Nomina Soggetto Autorizzato al Trattamento dei Dati
ASSISTENTI AMMINISTRATIVI

Regolamento UE 2016/679 del 27/04/2016

Al personale scolastico – Assistenti amministrativi

IL DIRIGENTE

1. VISTO il Regolamento UE 2016/679 con particolare riguardo agli artt. 24, 28, 29 e 32;
2. CONSIDERATO che questo Istituto è titolare del trattamento dei dati personali di alunni, genitori, personale dipendente, fornitori, e qualunque altro soggetto che abbia rapporti con l'Istituto medesimo e che a questo conferisca, volontariamente o per obbligo, propri dati personali;
3. CONSIDERATO che la titolarità del trattamento dei dati personali è esercitata dallo scrivente Dirigente dell'Istituto, in qualità di legale rappresentante dello stesso;
4. CONSIDERATO che le SS.LL, in servizio presso questo Istituto, per l'espletamento delle Loro funzioni, possono venire a conoscenza e dunque trattare dati personali relativi ad alunni, aziende fornitrici di servizi e al personale di questa istituzione scolastica, fermi restando gli obblighi e le responsabilità civili e penali;
5. CONSIDERATO che la presente nomina è effettuata ai sensi dell'art. 29 del Regolamento (UE) 2016/679 e dell'art. 2-quaterdecies del D.lgs. 196/2003 come modificato dal D.lgs. 101/2018.

DESIGNA

Le SS.LL. quali

SOGGETTO AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI (incaricato)
nell'ambito delle funzioni che Lei è chiamata/o a svolgere

In ottemperanza al RGPD, che regola il trattamento dei dati personali, laddove costituisce trattamento *"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione",* ed in relazione al presente atto di nomina, l' incaricato a trattare i dati personali (tutti quei dati idonei ad identificare direttamente o indirettamente una persona fisica) attenendosi alle modalità descritte nella presente nomina.

La presente nomina è effettuata ai sensi dell'art. 29 del Regolamento UE 2016/679 e dell'art. 2-quaterdecies del D.lgs. 196/2003 come modificato dal D.lgs. 101/2018.

La presente nomina autorizza il trattamento dei dati in relazione all'espletamento delle funzioni e dei compiti secondo mansionari, settori e reparti assegnati nell'ambito del rapporto di lavoro con questa istituzione scolastica e disciplinati dalla normativa in vigore e dai contratti di settore. In particolare, le SS.LL sono incaricate delle operazioni di trattamento connesse alle seguenti funzioni e attività svolte, ciascuno in relazione agli incarichi previsti dai contratti di lavoro nazionali ed integrativi, piano delle attività, incarichi specifici o altre mansioni assegnate di propria competenza.
Si indicano quali attività ad esempio:

- Gestione fascicoli personali
- Aggiornamento documentazione amministrativa
- Gestione contratti, permessi, assenze, malattie, accesso a INPS, SIDI, NoIPA
- Rendicontazione progetti (PON/PNRR)
- Ecc.

Le attività autorizzate si riferiscono per ciascun addetto **esclusivamente alle funzioni ad esso assegnate** secondo piano delle attività, mansionario e ordini di servizio.

La nomina autorizza l'accesso alle seguenti banche dati della scuola, a seconda del proprio profilo di autorizzazione:

- archivi cartacei;
- archivi digitali memorizzati sul server della scuola;
- banche dati presso gestori esterni in modalità cloud;
- caselle di posta elettronica dell'Istituto, da utilizzarsi ai soli fini dello svolgimento delle proprie mansioni lavorative.

I trattamenti dei dati vanno effettuati tenendo presenti le istruzioni operative che seguono, facendo comunque riferimento anche ad eventuali ulteriori istruzioni impartite dal Titolare del trattamento.

1. il trattamento dei dati personali cui le SS.LL. sono autorizzate ad accedere deve avvenire secondo le modalità definite dalla normativa in vigore, in modo lecito e secondo correttezza ed è consentito soltanto per lo svolgimento delle funzioni istituzionali della scuola;
2. i dati personali oggetto dei trattamenti devono essere verificati, esatti ed aggiornati, devono essere pertinenti, completi e non eccedenti le finalità per le quali vengono raccolti e trattati;
3. 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 DSGA o dal Dirigente scolastico. Si raccomanda particolare attenzione alla tutela del diritto alla riservatezza degli interessati (persone fisiche a cui afferiscono i dati personali);
4. l'accesso al protocollo, ai fascicoli, alle banche dati, alle caselle di posta e alle piattaforme amministrative è consentito esclusivamente in relazione alle pratiche e alle funzioni formalmente assegnate. È vietata la consultazione di documenti, registrazioni di protocollo o fascicoli per curiosità, interesse personale o comunque in assenza di una concreta necessità di servizio. Qualora il sistema renda visibili documenti non pertinenti alla propria funzione, l'assistente deve astenersi dall'aprirli e segnalare al DSGA l'eventuale necessità di rivedere i profili di autorizzazione;
5. le comunicazioni contenenti dati sanitari, giudiziari, disciplinari, sindacali, informazioni relative a disabilità, DSA, BES, affidamento familiare, contenzioso o altre situazioni riservate devono essere registrate utilizzando, quando previsto, il protocollo riservato e assegnate esclusivamente agli uffici e ai soggetti competenti. L'oggetto di protocollo deve essere formulato in modo sintetico e non deve contenere diagnosi, dettagli sanitari o altre informazioni eccedenti. Gli allegati riservati non devono essere inseriti in fascicoli o classificazioni accessibili a personale non autorizzato;
6. 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;
7. l'accesso agli archivi contenenti dati personali è permesso solo alle persone autorizzate e soggetto a controllo secondo le regole definite dallo scrivente;
8. i documenti contenenti dati personali vanno custoditi all'interno di cassetti o armadi con serratura;
9. i documenti della scuola contenenti dati personali non possono uscire dalla sede scolastica, né essere copiati, se non dietro espressa autorizzazione del Dirigente scolastico. In caso di custodia presso altre sedi, l'incaricato deve assicurare comunque la necessaria protezione ai dati personali evitando che famigliari o altri soggetti possano prendere visione dei dati;
10. le comunicazioni a terzi da parte degli incaricati devono avvenire in forma riservata; se effettuate per scritto dovranno essere consegnate in forma chiusa; 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; la comunicazione o diffusione a terzi dei dati personali è consentita nei casi previsti da legge o regolamento;
11. prima di pubblicare circolari, comunicazioni, allegati o documenti nel registro elettronico, l'assistente deve verificare la sezione utilizzata, i destinatari selezionati e i relativi permessi di visualizzazione;
12. Convocazioni GLO, PEI, PDP, certificazioni, comunicazioni disciplinari o riferite a un singolo alunno non devono essere inseriti in bacheche visibili all'intera classe, alle altre famiglie o a personale non coinvolto. In caso di dubbio sulla configurazione del registro o sulla corretta selezione dei destinatari, la pubblicazione deve essere sospesa e sottoposta a verifica del DSGA o del Dirigente;
13. si raccomanda di effettuare l'archiviazione dei dati personali all'interno del server scolastico o nella piattaforma digitale in cloud. Nel caso in cui per l'esercizio delle attività sopra descritte sia necessario l'uso di supporti rimovibili (quali ad esempio dispositivi USB), su cui sono memorizzati dati personali, essi vanno custoditi con cura; si ricorda che non è possibile memorizzare dati inerenti allo stato di salute su supporti elettronici rimovibili, se non provvisti di cifratura o pseudonimizzazione;

14. i documenti contenenti categorie particolari di dati devono essere conservati negli ambienti istituzionali autorizzati, protetti da adeguati profili di accesso. Cifratura, pseudonimizzazione o protezione mediante password devono essere utilizzate quando necessarie in relazione al canale di trasmissione e al rischio concreto;
15. PEI, PDP, diagnosi, certificazioni sanitarie, verbali GLO e altra documentazione relativa a disabilità, DSA o condizioni di salute devono essere conservati esclusivamente nelle aree riservate individuate dall'Istituto e resi accessibili soltanto al personale competente. È vietato inviare tali documenti mediante posta elettronica ordinaria a destinatari multipli, inserirli in cartelle con collegamento pubblico o accessibile a chiunque disponga del link, oppure salvarli su cloud, dispositivi o account personali;
16. prima dell'invio di e-mail o PEC, l'assistente deve verificare con particolare attenzione destinatario, oggetto, testo, allegati e presenza di precedenti conversazioni contenenti dati non pertinenti. In caso di invio a più destinatari, gli indirizzi devono essere inseriti nel campo CCN, salvo che la reciproca conoscibilità sia necessaria e autorizzata. Gli allegati devono essere aperti e controllati prima dell'invio, verificando che non contengano documenti riferiti ad altri interessati, pagine ulteriori, commenti, revisioni, firme, codici fiscali o dati non necessari;
17. prima di condividere una cartella o un documento, devono essere verificati nominativamente gli utenti autorizzati;
18. l'utilizzo di archivi in cloud deve avvenire esclusivamente tramite piattaforme istituzionali autorizzate;
19. non devono essere pubblicati codici fiscali, indirizzi, recapiti personali, firme autografe, dati bancari, documenti di identità, diagnosi, informazioni sanitarie, riferimenti a disabilità, DSA, BES, procedimenti disciplinari o situazioni familiari;
20. nelle graduatorie, negli elenchi e nei provvedimenti relativi al personale devono essere pubblicati esclusivamente i dati necessari. Non devono comparire data e luogo di nascita, codice fiscale, indirizzo, recapiti, firma, motivazioni sanitarie o altre informazioni eccedenti;
21. assenze, permessi, malattie, sostituzioni e altre informazioni riguardanti il personale devono essere visibili esclusivamente ai soggetti autorizzati per esigenze di servizio;
22. le eventuali credenziali di autenticazione (codice di accesso e parola chiave per accedere ai sistemi informatici) 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 al titolare del trattamento dei dati; la parola chiave deve essere scelta con cura, deve essere complessa (minimo 8 caratteri, con minuscole, maiuscole, numeri e almeno 1 carattere speciale) e non deve contenere riferimenti agevolmente riconducibili all'incaricato;
23. salvo diverse disposizioni dello scrivente, gli incaricati possono accedere alla documentazione cartacea amministrativa (segreteria) solo per specifiche operazioni sopra ricordate di pertinenza dell'incaricato stesso, escludendo l'accesso a dati di terzi per i quali non sia stato conferito un incarico;
24. stampe di prova, bozze, elenchi, fascicoli, cedolini, certificazioni e fogli contenenti dati personali non devono essere riutilizzati come carta da riciclo, distribuiti agli studenti o gettati nei normali cestini;
25. l'incaricato è tenuto a conservare con la massima segretezza le password e qualunque dispositivo elettronico di identificazione attribuito, a informare tempestivamente il proprio superiore o il Titolare di qualunque evento che pregiudichi la sicurezza dei dati, a non lasciare incustodita la postazione di lavoro durante le operazioni di accesso ad archivi di dati personali, a custodire le pratiche e i documenti affidati e restituirli al termine del trattamento avendo cura che agli stessi non avvengano accessi non autorizzati;
26. ogni accesso non autorizzato o anomalia rilevata dovrà essere immediatamente segnalato al DSGA o al RPD.
27. l'Assistente Amministrativo è tenuto a rispettare quanto previsto nel Regolamento interno per l'utilizzo degli strumenti digitali e la gestione documentale;
28. non devono essere fornite telefonicamente informazioni su voti, assenze, stato di salute, disabilità, procedimenti disciplinari, situazione familiare, rapporti di lavoro, stipendi o altre informazioni riservate senza aver previamente verificato l'identità e la legittimazione del richiedente;
29. è vietato inserire in chatbot o sistemi di intelligenza artificiale non autorizzati documenti amministrativi, dati di studenti o personale, e-mail, verbali, contratti, certificazioni, richieste di accesso, informazioni disciplinari o altri contenuti della scuola. Gli strumenti IA eventualmente autorizzati possono essere utilizzati esclusivamente secondo il Regolamento IA, la PUIA e le istruzioni dell'Istituto. Gli output devono essere verificati da una persona prima del loro utilizzo in atti o comunicazioni amministrative;
30. devono essere immediatamente segnalati al Dirigente e al DSGA: invii al destinatario errato, allegati sbagliati, pubblicazioni indebite, documenti smarriti, accessi anomali, credenziali compromesse, cartelle condivise con utenti non autorizzati, perdita di dispositivi, errato smaltimento di documenti e comunicazione verbale di dati a soggetti non legittimati. Quando possibile, l'assistente deve interrompere immediatamente la diffusione o revocare l'accesso, senza

cancellare log o altri elementi utili alla ricostruzione dell'evento. La segnalazione deve indicare dati coinvolti, destinatari, tempi dell'accaduto e misure già adottate.

È espressamente vietato a tutti gli incaricati dei trattamenti:

- consegnare sotto qualunque forma a personale non autorizzato elaborati o copie dei dati oggetto del trattamento;
- comunicare a personale non autorizzato notizie relative a dati personali trattati;
- effettuare copie non autorizzate dei dati oggetto del trattamento;
- utilizzare i dati raccolti per finalità diverse dalle proprie mansioni;
- divulgare ad altri la propria password di accesso ai software dell'Istituto;
- inviare dati personali tramite account personali non istituzionali (es. Gmail privato);
- salvare copie di documenti su dispositivi personali (es. smartphone);
- fotografare, scansionare o trasmettere documenti della scuola mediante smartphone personali, applicazioni private o servizi cloud non autorizzati.

Si informano gli incaricati che esclusivamente in funzione della sicurezza e della tracciabilità gli accessi alle banche dati potranno essere registrati.

La presente nomina non comporta alcuna modifica delle mansioni e della qualifica professionale. Si ricorda che le violazioni potranno essere perseguite ai sensi del Regolamento Ministeriale sul trattamento dei dati personali. La presente nomina è revocabile in qualunque momento senza preavviso.

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.

Il Dirigente Scolastico
dott.ssa Sara Rinaldi
Firmato digitalmente ai sensi del D.P.R. 445/2000
e del D.Lgs 82/2005 e ss.mm.ii.

PER PRESA VISIONE:

Nome e cognome ……..

Data …….. Firma ……