Ministero dell'Istruzione, dell'Università e della Ricerca -Ufficio Scolastico Regionale per il Lazio
ISTITUTO COMPRENSIVO "NELSON MANDELA"
Scuola dell'infanzia, scuola primaria, scuola secondaria di 1° grado
Via dei Torriani, 44 – 00164 Roma Tel. 0666000349 – Fax 0666040665
Distretto Scolastico XXIV- Codice meccanografico RMIC8FW00E - Codice fiscale 97712890587
E-mail RMIC8FW00E@ISTRUZIONE.IT posta certificata: RMIC8FW00E@PEC.ISTRUZIONE.IT
Sito web: www.icviatorriani.it

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

Attenersi scrupolosamente alle seguenti indicazioni per garantire la sicurezza dei dati personali e, in particolare, dei dati sensibili e giudiziari:

- 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, dotato di adeguata chiusura;
- accertarsi della corretta funzionalità dei meccanismi di chiusura dell'armadio, segnalando tempestivamente al Responsabile eventuali anomalie;
- non consentire l'accesso alle aree in cui sono conservati dati personali su supporto cartaceo a estranei e a soggetti non autorizzati;
- 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 conservare i documenti ricevuti da genitori/studenti o dal personale in apposite cartelline non trasparenti;
- provvedere personalmente a distruggere o rendere illeggibili i documenti cartacei non più utilizzati, specie se contenenti dati sensibili,prima che siano eliminati o cestinati
- 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
- 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 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

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

- non lasciare floppy disk, pen drive, CD-Rom, cartelle o altri documenti a disposizione di estranei;
- conservare i dati sensibili in armadi chiusi, ad accesso controllato o in files protetti da password;
- non consentire l'accesso ai dati a soggetti non autorizzati;
- riporre i supporti in modo ordinato negli appositi contenitori e chiudere a chiave classificatori e armadi dove sono custoditi;

- 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.);
- è 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);
- 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;
- 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.
- scegliere una password con le seguenti caratteristiche:
    - originale
    - composta da otto caratteri
    - che contenga almeno un numero
    - 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;
- utilizzare le seguenti regole per la posta elettronica:
    - non aprire documenti di cui non sia certa la provenienza
    - non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus
    - inviare messaggi di posta solo se espressamente autorizzati dal Responsabile
    - controllare accuratamente l'indirizzo dei destinatario prima di inviare dati personali

IL DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI
Responsabile del trattamento dati
(Nicolina Piluso)