Ministero dell'Istruzione, dell'Università e della Ricerca

ISTITUTO COMPRENSIVO DI VIA COMMERCIALE
Scuola dell'Infanzia R. Manna e F. Tomizza, Primaria R. Manna e V. Longo
e Secondaria di primo grado G. Corsi

Li 04/02/2022

Alla prof.ssa Annalisa Ameruoso
Alla DSGA
Al fascicolo personale

OGGETTO: Nomina incaricato al trattamento dei dati personali. Atto di designazione ai sensi degli artt. 29 e 32 del GDPR – Regolamento UE 2016/679

Spettabile prof.ssa Annalisa Ameruoso

con il presente atto il Dirigente Scolastico dott. Roberto Benes, in qualità di Legale Rappresentante dell'I.C. di via Commerciale, effettua la designazione della S.V. in qualità di incaricato del trattamento dei dati in relazione ai dati necessari al fine dell'espetamemto delle attività Istituzionali di incaricato/ responsabile della biblioteca della scuola. La fonte legale dell'utilizzo di tali dati ed il limite al loro utilizzo stesso risiede nel D.lgs 196/2003 all'art. 2 ter inserito dal D.lgs 101/18.
La nomina è effettuata in ottemperanza a quanto previsto dagli artt. 29 e 32 del Regolamento UE 2016/679.

OGGETTO della nomina:

Oggetto delle nomina è il trattamento dei dati personali degli alunni (nome, cognome, classe, raccolta di dati sulla restituzione dei libri e dei libri letti, eventuale raccolta di recensioni nominali in merito ai libri letti), finalizzato al servizio di prestito bibliotecario.

La S.V. potrà accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere i compiti assegnati in ragione del proprio ufficio e si asterrà in ogni caso dal compiere attività di trattamento che comportino un accesso ed una conoscenza di informazioni superiore rispetto all'ambito di trattamento dei dati attribuitogli.
La S.V. incaricata sarà tenuta a frequentare corsi di formazione e di aggiornamento sulle procedure e sui sistemi di sicurezza organizzativi, logici e fisici atti a tutelare il trattamento, la conservazione e l'integrità dei dati personali affidatigli per il trattamento.

Le fornisco inoltre le seguenti istruzioni da seguire in tutte le operazioni di trattamento dei dati :

1. comunicare tempestivamente al Dirigente Scolastico e al Responsabile della protezione dei dati (contattabile alla mail giancarlo.favero@capitalsecurity.it e al numero 335-5950674) qualsiasi evento di tipo "violazione dei dati personali", anche nel caso non ve ne sia la certezza ma solo il sospetto (es. manomissione di serrature, accesso abusivo a sistema informatico o telematico etc.);
2. eseguire esclusivamente i trattamenti di dati personali e sensibili indispensabili allo svolgimento dei compiti assegnati e delle responsabilità affidate, e raccogliere e trattare i soli dati personali o sensibili la cui conoscenza e gestione sia strettamente necessaria per lo svolgimento dei compiti assegnati, applicando sempre i principi di necessità, liceità, correttezza, non eccedenza e proporzionalità in tutte le operazioni di trattamento dei dati;
3. essere consapevole del fatto che, nell'espletamento delle proprie funzioni, può venire a conoscenza di dati personali e/o sensibili riguardanti i c.d. interessati (alunni, docenti, genitori, collaboratori, persone giuridiche, pubbliche amministrazioni, enti, associazioni, organismi, etc.). In questi casi, Lei è tenuta ad impegnarsi ad operare con serietà, correttezza e scrupolo, affinché detti dati siano gestiti in maniera corretta e riservata, nel rispetto della privacy e della dignità degli interessati, in ottemperanza con quanto prescritto dal GDPR – Regolamento UE 2016/679;
4. in merito a tutti i dati, fatti e notizie acquisite nell'ambito dell'Istituto è necessario mantenere una condotta equipollente al segreto professionale e al segreto d'ufficio; si ricorda che la violazione del segreto d'ufficio è punibile con la reclusione fino a tre anni e con l'obbligo, ai sensi dell'art. 2050 del Codice Civile, di risarcire il danno eventualmente causato come conseguenza della violazione del segreto d'ufficio e più in generale come conseguenza del trattamento;
5. non trasmettere, comunicare, diffondere e comunque portare a conoscenza dati personali o sensibili a soggetti esterno all'Istituto. L'eventuale comunicazione di dati a soggetti ben identificati esterni all'Istituto, dovrà di volta in volta essere autorizzata per iscritto dal Dirigente Scolastico;
6. informare prontamente il Dirigente Scolastico o il Responsabile della protezione dei dati in caso di richieste anomale, dubbi sulla condotta da tenere e incidenti, anche potenziali, che possano compromettere la sicurezza dei dati trattati e la privacy dei soggetti interessati, con particolare cura e riferimento ai dati sensibili degli alunni;
7. eseguire le operazioni di trattamento dei dati personali al riparo da sguardi indiscreti e comunque evitando accessi e conoscenza, anche fortuita, da parte di personale non autorizzato;
8. evitare nel modo più assoluto di lasciare abbandonati o incustoditi, anche per breve tempo, atti o documenti od apparati contenenti dati personali o sensibili;
9. procedere alla distruzione dei documenti in maniera tale da rendere illeggibile il documento; prestare particolare attenzione all'eventuale utilizzo di carta già utilizzata in precedenza (carta c.d. "riciclata");
10. impegnarsi a non soddisfare richieste di conoscenza o accesso ai dati personali o ai dati sensibili, nel caso in cui non sia chiara ed evidente la liceità delle richieste stesse e nel caso in cui le richieste siano formulate tramite telefono o posta elettronica;
11. essere consapevole che le tutte le risorse, in particolare quelle informatiche, telematiche e telefoniche, delle quali l'Istituto Le concede temporaneamente l'utilizzo, sono di proprietà esclusiva

dell'Istituto e devono essere utilizzate per fini strettamente lavorativi, e assolutamente non per scopi diversi né tanto meno per fini personali. In particolare la casella di posta ed il collegamento ad Internet devono essere considerati strumenti di lavoro, per cui Lei sarà responsabile del corretto, economico ed efficace utilizzo degli stessi e deve essere consapevole che il Dirigente Scolastico potrà effettuare in qualsiasi momento ispezioni e controlli per verificare che l'utilizzo sia conforme alle presenti prescrizioni e non avvenga in violazione di norme, leggi o regolamenti;

12. mettere in atto e rispettare le prescrizioni del ***Regolamento per il corretto utilizzo di Internet, della posta elettronica e degli strumenti informatici e telematici***;
13. per quanto riguarda il collegamento ad Internet, è fatto esplicito divieto di:
    a. visitare siti che non siano chiaramente riconducibili all'espletamento di attività lavorative istituzionali
    b. visitare siti a contenuto pornografico o pedo-pornografico
    c. visitare siti di hacker
    d. scaricare contenuti multimediali come musica, canzoni, film, brevi filmati o sequenze
    e. condividere o offrire in condivisione contenuti di qualsiasi tipo mediante applicazioni di tipo "peer-to-peer"
    f. modificare le configurazioni del browser, in particolare quelle relative alla privacy e alla sicurezza della navigazione e degli oggetti attivi presenti nelle pagine web
    g. ascoltare stazioni radio o televisive in modalità streaming continuo
    h. utilizzare applicazioni di "Instant Messaging"
    i. permettere l'accesso remoto al proprio computer.
14. seguire le linee guida qui di seguito elencate:
    A. **ACCESSO AL COMPUTER, ALLA RETE, AI PROGRAMMI APPLICATIVI E IN GENERALE A TUTTE LE RISORSE ASSEGNATE:** l'accesso al personal computer, alla rete, ai programmi applicativi e in generale a tutte le risorse che richiedono una procedura di identificazione e di autenticazione, dovrà avvenire con la user-id (altresì detta "nome utente" o "username" o "user name") a Lei assegnata dall'Istituto; è fatto esplicito divieto collegarsi o accedere alle risorse con user-id di altri utenti o comunque diverse da quelle assegnate dall'Istituto;
    B. **PASSWORD:** le proprie password devono essere custodite scrupolosamente e non devono essere comunicate ad altre persone; all'atto del primo utilizzo, le password devono essere obbligatoriamente modificate, anche quando tale codifica non sia imposta o suggerita dal sistema; se richiesto dal Dirigente Scolastico o dal Responsabile della protezione dei dati, le nuove password devono essere scritte sul un foglio di carta recante la data, nome e cognome dell'utente, user-id, programma o risorsa alla quale la user-id si riferisce, la vecchia password, e la nuova password; tale foglio deve essere posto in una busta chiusa e sigillata, firmata e datata sul lato esterno e consegnata al soggetto incaricato della custodia delle password;
    C. **VALIDITÀ PASSWORD:** la password per l'accesso alla rete, ai vari programmi applicativi e a tutti i software che ne prevedono l'uso per l'accesso devono essere sostituite almeno ogni sei mesi e

devono essere consegnate in busta chiusa al Custode delle Parole Chiave Applicative. **Per i dati sensibili la password deve essere sostituita ogni tre mesi**.

D. **SALVATAGGIO DEI DOCUMENTI:** tutti i documenti devono essere salvati obbligatoriamente sul server di rete: solo in questo modo è possibile assicurare il regolare salvataggio dei dati e il ripristino in caso di perdita, danneggiamento o necessità.
In casi del tutto eccezionali, i dati possono essere temporaneamente salvati su supporti rimovibili (quali, CD-ROM, chiavette USB, hard disk esterni etc), ma si fa presente che l'utilizzo di tali supporti aumenta sensibilmente il rischio di perdita, di diffusione indebita, di accesso ai dati da parte di soggetti non autorizzati. Se utilizzati, tali supporti mobili devono essere posti in custodie munite di chiavi o in armadi anch'essi muniti di serrature.

E. **CORRETTEZZA DEI DATI:** ciascun incaricato è responsabile del contenuto, della correttezza e della congruenza dei dati oggetto di trattamento; nel caso il trattamento effettuato consista nella verifica, nell'aggiornamento, nella "bonifica" dei dati, è necessario individuare chiaramente le versioni e le varie tipologie dei dati trattati, utilizzando anche qualificazioni temporali;

F. **CANCELLAZIONE DATI DA SUPPORTI MOBILI DI MEMORIZZAZIONE :** quando dei dati personali contenuti su supporto rimuovibile di memorizzazione devono essere definitivamente eliminati, si deve formattare il supporto stesso in quanto non è sufficiente la semplice cancellazione dei dati. Per quanto invece concerne i supporti di memorizzazione non riscrivibili (es. CD-ROM), essi devono esser fisicamente distrutti mediante frattura del supporto stesso. Nel caso sia necessario cancellare selettivamente uno o più files o archivi, è necessario utilizzare procedure e tecniche di cancellazione che non permettano di risalire o ricostruire il contenuto dei files oggetto di cancellazione; per questo tipo di operazioni è necessario attenersi a quanto specificato nell'allegato ***Regolamento il riutilizzo e lo smaltimento di apparecchiature elettroniche e supporti di memorizzazione***;

G. **SOFTWARE ANTIVIRUS:** il software antivirus installato sul PC non deve mai e per nessun motivo essere disabilitato o disinstallato in quanto, in tal caso, il PC non è più protetto da eventuali attacchi da virus, compromettendo così la sicurezza non solo del PC ma dell'intera rete. É necessario quindi verificare che vicino all'orologio della barra di avvio di Windows (posizione standard: basso a destra nel monitor) sia sempre presente l'icona dell'antivirus;

H. **VIRUS E POSTA ELETTRONICA:** si raccomanda di porre sempre attenzione al tipo di file allegati ai messaggi ricevuti, anche se il software antivirus è presente e abilitato. É necessario quindi diffidare dei file allegati con estensione del nome tipo EXE, COM, VBS, di tutti quelli che presentano una doppia "falsa" estensione (come ad esempio "VIDEO.AVI.VBS").
Queste tipologie di file sono infatti, in molti casi, i veicoli per la diffusione di virus.
Si raccomanda, nel caso in cui si ricevono messaggi con questo tipo di allegati, in caso di dubbio, di avvisare il Dirigente Scolastico o il D.S.G.A. prima di aprirli;

I. **RICHIESTA CONSULTAZIONE BANCHE DATI:** per poter consultare banche dati (cartacee e/o elettroniche) diverse da quelle inizialmente autorizzate, deve essere fatta richiesta al titolare del trattamento dei dati che provvederà a verificare la sussistenza di tutte le condizioni che

giustifichino l'accesso e a far attivare le procedure per permettere l'accesso alla banca dati richiesta;

J. **CONFIGURAZIONE DEL PC E DELLE RISORSE ASSEGNATE:** la configurazione hardware e software del PC – e più in generale di tutte le risorse assegnate o delle quali viene concesso l'utilizzo anche temporaneo - non deve essere modificata o alterata. Nel caso si ritenga sia necessario modificare una qualche configurazione, deve esserne fatta richiesta motivata al Dirigente Scolastico o al D.S.G.A.;

K. **INSTALLAZIONE DI SOFTWARE:** l'installazione di nuovi software, anche da Internet, può introdurre incompatibilità, instabilità, blocchi di sistema, rallentamenti e problemi nell'utilizzo del PC e dei programmi già installati. Per questo motivo se dovesse essere necessario utilizzare nuovi programmi, tali programmi **non devono essere installati autonomamente**, ma ne deve essere fatta richiesta scritta e motivata al Dirigente Scolastico o al D.S.G.A., che se del caso provvederà alle necessarie verifiche di compatibilità tecnica e funzionale e farà eseguire l'installazione da personale esperto. L'installazione di programmi non regolarmente acquistati e dotati di regolare licenza d'uso e/o manutenzione espone l?istituto al rischio di pesanti sanzioni per violazione della normativa sul diritto d'autore. Nel caso vengano installati programmi non autorizzati, l'Istituto si riserva il diritto di addebitarLe le somme eventualmente pagate per sanzioni amministrative comminate dalla Guardia di Finanza, dalla Polizia Postale, dal Garante per la protezione dei dati personali o da altri soggetti;

L. **ASSENZA ANCHE TEMPORANEA DAL POSTO DI LAVORO:** nel caso in cui ci si debba temporaneamente allontanare dal proprio PC (es. pausa caffè, spostamenti, brevi riunioni o incontri, etc.) è necessario bloccare la postazione di lavoro o il terminale; tale blocco può venire effettuato digitando la sequenza CTRL-ALT-CANC, oppure riposizionando il terminale sulla maschera iniziale. Alla fine dell'attività lavorativa quotidiana o prima della pausa pranzo, il computer deve essere spento e ci si deve accertare dell'avvenuto regolare spegnimento. Inoltre è obbligatorio impostare una password che permette di bloccare il PC nel momento in cui si avvia automaticamente lo screen saver;

M. **DOCUMENTI CARTACEI:** per quanto concerne i documenti cartacei, tali documenti devono esser gestiti e custoditi a cura dell'incaricato e, al termine del loro utilizzo o comunque al termine della giornata lavorativa, devono essere chiusi a chiave in armadi o cassetti o contenitori dotati di serratura e di chiave funzionante. In generale, i documenti devono essere gestiti e custoditi in maniera che non vi accedano persone prive di autorizzazione e che non vi possano essere furti o manomissioni. Quando non più necessari, i documenti cartacei devono essere consegnati al sovrintendente archivistico. I documenti contenenti dati sensibili devono essere custoditi all'interno di buste o raccoglitori chiusi, e conservati in armadi o archivi tenuti di norma chiusi, con serratura e chiave funzionante, con possibilità di controllo e tracciatura degli accessi.

N. **CARTELLE**: ciascun incaricato è responsabile del contenuto delle cartelle locali create sul PC, e di quelle assegnategli residenti su risorse di rete condivise (file server); è altresì responsabile delle condivisioni generate autonomamente alle cartelle da lui stesso create.

15. Lei è autorizzata a svolgere solo ed esclusivamente le seguenti operazioni sulla documentazione dei dati sensibili relativi al proprio ambito di lavoro:
    a. ricezione
    b. Eventuale protocollazione ai fini dell'attività di biblioteca
    c. presa in carico per le attività amministrative
    d. custodia per brevi periodi e solo ai fini istruttori
16. è tassativamente vietato comunicare, trasmettere o comunque portare a conoscenza dei dati sensibili e di tutte le informazioni ad essi collegate, soggetti esterni all'Istituto; se del caso, dette operazioni dovranno essere autorizzate per iscritto dal Dirigente Scolastico; nel caso, a seguito di autorizzazione scritta rilasciata dal Dirigente Scolastico, i dati siano comunicati, trasmessi o portati a conoscenza di soggetti esterni all'Istituto Comprensivo, è necessario compilare apposito registro o comunque tenere traccia per iscritto delle operazioni effettuate;
17. nel caso si verifichi un evento di tipo "data breach" (es. furto, perdita, accesso illecito, etc.), deve esserne immediatamente data notizia al Dirigente Scolastico e al Responsabile della protezione dei dati (contattabile alla mail **giancarlo.favero@capitalsecurity.it** e al numero **335-5950674**), che provvederà se del caso ad effettuare la notifica entro 72 ore dall'avvenuta conoscenza del fatto;
18. l'incaricato del trattamento dei dati è reso edotto del fatto che la mancata ottemperanza alle prescrizioni contenute nel presente atto di nomina può comportare gravi sanzioni civili, penali e disciplinari, tra le quali, ma non limitato a, la sanzione amministrativa pecuniaria fino a 10.000.000,00 Euro, ai sensi dell'art. 83 comma 5 del GDPR;
19. nel caso in cui la mancata ottemperanza alle prescrizioni contenute nel presente atto di nomina cagioni un danno di qualsiasi tipo (patrimoniale, biologico, di immagine, morale, esistenziale etc.) all'interessato, il soggetto designato è tenuto a risarcire personalmente il danno cagionato, ai sensi di quanto previsto dal combinato disposto dell'art. 82 del GDPR e dell'art. 2050 del Codice Civile. A titolo informativo si ricorda il risarcimento danni di **500.000,00 Euro** chiesto ed ottenuto da un cittadino a causa di inadeguata custodia della cartella clinica, e la sanzione di **60.000,00 Euro** comminata dal Garante per la protezione dei dati personali a seguito della comunicazione di dati sensibili relativi allo stato di salute a soggetti non autorizzati (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2337641).
20. Il trattamento dei dati deve rispettare in modo rigoroso quanto inoltre prescritto dal **Manuale per la gestione dei flussi documentali e suoi allegati**, documenti già pubblicati tramite apposite circolari.

Il Dirigente Scolastico

Dott. Roberto Benes

La preghiamo di restituirci il presente atto, da Lei firmato per ricevuta e presa visione.

Per ricevuta e presa visione, l'incaricato del trattamento dei dati:

DATA: _____

NOME E COGNOME: _____

Firma leggibile: _____