



## I.I.S.S. "DON MILANI PERTINI - E. MORANTE"

### Sede di Grottaglie:

**Istituto Tecnico Economico** (Amministrazione, Finanza e Marketing - Turismo) **Istituto Tecnico Tecnologico** (Logistica e Trasporti)  
**Istituto Professionale** per i Servizi Commerciali e per i Servizi per la Sanità e l'Assistenza Sociale  
**Corso Istruzione Adulti** (Amministrazione, Finanza e Marketing - Servizi Socio Sanitari)

### Sede di Crispiano:

**Istituto Professionale** per i Servizi di Enogastronomia ed Ospitalità Alberghiera e Servizi Culturali e dello Spettacolo  
**Corso Istruzione Adulti** "Servizi per l'Enogastronomia e l'Ospitalità Alberghiera"

Via XXV Luglio n. 89, 74023 Grottaglie (TA) - Tel. 0995661026 - Corso Umberto I – Crispiano (TA) Tel. 099611313  
Ambito PUG0000023 Codice scuola TAIS04700T - C.F. 90287460738 - Codice IPA 7CYTCUK9 – Codice Univoco MQ7LJ5  
E-mail: [tais04700t@istruzione.it](mailto:tais04700t@istruzione.it); Pec: [tais04700t@pec.istruzione.it](mailto:tais04700t@pec.istruzione.it) - Sito Web: [www.donmilanipertinimorante.edu.it](http://www.donmilanipertinimorante.edu.it)

Al DSGA

Agli assistenti amministrativi

Ai docenti titolari di incarichi di governance

*(Collaboratori del DS, FF. SS., responsabili di plesso, referenti con incarichi specifici)*

I.I.S.S. DON MILANI-PERTINI-MORANTE  
Prot. 0001709 del 03/10/2025  
VII (Uscita)

Bacheca Argo DidUp  
Amministrazione Trasparente  
Al sito web dell'Istituto

Grottaglie, 02/10/2025

**Oggetto: PROTOCOLLI ORGANIZZATIVI - istruzioni in qualità di persona autorizzata al trattamento dati ex GDPR Regolamento UE 679/2016 e D. Lgs. 101/2018 – PERSONALE AMMINISTRATIVO E DOCENTI CON INCARICHI DI GOVERNANCE**

### 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 (persone autorizzate al 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;

### **FORNISCE ALLE SS.LL.**

le istruzioni in qualità di persone autorizzate al trattamento dei dati personali, 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. 44/2001 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:

Qualsiasi operazione o insieme di operazioni effettuate su dati personali, con o senza l'ausilio di strumenti automatizzati — quali, a titolo esemplificativo, la raccolta, registrazione, organizzazione, strutturazione,

conservazione, adattamento, modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, raffronto, interconnessione, limitazione, cancellazione o distruzione — dovranno essere eseguite nel pieno rispetto delle seguenti istruzioni operative, al fine di evitare la dispersione e/o la perdita dei dati trattati.

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, la persona autorizzata al trattamento 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 la persona autorizzata al trattamento 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.
15. Accertarsi, anche durante i trattamenti, che i documenti contenenti dati personali non siano alla portata di vista di persone non autorizzate.
16. L'accesso agli archivi contenenti dati particolari e/o giudiziari deve essere consentito esclusivamente a persone autorizzate, mediante la definizione di accessi logici e sistemi di autenticazione agli applicativi o alle cartelle condivise, in base ai ruoli, alle responsabilità e ai profili utente assegnati. Al fine di

rafforzare la sicurezza e migliorare la gestione dei dati archiviati, si raccomanda inoltre di mantenere separati, sia su supporti informatici che cartacei, i dati particolari e/o giudiziari da quelli non appartenenti a tali categorie, utilizzando partizioni distinte e applicando misure di sicurezza differenziate, come l'anonimizzazione o la pseudonimizzazione.

17. Effettuare le comunicazioni agli interessati (persone fisiche a cui afferiscono i dati personali) SEMPRE in forma riservata; in particolare nel caso di comunicazioni a mezzo lettera, dovranno essere consegnate in buste chiuse. Se trasmesse tramite posta elettronica, occorre adottare adeguati protocolli di sicurezza quali la trasmissione cifrata del file, ad esempio con formato compresso tipo .zip, rar, ecc. protetto da password (password da inviarsi separatamente e con sistema diverso da quello utilizzato per inviare il file); 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; è opportuno che tutti i documenti contenenti dati relativi lo stato di salute e altri dati particolari siano consegnati direttamente agli uffici amministrativi competenti al fine di evitarne la dispersione o perdita durante la trasmissione.
18. Utilizzare sempre i canali istituzionali per le comunicazioni elettroniche ad alunni, colleghi, genitori, personale della scuola o altri soggetti coinvolti, avendo sempre presente il principio di minimizzazione e di riservatezza delle comunicazioni stesse e dei dati coinvolti.
19. all'atto della consegna/inoltro/invio di documenti contenenti dati personali l'incaricato dovrà altresì verificare la corrispondenza tra il documento da trasmettere e il soggetto destinatario della comunicazione.
20. Garantire la riservatezza ed integrità dei messaggi di posta elettronica; è vietato cedere a terzi qualsiasi informazione, anche in forma sintetica, sul contenuto del messaggio ricevuto tramite posta elettronica. L'Utente si assume ogni responsabilità penale e civile ed il carico di ogni eventuale onere derivante dall'uso improprio del servizio.
21. tutte le comunicazioni elettroniche rivolte a più destinatari dovranno essere eseguite in copia conoscenza nascosta (CCN) per evitare di rendere pubblici dati personali a tutti i destinatari.
22. Epurare dai documenti, per i quali vi è un obbligo di pubblicazione in capo all'Amministrazione, tutti i dati personali non strettamente necessari al raggiungimento delle finalità di pubblicità e trasparenza dell'istituto.
23. Tutte le attrezzature informatiche (PC, LIM, schermi TV ecc) della Scuola devono essere utilizzate esclusivamente per lo svolgimento delle attività didattiche, per le esigenze dell'ufficio di segreteria e di Presidenza e in generale per tutte le attività didattiche o propedeutiche alla gestione degli alunni e genitori, personale ATA e Docenti, contabilità e finanza, protocollo e archivio, corrispondenza ordinaria.
24. non è consentito servirsi delle attrezzature informatiche per uso personale e/o privato.
25. le apparecchiature tecnologiche (hardware, software e configurazioni varie) sono gestite dall'amministratore di sistema e/o dalle ditte incaricate della manutenzione.
26. Non scaricare o salvare file di origine incerta sul PC, né aprire o inoltrare e-mail provenienti da mittenti sconosciuti o appartenenti a catene e mailing list
27. non salvare documenti contenenti dati personali sulla memoria del computer o su altri dispositivi elettronici (videocamera, fotocamera ecc..) dotati di scheda di memoria (tutte le attrezzature vengono ciclicamente formattate, pertanto i dati presenti vengono cancellati senza preavviso); se necessario, utilizzare servizi di cloud storage (Google Drive, Dropbox, iCloud, One Drive, ecc.) istituzionali o dispositivi di memoria rimovibili, ricorrendo sempre a sistemi di archiviazione sicuri (pseudonimizzare o

cifrare i documenti). Al termine del lavoro, rimuovere e cancellare dalla memoria del computer o di altri dispositivi elettronici (videocamera, fotocamera ecc..) i dati personali eventualmente presenti

28. Il salvataggio di dati, documenti e cartelle deve avvenire su server o in cloud. È opportuno seguire il principio di clear screen ("schermo pulito"), evitando di conservare i file sul desktop del PC per assicurare la disponibilità degli stessi in caso di malfunzionamento o compromissione della macchina
29. Garantire la sicurezza dei dati attraverso la distruzione di documenti o fotocopie non necessari o non più utilizzati. La cancellazione deve avvenire in maniera irreversibile, assicurando l'indisponibilità dei documenti archiviati tramite, ad esempio, l'utilizzo di dispositivi distruggi documenti o l'eliminazione definitiva dai supporti informatici, ad esempio svuotando il cestino del PC e formattando i supporti di memoria esterni.
30. Accertarsi della distruzione di documenti inutilizzati contenenti dati personali, particolari e giudiziari.
31. assicurarsi di aver eseguito il logout da qualsiasi piattaforma web o dai programmi utilizzati e spegnere correttamente tutte le attrezzature utilizzate (PC, Lim, notebook, tablet, proiettori, ecc.) al termine della sessione di lavoro, non solo per evitare accessi non autorizzati ma anche per garantire il corretto funzionamento delle stesse.
32. Il personale deve, prima di lanciare una stampa, verificare che le impostazioni di stampa e la carta presente nel cassetto della stampante siano adeguate alle sue esigenze.
33. Qualora, a stampa iniziata, il personale dovesse riscontrare anomalie, ad esempio perché la stessa non risponde alle sue aspettative, il medesimo deve annullare prontamente il prosieguo premendo il tasto annulla sulla stampante stessa
34. Una volta inviato in stampa il file il personale deve prontamente recarsi presso la stampante e raccogliere il documento.
35. Nel caso in cui la stampante non dovesse funzionare correttamente, è necessario eliminare la coda di stampa, operazione che può svolgere da solo dal PC che ha utilizzato.
36. È vietato lasciare nel cassetto di uscita della stampante il documento inviato.
37. Il personale è tenuto a segnalare prontamente eventuali guasti delle attrezzature contattando il personale tecnico di competenza.
38. Ogni responsabilità relativa al corretto uso delle macchine è attribuito al personale scolastico utilizzatore.  
Si richiama, all'occorrenza, l'osservanza integrale delle **«linee guida in tema di privacy e sicurezza informatica per il trattamento di dati personali effettuato al di fuori della sede di lavoro e/o mediante le modalità di svolgimento agile della prestazione lavorativa».**

Si allegano le linee guida specifiche per il personale amministrativo.

La Dirigente Scolastica

**Prof.ssa Angela Scatigna**

Documento informatico firmato digitalmente  
ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate,  
il quale sostituisce il documento cartaceo  
e la firma autografa

# **Linee guida specifiche per il personale amministrativo**

## **Misure operative per garantire la sicurezza del trattamento dati**

### **GDPR Regolamento UE 679/2016**

---

1. Garantire la segretezza delle credenziali riservate per l'accesso a qualunque area riservata connessa al proprio incarico. Si rammenta, inoltre, che non è consentito memorizzare tali credenziali nei browser.
2. Acquisire i certificati medici esibiti dagli alunni a giustificazione delle assenze (o qualunque altro documento contenente dati personali o particolari) direttamente dei collaboratori scolastici delegati alla consegna in segreteria.
3. Le copie della documentazione relativa ai Piani Didattici Personalizzati e i Piani Educativi Individuali sottoscritti dai docenti e dai genitori devono essere autorizzate dal titolare del trattamento e saranno prive dei dati personali che possano consentire l'individuazione dell'alunno.

**Nell'uso dei PC e delle dotazioni tecnologiche dell'Istituto è necessario attenersi alle seguenti istruzioni operative:**

1. È vietato l'utilizzo di Pen Drive, Hard Disk portatili e ogni altro dispositivo di storage personale, ovvero l'utilizzo di tali dispositivi è condizionato alla predisposizione preventiva degli stessi con tecniche crittografiche;
2. È vietato memorizzare documenti sui PC della scuola;
3. Curare la conservazione e la segretezza delle proprie credenziali di accesso alle diverse aree riservate; Le password impostate devono essere di tipologia "forte", intendendosi una combinazione casuale di lettere (maiuscole e minuscole), numeri, caratteri speciali, in alcun modo riconducibile al titolare dell'account.
4. È vietata la consultazione della propria casella di posta elettronica sui PC della scuola;
5. Nel caso in cui sia necessario accedere ad un proprio account di servizi cloud (ad esempio Google Drive), al termine dell'utilizzo assicurarsi che sia avvenuta la disconnessione dal proprio account.
6. Comunicare tempestivamente al Titolare qualunque anomalia riscontrata nel funzionamento del computer;
7. Spegnerne correttamente il computer al termine di ogni sessione di lavoro, evitando di abbandonare la propria postazione di lavoro senza averla spenta.