o atti che contengono dati sensibili o giudiziari devono essere conservati in archivi (ad esempio stanze, armadi, schedari, contenitori in genere) chiusi a chiave;
- non fornire telefonicamente o a mezzo email dati e informazioni relativi a terzi, senza una specifica autorizzazione del titolare;
- qualora giungano richieste telefoniche di dati sensibili da parte dell'Autorità Giudiziaria o degli Organi di Polizia si deve richiedere l'identità del chiamante. Quindi si provvederà a richiamare avendo così la certezza sull'identità del richiedente;
- non fornire, anche telefonicamente o per mail, dati e informazioni ai diretti interessati senza avere la certezza della loro identità;

- nella comunicazione di dati sensibili adottare sempre procedure che permettano di garantire la sicurezza e la riservatezza delle informazioni anche mediante tecniche di anonimizzazione e di pseudonimizzazione;
- i documenti cartacei non più utilizzati, specie se sensibili, devono essere distrutti o comunque resi illeggibili, prima di essere eliminati o cestinati;
- non consentire l'accesso alle aree in cui sono conservati dati personali su supporto cartaceo a estranei e a soggetti non autorizzati;
- conservare i documenti ricevuti da genitori/studenti o dal personale in apposite cartelline non trasparenti;
- consegnare al personale o ai genitori/studenti documentazione inserita in buste non trasparenti;
- non consentire l'accesso a estranei ad aree in cui sono custoditi documenti cartacei o contengano supporti informatici di memorizzazione;
- effettuare esclusivamente copie fotostatiche o su supporto informatico di documenti per i quali si è autorizzati;
- non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o sensibili ma accertarsi che vengano sempre distrutte;
- non lasciare incustodito il registro contenente gli indirizzi e i recapiti telefonici del personale e degli studenti e non annotarne il contenuto sui fogli di lavoro;
- non abbandonare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati;
- segnalare tempestivamente al Titolare la presenza dì 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.

Trattamento di dati sensibili

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, quali:

- dati relativi alla salute degli alunni o del personale (certificati medici, documentazione disabilità, DSA, BES, allergie o intolleranze alimentari, infortuni);
- dati che rivelano convinzioni religiose o filosofiche (ad esempio per esoneri da determinate attività o 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;

- 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 all'interno delle procedure autorizzate dall'Istituto, sotto la responsabilità del Dirigente scolastico.

È fatto assoluto divieto di condividere dati sensibili attraverso canali informali (chat, e-mail personali, social network).
Eventuali comunicazioni a soggetti esterni (ASL, enti locali, autorità giudiziaria) devono sempre essere autorizzate dal Dirigente scolastico e avvenire con canali sicuri.

Riguardo ai trattamenti eseguiti con supporto informatico attenersi scrupolosamente alle seguenti indicazioni:

- per l'accesso al sistema informatico utilizzare le credenziali di accesso ricevute;
- adottare le necessarie cautele per assicurare la segretezza della parola chiave e la diligente custodia di ogni altro dispositivo di autenticazione informatica (badge, schede magnetiche, chiavi USB, etc.);
- è fatto divieto comunicare a qualunque altro incaricato le proprie credenziali di accesso al sistema informatico;
- la parola chiave deve essere modificata almeno ogni tre mesi;
- tutte le volte che si abbandoni la propria postazione di lavoro i pc e/o i terminali devono essere posti in condizione di non essere utilizzati da estranei. In particolare si raccomanda di chiudere tutte le applicazioni in uso e di porre un blocco del sistema mediante password;
- spegnere sempre il PC alla fine della giornata lavorativa o in caso di assenze prolungate dalla postazione di lavoro;
- qualora si dovessero riscontrare difformità dei dati trattati o nel funzionamento degli elaboratori occorre darne immediata comunicazione al titolare del trattamento;
- utilizzare l'antivirus per la verifica di ogni documento trattato o di qualunque file scaricato da Internet;
- utilizzare sempre l'antivirus per verificare il contenuto di qualunque supporto di memorizzazione sospetto;
- aggiornare con frequenza l'antivirus.
- utilizzare esclusivamente le piattaforme identificate dalla scuola come sicure e nominate dalla stessa responsabili del trattamento, specie qualora si renda necessario effettuare delle attività lavorative a distanza, come previsto dalle modalità organizzative della scuola e dalla normative vigente;

- verificare sempre la corretta modifica e/o cancellazione di dati su documenti, cartelle o informazioni condivise alle quali si abbia accesso nell'esercizio delle proprie funzioni (double check), al fine di evitare modifiche o cancellazioni indesiderate che possano arrecare danno agli interessati o limitare le possibilità di lavoro di colleghi;
- nelle comunicazioni via mail assicurarsi di non usare impropriamente il campo CC con la conseguenza di portare indebitamente a conoscenza di tutti i destinatari del messaggio i relativi indirizzi email (usare invece il campo CCN se è necessario tenere riservati gli indirizzi email di coloro che sono coinvolti nella comunicazione).

Regole per la scelta delle parole chiave

- usare una parola chiave di almeno dodici caratteri;
- la parola chiave non deve contenere riferimenti facilmente riconducibili all'incaricato (come per esempio nome, cognome, data di nascita, numeri di telefono, etc. propri o dei propri familiari);
- usare una combinazione di caratteri alfabetici e numerici, meglio se contenente almeno un segno di interpunzione o un carattere speciale;
- conservare con cura la parola chiave evitando di trascriverla su fogli posti in vista in prossimità del PC o sulla rubrica dell'ufficio.

Si precisa che il titolare è sempre e comunque responsabile della mancata esecuzione degli adempimenti previsti dal D.lgs. n.196/2003 e del Regolamento UE 2016/679. Tuttavia le responsabilità, per l'inosservanza delle istruzioni impartite dal Titolare e/o dai responsabili, possono riguardare anche gli incaricati, che non rispettino o non adottino le misure necessarie.

La Dirigente scolastica

Daniela Massimiliani