



ISTITUTO COMPRENSIVO EX "S.M. PASCOLI"
Via Parini, 1 - 75100 MATERA

Cod. Ministeriale: MTIC82700A / E-mail: mtic82700a@istruzione.it / Pec: mtic82700a@pec.istruzione.it
C.F.: 93051600778 / Sito: www.icpascolimatera.edu.it / Telefono: 0835.386254

INCARICO GDPR DSGA E ASSISTENTI AMMINISTRATIVI

Oggetto: designazione incaricato al trattamento dati ex GDPR Regolamento UE 679/2016 e D. Lgs. 101/2018.

IL DIRIGENTE

- VISTO il Regolamento UE 2016/679 con particolare riguardo agli artt. 24, 28, 29 e 32;
- VISTO il Decreto Legislativo 30 giugno 2003, n. 196 e ss. mm. e ii. (in particolare il D. Lgs. 101(2018), "Codice in materia di protezione dei dati personali", nel seguito indicato sinteticamente come Codice, ed in particolare gli artt. 28 (titolare del trattamento), 29 (responsabile del trattamento) e 30 (incaricati del trattamento);
- CONSIDERATO che questo Istituto è titolare del trattamento dei dati personali di alunni, genitori, personale dipendente, fornitori, e qualunque altro soggetto abbia rapporti con l'Istituto medesimo;
- CONSIDERATO che le SS.LL, in servizio presso questo Istituto in qualità di assistenti amministrativi per l'espletamento delle loro funzioni, hanno necessità di trattare dati relativi agli alunni, alle loro famiglie e agli esercenti la funzione genitoriale, al personale dipendente, ai fornitori e a qualunque altro soggetto che abbia a che fare con l'istituzione scolastica, fermo restando gli obblighi e le responsabilità civili e penali;

DESIGNA

La SS.LL. quali incaricati al trattamento dati, su supporto cartaceo o digitale, nell'espletamento delle funzioni e dei compiti assegnati nell'ambito del rapporto di lavoro con questa istituzione scolastica e disciplinati dalla normativa in vigore e dai contratti di settore.

In particolare, in qualità di assistenti amministrativi, le SS.LL sono incaricate delle operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modifica, comunicazione (nei soli casi autorizzati dal titolare o dal responsabile del trattamento), selezione, estrazione di dati, connesse alle seguenti funzioni e attività dalle SS.LL esercitate:

Alunni e genitori

- gestione archivi cartacei/elettronici alunni e genitori (o esercenti funzione genitoriale);
- consultazione documenti e registri di attestazione dei voti e di documentazione della vita scolastica dello studente, nonché delle relazioni tra scuola e famiglia quali ad esempio richieste, istanze e corrispondenza con le famiglie;

- gestione contributi e/o tasse scolastiche versati da alunni e genitori;
- adempimenti connessi alla corretta gestione del registro infortuni;
- adempimenti connessi a viaggi di istruzione, visite guidate e uscite didattiche.

Personale ATA e Docenti

- gestione archivi cartacei/elettronici Personale ATA e Docenti;
- tenuta documenti e registri relativi al rapporto di lavoro dei dipendenti (quali ad es. assenze, convocazioni, comunicazioni, documentazione sullo stato del personale, atti di nomina del personale a tempo determinato, decreti del Dirigente).

Contabilità e finanza

- gestione archivi cartacei/elettronici della contabilità;
- gestione stipendi e pagamenti, nonché adempimenti di carattere previdenziale;
- gestione documentazione ore di servizio (quali ad esempio, registrazione delle ore eccedenti);
- gestione rapporti con i fornitori;
- gestione programma annuale e fondo di istituto;
- corretta tenuta dei registri contabili previsti dal Decreto Interministeriale n. 129/2018 e correlata normativa vigente.

Protocollo e archivio corrispondenza ordinaria

- attività di protocollo e archiviazione della corrispondenza e della documentazione ordinaria.

Attività organi collegiali

- eventuale operazione di consultazione e estrazione dati dai verbali degli organi collegiali.

Si rende noto, a tal fine, che le operazioni sopra descritte vanno rigorosamente effettuate tenendo presenti le istruzioni operative che seguono:

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 e con l'osservanza delle prescrizioni di cui al Regolamento UE 2016/679;
2. il trattamento dei dati è consentito soltanto per lo svolgimento delle funzioni istituzionali della scuola;
3. i dati, oggetto dei trattamenti, devono essere esatti ed aggiornati, inoltre devono essere pertinenti, completi e non eccedenti le finalità per le quali vengono raccolti e trattati;
4. è vietata qualsiasi forma di diffusione e comunicazione dei dati trattati che non sia strettamente funzionale allo svolgimento dei compiti affidati e autorizzata dal responsabile o dal titolare del trattamento;
5. 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;
6. 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;
7. le eventuali credenziali di autenticazione 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 titolare del trattamento dei dati;

8. in caso di trattamento su supporto cartaceo, i documenti dovranno essere custoditi in luoghi ad accesso controllato e riservato;
9. l'accesso agli archivi contenenti dati sensibili o giudiziari è permesso solo alle persone autorizzate e soggetto a continuo controllo secondo le regole definite dallo scrivente;
10. i documenti della scuola contenenti dati personali non possono uscire dalla sede scolastica, né copiati, se non dietro espressa autorizzazione del responsabile o dal titolare del trattamento;
11. in caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati, l'incaricato dovrà verificare che non vi sia possibilità da parte di terzi non autorizzati, di accedere a dati personali per i quali era in corso il trattamento;
12. le comunicazioni agli interessati dovranno avvenire in forma riservata;
13. 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 in forma scritta;
14. in caso di comunicazioni elettroniche ad alunni, colleghi, genitori, personale della scuola o altri soggetti coinvolti per finalità istituzionali, queste (comunicazioni) vanno poste in essere seguendo le indicazioni fornite dall'Istituzione scolastica e avendo presente la necessaria riservatezza delle comunicazioni stesse e dei dati coinvolti.

Il presente incarico è a tempo indeterminato e s'intende automaticamente revocato alla data di cessazione del rapporto di lavoro in essere con questa istituzione scolastica.

Si allegano le linee guida specifiche per il personale amministrativo.

Matera, 12/09/2023

IL DIRIGENTE SCOLASTICO
Michele Ventrelli

Linee guida specifiche per il personale amministrativo

Misure operative per garantire la sicurezza del trattamento dati

GDPR Regolamento UE 679/2016

Misure di sicurezza da osservare nell'adempimento dei propri compiti per il trattamento dei dati personali.

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

- Durante i trattamenti i documenti contenenti dati personali vanno mantenuti in modo tale da non essere alla portata di vista di persone non autorizzate (ciò implica che durante l'accesso dell'utenza i documenti dovranno essere coperti o girati);
- Al termine del trattamento occorre custodire i documenti contenenti dati personali all'interno di archivi/cassetti/ armadi preferibilmente chiusi a chiave, segnalando tempestivamente al Referente del trattamento eventuali anomalie;
- **I documenti della scuola contenenti dati personali non possono uscire dalla sede scolastica, né copiati, se non dietro espressa autorizzazione del referente o del titolare del trattamento (DSGA e DS);**
- In caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati, l'incaricato dovrà verificare che non vi sia possibilità da parte di terzi, anche se dipendenti non autorizzati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento;
- 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 in forma scritta;
- **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;
- Provvedere personalmente alla distruzione quando è necessario eliminare documenti inutilizzati;
- Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o particolari 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 Referente 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 referente o dal Titolare.

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

- Non salvare file o cartelle nel DESKTOP. Se si ritiene di dover avere una cartella sul desktop questo dovrà essere salvato in apposita cartella sul SERVER e poi collegata/inviata al Desktop.

Diversamente, non sarà possibile recuperare eventuali file quando chi lo ha creato è assente e garantire che le cartelle o i file non vadano persi in caso di rotture del PC.;

- Non lasciare SUPPORTI INFORMATICI, cartelle o altri documenti a disposizione di estranei;
- Nel caso in cui per l'esercizio delle attività sopra descritte sia inevitabile l'uso di supporti rimovibili (quali ad esempio chiavi USB, CD-ROM, ecc), su cui sono memorizzati dati personali, essi vanno custoditi con cura, né messi a disposizione o lasciati al libero accesso di persone non autorizzate; tali supporti dovranno essere obbligatoriamente crittografati;
- Conservare i dati particolari 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 informatici (CD, Chiavette ecc.) in modo ordinato negli appositi contenitori e chiudere a chiave classificatori e armadi dove sono custoditi;
- **È severamente vietato far utilizzare la propria postazione di lavoro ai docenti e ai collaboratori scolastici;**
- Scegliere una password con le seguenti caratteristiche:
 1. Originale
 2. Composta da otto caratteri
 3. 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;
- Cambiare periodicamente (almeno una volta ogni tre mesi) la propria password;
- Trascrivere su un biglietto chiuso in busta sigillata e controfirmata la nuova password e consegnarla al custode delle credenziali;
- Spegnerne correttamente il computer al termine di ogni sessione di lavoro;
- Non abbandonare la propria postazione di lavoro per la pausa o altri motivi senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
- Comunicare tempestivamente al Titolare o al Referente qualunque anomalia riscontrata nel funzionamento del computer;
- Non riutilizzare i supporti informatici utilizzati per il trattamento di dati particolari per altri trattamenti;
- Non gestire informazioni su più archivi ove non sia strettamente necessario e comunque curarne l'aggiornamento in modo organico;
- **Utilizzare le seguenti regole per la posta elettronica:**
 1. Non aprire documenti di cui non sia certa la provenienza
 2. Non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus
 3. Inviare messaggi di posta solo se espressamente autorizzati dal Referente
 4. Controllare accuratamente l'indirizzo del destinatario prima di inviare dati personali
 5. Verificare che sia presente in calce alla mail la clausola di esclusione di responsabilità

Ogni inosservanza delle presenti disposizioni sarà imputata ai diretti interessati.