Ministero dell'Istruzione, dell'Università e della Ricerca
Ufficio Scolastico Regionale per il Lazio
ISTITUTO COMPRENSIVO - ZONA LEDA DI APRILIA
Via Carano 4D/E- 04011 APRILIA (LT)- ☎**. Tel: 06.92732870**- Fax: *0692732189*
posta certificata ltic83100c@pec.istruzione.it ltic83100c@istruzione.it
SITO WEB: *www.icszonaleda.edu.it*
C.F. 91101740594- Codice scuola LTIC83100C – Cod. Univoco fatt. elettr. UF09TF

ALLEGATO INF_01

COMUNICAZIONE DI AUTORIZZAZIONE PER IL TRATTAMENTO DEI DATI PERSONALI ASSISTENTE AMMINISTRATIVO

(Regolamento Europeo n. 679/2016 in materia di protezione dei dati personali)

IL DIRIGENTE SCOLASTICO
In qualità di Titolare del trattamento dei dati personali dell'Istituzione scolastica autorizza

ai sensi e per gli effetti del Regolamento UE n.2017/679 e ss. mm. e ii., la S.V. al trattamento dei dati personali riportati in allegato, che si svolgerà presso la sede della segreteria dell'Istituto Comprensivo Zona Leda attenendosi al regolamento contenuto nella presente nomina.

Nella sua qualità di impiegato/a nella segreteria amministrativa dell'Istituzione scolastica, Lei necessariamente partecipa a trattamenti di dati personali (intesi nell'ampia accezione di cui agli artt. da 1 a 6 del Regolamento UE n.2016/679), riguardanti le operazioni specifiche svolte nell'area di attività nella quale è impegnata e nell'ambito delle Sue competenze professionali. Lei è pertanto autorizzata all'accesso ed al trattamento dei dati personali anche particolarmente particolari e giudiziari (artt. 9-10 del Regolamento UE n. 2016/679), riguardanti tutti i soggetti con i quali l'Istituzione scolastica entra in relazione per i suoi fini istituzionali, nella misura e nei limiti stabiliti dal GDPR recante "l'identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione in attuazione degli articoli 20 e 21 del "Codice in materia di trattamento dei dati personali" (D.M. n.305 del 07.12.06).

Nel precisare che gli indirizzi operativi sinora a Lei forniti risultano coerenti con finalità e metodi cui la suddetta normativa GDPR riconosce legittimità, intendo con la presente indicarle formalmente i principi cui dovrà comunque continuare ad attenersi nel trattamento dei dati personali fornendoLe le seguenti:

ISTRUZIONI SPECIFICHE SUL TRATTAMENTO DEI DATI PERSONALI

- Lei acquisirà solo dati necessari e sufficienti per le finalità cui è preposta la Sua unità lavorativa;
- Lei provvederà a raccogliere ed a registrare dati, agli esclusivi fini dell'inserimento nelle banche dati presenti nella Sua unità e/o dell'arricchimento delle stesse, secondo la metodologia oggi applicata e li tratterà all'unico scopo di favorire il perseguimento degli obiettivi istituzionali affidati all'Istituzione scolastica;
- Lei, nell'ambito delle Sue attribuzioni lavorative, curerà l'esattezza, la disponibilità, l'integrità, nonché il tempestivo aggiornamento dei dati, verificando inoltre che questi ultimi siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali essi stessi sono stati raccolti e successivamente trattati;
- Nello svolgimento della sua attività lavorativa Lei potrà effettuare le operazioni di trattamento dei dati personali indicati in allegato e descritte nel documento "Registro dei trattamenti" dell'Istituto;
- Lei potrà conservare i dati 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 ed eserciterà altresì la dovuta diligenza affinché non vengano conservati, nel Suo settore operativo, dati non necessari o divenuti ormai superflui;

- Lei avrà cura, secondo le comuni regole della prudenza e della diligenza, di trattare i dati stessi con la massima riservatezza e di impedire, per quanto possibile, che estranei non autorizzati prendano conoscenza dei dati che lei detenga all'esclusivo fine lavorativo;
- Lei potrà 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 da un Responsabile o dal Titolare del trattamento;
- Al termine del trattamento, Lei dovrà assicurarsi che gli atti e i documenti contenenti dati sensibili e giudiziari vengano conservati in contenitori muniti di serratura o in ambienti ad accesso selezionato e vigilato, fino alla restituzione;
- Lei sarà tenuta a rispettare ed applicare le misure di sicurezza idonee a salvaguardare la riservatezza e l'integrità dei dati, indicate nell'allegato A in calce.

Le stesse norme si applicano obbligatoriamente al trattamento interamente o parzialmente automatizzato di dati personali, contenuti in un archivio o destinati a figurarvi, e si differenziano in base alle modalità di trattamento.
Lei in qualità di autorizzato è in possesso di una password e di un username (una o più credenziali di autenticazione), che dovrà utilizzare e gestire attenendosi alle seguenti istruzioni. Le credenziali di autenticazione per l'accesso alle applicazioni sono individuali pertanto non vanno mai condivise con altri utenti (anche se Autorizzati del trattamento). La Sua password deve essere composta da almeno otto caratteri (o se il software non lo permette dal massimo dei caratteri disponibili), non deve essere riconducibile alla Sua persona e deve essere cambiata da Lei almeno ogni 3 mesi. Qualora abbia qualche problema può rivolgersi all'amministratore di sistema, al Direttore SGA o al Titolare del trattamento.

Per evitare accessi illeciti, al termine di ciascun trattamento uscire dall'applicazione utilizzata assicurandosi di avere eseguito il logout. I dati personali archiviati su supporti di tipo magnetico e/o ottico devono essere protetti con le stesse misure di sicurezza previste per i supporti cartacei. A tal fine, se è necessario allontanarsi dalla sua postazione di lavoro, dovrà verificare che i contenitori degli archivi e banche dati (scrivanie, cassetti, armadi, computer, etc.) siano chiusi a chiave e/o protetti da password e che i dati dagli stessi estratti non possano divenire oggetto di trattamento improprio. In caso di sostituzione del computer da Lei utilizzato, Lei si assicurerà che siano compiute le necessarie operazioni di formattazione. Per qualsiasi problema tecnico sulla sicurezza si dovrà rivolgere tempestivamente all'amministratore di sistema o al Titolare. La presente costituisce pertanto conferimento formale dell'incarico di compiere, nei limiti di cui sopra, tutte le operazioni di trattamento di dati personali attinenti alla Sua funzione.

Tale designazione ha validità per l'intera durata del rapporto di lavoro e viene comunque a cessare al modificarsi del rapporto di lavoro o con esplicita Revoca.

ARCHIVI CONTENENTI DATI PERSONALI

Descrizione del trattamento	Archivi interessati
Trattamento di dati personali, anche relativi a condanne civili e penali, e dati relativi alla salute, nell'ambito delle attività di selezione e reclutamento del personale a tempo indeterminato o determinato e gestione del rapporto di lavoro	Fascicoli del personale ATA Fascicoli del personale docente scuola infanzia Fascicoli del personale docente scuola primaria Fascicoli del personale docente scuola media Contratti per supplenze Gestione organico (graduatorie, trasferimenti, ecc.) Fascicoli supplenti Retribuzioni e documenti contabili e fiscali del personale Dichiarazioni per finalità assistenziali, previdenziali e pensionistici Visite collegiali e fiscali Assenze e permessi Fascicoli Ricostruzione di carriera
Organismi collegiali	Documentazione degli Organi collegiali (Verbali di assemblea, convocazioni, provvedimenti, ecc.) e comunicazioni di vario tipo per la gestione dei rapporti sindacali con le RSU

Attività propedeutiche all'avvio dell'anno scolastico	Fascicoli degli alunni Fascicoli riservati alunni con disabilità Documentazione propedeutica all'avvio dell'anno scolastico (iscrizione, classi, graduatorie, trasferimenti, ecc.) Documenti necessari per assicurazione e denuncia infortuni Procedimenti relativi alla frequenza (prolungamento orario, organizzazione servizio mensa) Archivio generale storico
Attività educative formative didattiche e di valutazione	Documenti di varia natura connessi all'attività educativa, didattica, formativa e di valutazione (diplomi, prove di valutazione intermedie e finali, registri, verbali, piano individualizzato, ecc.) Procedure Invalsi Organizzazione gite scolastiche Convocazioni GLH
Rapporti scuola-famiglia compresa la gestione del contenzioso	Documenti e comunicazioni di vario tipo relativi a: informazioni riservate, provvedimenti disciplinari e vicende giuridiche in corso e contenziosi
Rapporti con: MIUR, Servizio Mensa, altre Istituzioni scolastiche, Enti Locali, ASL e centri Handicap e sostegno di riabilitazione (trasmissione schede rilevazioni alunni H) e privati (Società e liberi professionisti)	Documenti e comunicazioni di vario tipo del protocollo e della posta elettronica PEO e PEC dell'Istituto Fornitori ed esperti esterni
Tutti i trattamenti sopra descritti nei relativi contesti	Archivio generale storico

Il Dirigente Scolastico
Dott.ssa Monica Comuzzi
(firma autografa ai sensi dell'art.3 c.2 D.Lgs. 3993)

Allegato A

RACCOMANDAZIONI E ISTRUZIONI SULLA GESTIONE DEGLI ACCESSI NEL LUOGO DI LAVORO

- impedire l'intrusione nei locali che gli sono stati affidati in custodia da parte di persone non autorizzate secondo quanto stabilito dal Titolare del Trattamento;
- impedire il danneggiamento, la manomissione, la sottrazione, la distruzione, o la copia di dati nei locali che gli sono stati affidati in custodia da parte di persone non autorizzate secondo quanto stabilito dal Titolare del Trattamento;
- conservare i documenti contenenti i dati sensibili in contenitori muniti di serratura;
- identificare e registrare i soggetti ammessi dopo l'orario di chiusura degli uffici stessi.

CLEAN DESK

Le postazioni di lavoro portatili, la carta e i supporti informatici, quando non sono presidiati per periodi di tempo significativi, devono essere sistemati in armadi adeguatamente chiusi o in altri contenitori fisicamente protetti. Le informazioni riservate su carta o supporto informatico, devono essere messe sotto chiave. Per le informazioni strettamente riservate se possibile ricorrere a una cassaforte o un armadio blindato e ignifugo in cui riporle quando non sono utilizzate, e in particolare quando in ufficio non c'è nessuno.

CLEAN SCREEN

Per quanto riguarda i PC, quando non sono utilizzati, non devono essere lasciati incustoditi con sessioni applicative aperte o con logon effettuato, ma devono essere protetti da chiavi fisiche, password o altri tipi di blocchi/controlli (come ad es. screen saver).

GESTIONE DELLE PASSWORD

Per quanto riguarda la gestione della Password di accesso alla postazione è necessario attenersi alle seguenti norme:

- deve essere custodita con la massima cura;
- non deve essere comunicata ad altri;
- non deve essere scritta su supporti facilmente accessibili (post-it, blocco appunti, ecc.). Nel caso si voglia mantenerne traccia scritta, per propria memoria, essa deve essere conservata in luogo sicuro;
- deve essere cambiata almeno ogni 3 mesi;
- deve avere una lunghezza minima di 8 caratteri;
- non deve essere legata al nome dell'utente, oppure alla sua User-id, o in generale a parole a lui riconducibili (nome della moglie o dei figli, luogo e data di nascita);

GESTIONE DELLA SMARTCARD

- La carta è strettamente personale e non è cedibile.
- La segretezza dei PIN e del PUK è fondamentale per evitare usi fraudolenti della carta in caso di furto o smarrimento della carta stessa.

GESTIONE DEI PIN

Per quanto riguarda la gestione dei PIN della propria smart card è necessario attenersi alle seguenti norme. Sia il PIN Utente che il PIN Firma devono:

- non essere formati da caratteri continui sulla tastiera (12345678 è un PIN poco sicuro);
- non essere un numero, parola o nome riconducibile alla propria vita (la data di nascita della moglie, il nome del cane, il numero di conto corrente, il numero di passaporto sono password poco sicure);
- non devono essere scritti su supporti facilmente accessibili (post-it, blocco appunti, ecc.). Nel caso si voglia mantenerne traccia scritta, per propria memoria, essa deve essere conservata in luogo sicuro;
- non vanno confidati a nessuno per nessun motivo.

USO DEGLI ARMADI IGNIFUGHI E BLINDATI

Per l'uso degli armadi ignifughi e blindati e delle relative chiavi, il designato dovrà applicare scrupolosamente le regole e le procedure espressamente definite dall'Istituzione scolastica.