PRIVACY - LINEE GUIDA IN MATERIA DI SICUREZZA PER GLI ASSISTENTI AMMINISTRATIVI INCARICATI DEL TRATTAMENTO DATI – EX D.LGS. N. 196/2003 E REGOLAMENTO UE 2016/679 IN VIGORE DAL 25/5/2018.

in relazione alle operazioni di elaborazione di dati personali, su supporto cartaceo e/o elettronico, ai quali gli Assistenti Amministrativi hanno accesso nell'espletamento delle funzioni e dei compiti assegnati nell'ambito del rapporto di lavoro e disciplinati dalla normativa in vigore e dai contratti di settore, gli Assistenti Amministrativi sono incaricati delle operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modifica, comunicazione, selezione, estrazione di dati, connesse alle seguenti funzioni e attività dalle SS.LL esercitate (nei soli casi autorizzati dal titolare o dal responsabile del trattamento). il Direttore dei Servizi Generali ed Amministrativi, nel proporre quanto previsto nel presente piano, prospetta al personale ATA, tutto per norma, gli standard di qualità che bisogna assicurare :

1. i dati personali, oggetto dei trattamenti, devono essere esatti ed aggiornati, inoltre devono essere pertinenti, completi e non eccedenti le finalità per le quali vengono raccolti e trattati;
2. è vietata qualsiasi forma di diffusione e comunicazione dei dati personali trattati che non sia strettamente funzionale allo svolgimento dei compiti affidati e autorizzata dal responsabile o dal titolare del trattamento, si raccomanda particolare attenzione al tutela del diritto alla riservatezza degli interessati (persone fisiche a cui afferiscono i dati personali);
3. si ricorda che l'obbligo di mantenere la dovuta riservatezza in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico, deve permanere in ogni caso, anche quando sia venuto meno l'incarico stesso;
4. i trattamenti andranno effettuati rispettando le misure di sicurezza predisposte nell'istituzione scolastica; in ogni operazione di trattamento andrà garantita la massima riservatezza e custodia degli atti e dei documenti contenenti dati personali che non andranno mai lasciati incustoditi o a disposizione di terzi non autorizzati ad accedervi, prendervi visione o ad effettuare qualsivoglia trattamento;
5. le eventuali credenziali di autenticazione (codice di accesso e parola chiave per accedere ai computer e ai servizi web) attribuite alle SS.LL sono personali e devono essere custodite con cura e diligenza; non possono essere messe a disposizione né rivelate a terzi; non possono essere lasciate incustodite, né in libera visione. in caso di smarrimento e/o furto, bisogna darne immediata notizia al responsabile (o, in caso di assenza del responsabile, al titolare) del trattamento dei dati;
6. nel caso in cui per l'esercizio delle attività sopra descritte sia inevitabile l'uso di supporti rimovibili (quali ad esempio chiavi usb, cd-rom, ecc), su cui sono memorizzati dati personali, essi vanno custoditi con cura, né messi a disposizione o lasciati al libero accesso di persone non autorizzate;
7. si ricorda inoltre che l'accesso agli archivi contenenti dati sensibili o giudiziari è permesso solo alle persone autorizzate e soggetto a continuo controllo secondo le regole definite dallo scrivente;
8. durante i trattamenti i documenti contenenti dati personali vanno mantenuti in modo tale da non essere alla portata di vista di persone non autorizzate;
9. al termine del trattamento occorre custodire i documenti contenenti dati personali all'interno di archivi/cassetti/ armadi muniti di serratura;
10. i documenti della scuola contenenti dati personali non possono uscire dalla sede scolastica, né copiati, se non dietro espressa autorizzazione del responsabile o dal titolare del trattamento;
11. in caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati, l'incaricato dovrà verificare che non vi sia possibilità da parte di terzi, anche se dipendenti non incaricati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento;

12. le comunicazioni agli interessati (persone fisiche a cui afferiscono i dati personali) dovranno avvenire in forma riservata, se effettuate per scritto dovranno essere consegnate in contenitori chiusi;
13. all'atto della consegna di documenti contenenti dati personali l'incaricato dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta.
14. in caso di comunicazioni elettroniche ad alunni, colleghi, genitori, personale della scuola o altri soggetti coinvolti per finalità istituzionali, queste (comunicazioni) vanno poste in essere seguendo le indicazioni fornite dall'istituzione scolastica e avendo presente la necessaria riservatezza delle comunicazioni stesse e dei dati coinvolti

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

A. non lasciare dispositivi di archiviazione (supporti usb/hard disk esterni, ecc.), cartelle o altri non salvare file o cartelle nel desktop.
B. documenti a disposizione di estranei;
C. conservare i dati sensibili in armadi chiusi, ad accesso controllato o in files protetti da password;
D. non consentire l'accesso ai dati a soggetti non autorizzati;
E. riporre i supporti in modo ordinato negli appositi contenitori e chiudere a chiave classificatori e armadi dove sono custoditi;
F. scegliere una password con le seguenti caratteristiche:

- ✓ originale
- ✓ composta da almeno otto caratteri alfanumerici
- ✓ che non sia facilmente intuibile, evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili.
- ✓ curare la conservazione della propria password ed evitare di comunicarla ad altri;
- ✓ cambiare periodicamente (almeno una volta ogni tre mesi) la propria password;
- ✓ modificare prontamente (ove possibile) la password assegnata dal custode delle credenziali;
- ✓ trascrivere su un biglietto chiuso in busta sigillata e controfirmata la nuova password e consegnarla al custode delle credenziali;
- ✓ spegnere correttamente il computer al termine di ogni sessione di lavoro;
- ✓ non abbandonare la propria postazione di lavoro per la pausa o altri motivi senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
- ✓ comunicare tempestivamente al titolare o al responsabile qualunque anomalia riscontrata nel funzionamento del computer;
- ✓ non riutilizzare i supporti informatici utilizzati per il trattamento di dati sensibili per altri trattamenti;
- ✓ non gestire informazioni su più archivi ove non sia strettamente necessario e comunque
- ✓ curarne l'aggiornamento in modo organico.