



ISTITUTO COMPRENSIVO

"Gian Giacomo Ciaccio Montalto"

Via Tunisi, 37 - 91100 TRAPANI – Tel 0923 20398 Telefax 0923 20106

CF: 80004160810 - C.M.: TPIC836004

e-mail tpic836004@istruzione.it – PEC tpic836004@pec.istruzione.it

www.icciacciomontalto.gov.it

Prot. n. 1163/C2

Trapani, 07/02/2018

Al personale di Segreteria

Al Sito Web

E p.c. **Al Dirigente Scolastico
dell'I.C. "G.G. Ciaccio Montalto"
Trapani**

Oggetto: Nomina Incaricati del trattamento dei dati personali - Assistenti Amministrativi.

IL DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI

- In qualità di Responsabile del trattamento dei dati personali dell'Istituzione scolastica;
- Ai sensi degli art. 29 e 30 del Codice in materia di protezione dei dati personali D.Lgs. 196/03;
- Tenuto conto del ruolo funzionale svolto dalle SS.LL. nell'istituzione scolastica ai sensi della Tabella A, area B del vigente CCNL del Comparto scuola;
- Considerato che, nell'ambito di tali mansioni, le SS.LL. compiono attività che possono comprendere il trattamento dei dati personali;
- Visto il Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione emanato con Decreto Ministeriale n.305 del 07/12/2006;

NOMINA le SS.LL.

INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI

Le SS.LL. sono, pertanto, autorizzate all'accesso e al trattamento dei dati personali di tutti i soggetti con i quali l'istituzione scolastica entra in relazione per i suoi fini istituzionali, nella misura e nei limiti previsti dalle mansioni assegnate, dagli ordini di servizio ricevuti e dalle istruzioni ivi contenute e nel rispetto del Testo Unico e del Regolamento citati nelle premesse.

In particolare, alle SS.LL. è affidato l'incarico di trattare i dati personali relativi all'area di assegnazione risultante dal Piano delle attività e dagli ordini di servizio.

Istruzioni specifiche sul trattamento dei dati

Nello svolgimento dell'incarico le SS.LL. avranno accesso ai dati personali gestiti da questa istituzione scolastica e dovranno attenersi alle seguenti istruzioni, ai sensi dell'art. 11 del D.Lgs. 196/2003:

- Trattare i dati personali in modo lecito e secondo correttezza;
- Raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi, ed utilizzarli in altre operazioni del trattamento in termini compatibili con tali scopi;
- Verificare che siano esatti e, se necessario, aggiornarli;
- Verificare che siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;

- Conservarli in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
- Comunicare o eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati e riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute;
- Non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale
- Informare prontamente il Titolare e il Responsabile del trattamento di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi;
- Informare prontamente il Titolare e il Responsabile del trattamento qualora si verificasse la necessità di porre in essere operazioni di trattamento di dati personali per finalità o con modalità diverse da quelle risultanti dalle istruzioni ricevute, nonché di ogni istanza di accesso ai dati personali da parte di soggetti interessati e di ogni circostanza che esuli dalle istruzioni impartite alle SS.LL.;
- Accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni;
- Accertarsi dell'identità degli interessati e della loro autorizzazione al trattamento e dell'eventuale autorizzazione scritta a terzi, al momento del ritiro di documentazione in uscita;
- Non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Titolare o del Responsabile del trattamento;
- Non fornire telefonicamente o a mezzo fax dati e informazioni ai diretti interessati, senza avere la certezza della sua identità;
- Relazionarsi e collaborare con gli altri incaricati del trattamento dei dati, attenendosi alle indicazioni fornite e provvedendo, a propria volta, a dare indicazioni esaustive in caso di coinvolgimento di altri incaricati nei trattamenti effettuati;
- Rispettare ed applicare le misure di sicurezza idonee a salvaguardare la riservatezza e l'integrità dei dati, indicate nelle allegate "Linee guida in materia di sicurezza" elaborate ai sensi dell'art. 31 del D.lgs 196/2003;
- Seguire le attività di formazione organizzate dall'Istituzione scolastica per gli incaricati del trattamento dati;

Istruzioni specifiche sul trattamento dei dati sensibili e giudiziari

Le SS.LL., relativamente ai dati sensibili e giudiziari, nel caso in cui siano coinvolte nel loro trattamento, si atterranno alle specifiche istruzioni impartite dal Titolare, dal Responsabile e dagli Incaricati dei trattamenti stessi.

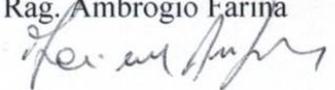
La presente nomina di Incaricato al trattamento dei dati personali è a tempo indeterminato e può essere revocata in qualsiasi momento dal Titolare o dal Responsabile del trattamento dei dati personali senza preavviso.

La presente nomina si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa Istituzione scolastica, per trasferimento ad altra istituzione o cessazione del rapporto di lavoro. Successivamente a tale data, le SS.LL. non saranno più autorizzate ad effettuare alcun tipo di trattamento di dati per conto di questa Istituzione scolastica.

Qualunque violazione delle modalità sopra indicate e delle linee guida consegnate con la presente dà luogo a precise responsabilità, ai sensi delle norme contenute nel D.Lgs 196/03.

In allegato:

- linee guida in materia di sicurezza per l'Assistente Amministrativo incaricato del trattamento.

Il Direttore S.G.A.
 Rag. Ambrogio Farina


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. Ricevere quindi il modello opportunamente firmato da parte dell'interessato o di chi lo rappresenta;
- Procedere alla raccolta dei dati con la massima cura, verificando l'esattezza dei dati stessi;
- 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;
- Conservare in archivi chiusi a chiave (stanze, armadi, schedari, contenitori in genere, etc.) documenti o atti che contengono dati sensibili o giudiziari;
- Non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Responsabile o del Titolare del trattamento;
- Richiedere l'identità del chiamante qualora giungano richieste telefoniche di dati sensibili da parte dell'Autorità Giudiziaria o degli organi di polizia; 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 loro identità;
- Evitare di inviare per fax documenti in chiaro contenenti dati sensibili;
- I documenti cartacei non più utilizzati, specialmente se contenenti dati 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 o al Titolare del trattamento la presenza di 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 del trattamento.

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 associate 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 di 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);

- La parola chiave deve essere chiusa in una busta opaca, sigillata e controfirmata sui lembi, da consegnare all'Incaricato della custodia delle copie delle credenziali, che ne curerà la conservazione;
- In caso di necessità, il Responsabile o l'Incaricato della custodia delle copie delle credenziali hanno la possibilità, previa comunicazione all'incaricato, di aprire la busta per esigenze operative o di organizzazione. L'incaricato nel tal caso provvederà a sostituire la parola chiave violata;
- 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;
- Spegner 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

- usare una parola chiave di almeno otto caratteri, oppure, nel caso in cui lo strumento elettronico non lo permetta, costituita da un numero di caratteri pari al massimo consentito;
- 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 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 dal Responsabile, possono riguardare anche gli incaricati che non rispettino o non adottino le misure necessarie.