Prot 4468/c19
Perugia 8 settembre 2015

LINEE GUIDA IN MATERIA DI SICUREZZA PER L'ASSISTENTE AMMINISTRATIVO INCARICATO DEL TRATTAMENTO

Vengono di seguito riportate le norme cui dovrà attenersi il personale amministrativo incaricato del trattamento dei dati personali e sensibili.

- 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 al Responsabile 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 e farsi restituire 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 e in busta chiusa con la dicitura contiene dati sensibili;
- Non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Responsabile;
- 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 telefonicamente o a mezzo fax dati e informazioni ai diretti interessati senza avere la certezza della sua identità;
- evitare di inviare per fax documenti in chiaro contenenti dati sensibili
- 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 al fax e alla stampante che contengano documenti non ancora ritirati dal personale:
- Effettuare esclusivamente copie fotostatiche 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 Responsabile 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 Responsabile o dal Titolare

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

- per l'accesso al sistema informatico utilizzare le parole chiave definite dal Responsabile della gestione e della manutenzione del sistema informatico e alle quali sono associati le relative autorizzazioni
- 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.)
- E' fatto divieto comunicare a qualunque altro incaricato le proprie credenziali di accesso al sistema informatico
- la parola chiave, che viene assegnata dal responsabile del trattamento o dal Responsabile della gestione e della manutenzione del sistema informatico, deve essere modificata almeno ogni sei mesi (tre mesi nel caso di dati sensibili)
- 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 Responsabile del Trattamento;
- i supporti informatici, già utilizzati per il trattamento dei dati sensibili e giudiziari, possono essere riutilizzati solo se le informazioni precedentemente contenute non sono più in alcun modo recuperabili, dovendo altrimenti essere distrutti;
- 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 e comunicare al Responsabile della gestione e della manutenzione del sistema informatico ogni problema a riguardo

Ove l'antivirus riscontri la presenza di un virus informatico informare il Responsabile del trattamento ed il Responsabile della gestione e della manutenzione del sistema informatico

- Non installare sui PC alcun software senza l'autorizzazione del Responsabile del trattamento e del Responsabile della gestione e della manutenzione del sistema informatico.
- E' vietato modificare le impostazioni effettuate sul sistema dal Responsabile della gestione e della manutenzione del sistema informatico

Regole per la scelta delle parole chiave

- 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.

Protocollo e Posta

La posta in entrata e in uscita va sempre protocollata.

Fanno eccezione riviste, gazzette e bollettini ufficiali, pubblicità

Ogni giorno la posta va portata alla firma del DS (o suo sostituto) e del DSGA (o suo sostituto)

Laddove il DS apponesse di inoltrare la posta a figure particolari (es FF.SS. Coordinatori, Fiduciari) va immediatamente fatto o dandone una copia alla persona interessata e facendo apporre sull'originale la firma di consegna o inviando via mail con ricevuta di consegno

La posta contenente sulla busta “dati sensibili”, “riservato”, non va aperta ma consegnata direttamente al DS
La posta indirizzata esclusivamente al personale non va aperta, ma consegnata allo stesso protocollando in entrata, apponendo il protocollo sulla busta chiusa, facendone una copia e facendo firmare all’interessato la copia per consegna
Eventuali plichi inerenti gare/appalti NON vanno mai aperti; il protocollo va apposto sulla busta e vanno consegnati al DS

Si precisa che in base alla legge sulla privacy il Titolare è sempre e comunque responsabile della mancata esecuzione degli adempimenti previsti dal D.Lgs. n.196/2003, in materia di sicurezza. 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.

F.to Il Dirigente Scolastico

Prof.ssa Francesca Volpi

_____

-