**ISTITUTO COMPRENSIVO STATALE "FILIPPO MAZZEI"**
Via Don Lorenzo Milani 2/4, 59016 - Poggio a Caiano (PO)
*e-mail:* poic81000b@istruzione.it, PEC: poic81000b@pec.istruzione.it
Sito Web: https://www.icfilippomazzei.edu.it
*Tel.* 055/8778366 – *C.F.84032620480*

**Prot.**

**A tutti gli assistenti amministrativi**

# Istruzioni generali per il trattamento dei dati personali, ai sensi degli artt. 29 e 32 del GDPR 2016/679, per gli Assistenti Amministrativi

Definizioni utili alla lettura del documento:

**Dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile mediante riferimento a qualsiasi altra informazione disponibile.

**Dato particolare**: i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

**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;

**Titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

**Autorizzati al trattamento**: le persone fisiche autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare del trattamento (o del responsabile).

***

L'Istituto Comprensivo Statale "Filippo Mazzei", in persona del Dirigente Scolastico (di seguito, la "**Scuola**"), in qualità di Titolare del trattamento dei dati personali raccolti nell'ambito della propria organizzazione, considerato che ai sensi dell'art. 29 del Regolamento (UE) 2016/679 "*chiunque agisca sotto… [l'] autorità …del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento*", fornisce di seguito le **istruzioni/regole** che tutti gli assistenti amministrativi, di ruolo o supplenti (di seguito gli "**Addetti**"), sono tenuti ad osservare per assicurare il corretto trattamento dei dati personali di cui vengono a conoscenza nell'ambito dello svolgimento della propria attività professionale, secondo il proprio ruolo e mansione definiti contrattualmente e nella documentazione interna rilevante (come il mansionario).

Considerato che tutti gli Addetti operano trattamenti affini per finalità e modalità, la Scuola provvede ad individuare in modo uniforme l'ambito di trattamento a loro consentito e le relative istruzioni e pertanto con la presente

**AUTORIZZA**

ciascun Addetto a compiere - con strumenti sia cartacei, sia elettronici e con modalità automatiche e manuali - le operazioni di trattamento di dati personali limitatamente a quanto necessario per l'esecuzione delle attività affidate e secondo le seguenti informazioni e istruzioni e di quelle che verranno di volta in volta comunicate dalla Scuola (come nell'ambito di circolari, ordini di servizio, policy, *etc.*) e comunque nel rispetto della normativa in materia di protezione dei dati personali vigente.

Salvo espressa e diretta autorizzazione (anche verbale) della Scuola, gli Addetti non sono autorizzati a eseguire trattamenti con finalità diverse da quelle strettamente necessarie allo svolgimento dei compiti agli stessi assegnati e derivanti dall'area di assegnazione risultante dal piano delle attività e dagli ordini di servizio.

Gli Addetti, nella loro qualità di Autorizzati al Trattamento, nell'esecuzione dell'incarico, sono tutti tenuti a seguire le seguenti

**Istruzioni:**

1. operare in modo lecito e corretto; pertanto, dovranno:

- trattare i Dati Personali esclusivamente al fine di adempiere alle obbligazioni nascenti dal proprio ruolo e funzione e, in ogni caso, per gli scopi per i quali i Dati Personali sono stati raccolti;

- verificare la completezza e la pertinenza dei Dati Personali trattati, nonché la loro non eccedenza rispetto alle finalità della relativa raccolta e del successivo trattamento. In ogni caso, i Dati Personali non potranno essere comunicati a terzi e diffusi, salvo che la Scuola per esigenze scolastiche e educative ovvero pubbliche e di interesse generale e per qualsiasi altra legittima motivazione disponga diversamente;

- prestare particolare attenzione ai dati classificati come particolari (già dati sensibili);

- procedere alle operazioni di trattamento in condizioni che assicurino che i Dati Personali agli stessi affidati e i documenti in cui sono contenuti non siano accessibili a soggetti non autorizzati, seppure dipendenti o Addetti della Scuola. I Dati Personali devono quindi essere potetti da accessi non autorizzati, che possono avvenire di persona (si pensi a un soggetto non autorizzato che entra fisicamente in un ufficio e prova a conoscere o sottrarre dati) o tramite contatti telematici o telefonici che possono rivelarsi truffaldini (ad esempio una telefonata mediante la quale si provino a raccogliere determinati dati o informazioni);

2. ove possibile, verificare l'esattezza dei Dati Personali trattati e, se necessario, opportunamente aggiornarli e/o informare direttamente il Dirigente (anche per il tramite del responsabile dell'area di competenza) di ogni variazione intervenuta o inesattezza constatata;

**3.** custodire con cura i supporti esterni (es. chiavette USB, dischi esterni, tablet, smartphone, *etc.*), evitando di lasciarli in luoghi non protetti;

**4.** in caso di interruzione, anche temporanea, delle operazioni di trattamento, verificare che i Dati Personali non siano accessibili a terzi non autorizzati. In particolare, i documenti cartacei contenenti Dati Personali, quando non presidiati, dovranno essere, conservati e custoditi in armadi/cassettiere adeguatamente chiusi o in altri contenitori protetti e non accessibili a soggetti non autorizzati. Parimenti, al fine di proteggere la documentazione memorizzata su supporti informatici, si precisa che l'Addetto non dovrà lasciare incustodito il dispositivo eventualmente assegnato o a sua disposizione (in caso di dispositivi condivisi) con sessioni applicative aperte o con login effettuato, ma dovrà assicurarsi di proteggere il dispositivo e il relativo contenuto tramite l'uso di password o altri tipi di blocchi/controlli come, ad esempio, *screen saver*;

5. al termine di ciascuna attività che comporta un trattamento di dati personali (come la consultazione di documenti, l'archiviazione, *etc*.) e, in particolare, delle proprie ore di servizio, riporre/chiudere i documenti/file contenenti i Dati Personali negli appositi archivi cartacei ed elettronici. Richiamato quanto detto al punto precedente in merito all'accesso a strumenti informatici da parte degli Addetti, tutti i computer (desktop e portatili) che vengono usati a Scuola, al termine delle ore di servizio, devono essere spenti, a meno che per particolari ragioni tecniche o di servizio debbano rimanere in funzione (in tal caso, il computer acceso deve risiedere in un ufficio o in un locale chiuso a chiave o protetto e con salvaschermo attivo e protetto da credenziali);

6. non creare archivi o banche dati nuove senza espressa autorizzazione da parte della Scuola, né effettuare *backup*, anche parziali, su sistemi e supporti, anche rimovibili, diversi da quelli messi a disposizione dalla Scuola e senza il preventivo consenso di quest'ultima;

7. prestare attenzione alla stampa di documenti su stampanti condivise o fotocopiatrici di rete, avendo cura di recuperare tempestivamente la stampa e di non lasciare i documenti incustoditi. La protezione dei dati si applica anche a documenti cartacei, cui va garantita custodia e controllo. Non riutilizzare per appunti il retro di fogli stampati o fotocopiati se contengono dati personali. Qualora sia fornito, è sempre necessario utilizzare il "distruggi-documenti" per rendere non leggibili i documenti contenenti dati personali o informazioni rilevanti. Nel caso si debbano smaltire grandi moli di documenti cartacei connessi all'attività di ricerca e didattica (esempio documenti correlati a prove d'esame di studenti) e contenenti dati personali è necessario contattare il Dirigente Scolastico per ottenere l'autorizzazione da parte della Soprintendenza Archivistica competente e quindi fruire, nel caso, del servizio di gestione dei rifiuti;

8. garantire la massima riservatezza durante lo svolgimento delle operazioni di trattamento e quindi applicare le misure di sicurezza previste dalla presente lettera o comunque impartite, anche verbalmente, dalla Scuola. A tale proposito, si precisa che qualora gli Addetti nello svolgimento delle proprie funzioni dovessero accedere a strumenti e servizi dotati di procedure di autenticazione, sono tenuti a conservare le proprie credenziali, così come l'eventuale parola chiave, con la massima segretezza e utilizzarle in modo esclusivo, senza comunicarle ad altri, ad eccezione del Dirigente, della coordinatrice o del personale

tecnico addetto all'infrastruttura informatica in caso di particolare necessità o urgenza. Infatti, qualora l'accesso ai Dati Personali e agli strumenti elettronici sia consentito esclusivamente tramite uso della componente riservata della credenziale per l'autenticazione, la Scuola, in caso di prolungata assenza o impedimento dell'Addetto, potrà assicurare la disponibilità dei dati o degli strumenti elettronici qualora ciò si rendesse indispensabile e indifferibile, per esclusive necessità di operatività e di sicurezza del sistema e/o per l'ottimale svolgimento delle attività della Scuola, accendendo agli stessi. Per tale caso, la Scuola – per il tramite dell'amministratore di sistema se designato o del personale tecnico interno o del consulente informatico esterno – è autorizzata a modificare le credenziali di autenticazione dell'Addetto assente o impedito, dando a quest'ultimo tempestiva comunicazione, e che comunque l'Addetto provvederà a cambiare una volta rientrato o comunque operativo/reperibile;

9. sempre in un'ottica di massima tutela della riservatezza dei dati personali per l'uso del Registro Elettronico, della Posta elettronica e degli applicativi utilizzati per la gestione della segreteria (tra cui il SIDI), scegliere una password con le seguenti caratteristiche: originale, composta da almeno otto caratteri, che contenga almeno un numero e 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) e cambiarla periodicamente (almeno una volta ogni tre mesi) e ogni volta che ci sia il rischio che la sicurezza della password sia stata compromessa (poiché, ad esempio, entrata nella disponibilità di terzi non autorizzati o comunque conoscibile dagli stessi);

10. segnalare prontamente alla Scuola ogni tentativo di violazione, illecito, errore e/o anomalia riscontrati;

11. mantenere sempre un atteggiamento prudenziale e rispondere sempre in maniera negativa a richieste di dati, effettuate in qualunque modo, che non pervengano chiaramente da soggetti autorizzati, e la cui identità, in caso di dubbio, non sia stata accuratamente verificata. Le richieste di dati devono avvenire obbligatoriamente in forma scritta e, nel caso, autorizzate dal Dirigente Scolastico. È vietato, altresì, fornire o rendere disponibili informazioni tecniche, riferite alla rete e ai sistemi della Scuola, alle policies e alle credenziali usate, ai software e alle applicazioni utilizzate, a soggetti esterni alla Scuola. Tali informazioni sono solitamente domandate per cercare di violare i sistemi della Scuola. Inoltre non devono essere fornite informazioni personali riservate, come i motivi dell'assenza di un dipendente o il numero telefonico personale del lavoratore etc., nonché deve essere sempre valutata la pertinenza e la legittimità della richiesta. Si precisa altresì che le comunicazioni agli interessati (persone fisiche a cui afferiscono i dati personali) dovranno avvenire in forma riservata e personale;

12. utilizzare la strumentazione informatica fornita dalla scuola, la posta istituzionale, gli applicativi e la rete internet solamente per finalità lavorative, applicando le qui elencate istruzioni;

13. partecipare ai corsi di formazione finalizzati a renderlo edotto dei rischi connessi alle operazioni di trattamento ed alla sua istruzione circa le modalità per prevenire eventuali danni o dispersioni dei Dati Personali;

14. applicare le misure di sicurezza impartite dalla Scuola in qualsiasi tempo, per iscritto o verbalmente e in particolare con le procedure eventualmente predisposte dalla Scuola per l'uso del proprio materiale informativo ed eventualmente dei device personali, ove esplicitamente consentiti dalla Scuola.

Fermo restando quanto sopra, la Scuola rinvia alle ulteriori policy inerenti, ad esempio, all'uso degli strumenti elettronici (sia hardware che software), nonché a eventuali procedure o manuali in relazione a specifiche situazioni/modalità di svolgimento delle attività o inerenti alla gestione di eventi particolari (tra cui, ad esempio, incidenti informatici, violazione dei dati, *etc.*), riservandosi la facoltà di fornire, in ogni momento, ulteriori e diverse indicazioni in merito a tali aspetti.

**Obblighi di riservatezza**

Gli Addetti non potranno comunicare o diffondere i Dati Personali senza la preventiva autorizzazione scritta della Scuola, salvi i casi previsti dalla legge o in forza di ordini dell'Autorità giudiziaria.

I suddetti obblighi dovranno essere osservati per l'intera durata del rapporto di lavoro instaurato ed anche dopo la relativa cessazione, salvo in relazione a quei dati personali che la Scuola (anche in ragione dei propri doveri di trasparenza) abbia reso pubblici o che comunque siano divenuti lecitamente tali (non si considerano lecitamente pubbliche quelle rese note in violazione di quanto previsto dalla Scuola e più in generale della normativa vigente e rilevante in materia), fermo restando che con riferimento ai dati personali, a prescindere dalla pubblicazione degli stessi da parte della Scuola qualora ricorrano le basi giuridiche, sussiste in ogni caso l'obbligo dell'Addetto di rispettare i principi, limiti e divieti e le condizioni di liceità di trattamento di dati personali previsti dalla normativa vigente in materia di privacy (anche con riferimento alle limitazioni di trattamento dei dati resi manifestamente pubblici).

**Disposizioni finali**

La presente lettera di autorizzazione è rilasciata ai sensi della normativa sulla protezione dei dati personali e non attribuisce agli Addetti alcun diritto o aspettativa a ricevere qualsiasi ulteriore compenso, essendo l'adempimento delle relative istruzioni parte integrante della prestazione contrattuale e di quella di servizio presso la Scuola e, come tale, già remunerato.

La Scuola potrà in qualsiasi momento fornire istruzioni aggiuntive, anche verbalmente, o modificare quelle precedentemente impartite.

Gli Addetti potranno rivolgersi alla Scuola per qualsiasi ulteriore informazione concernente la presente lettera e le operazioni loro affidate.

Il Dirigente Scolastico

**ISTITUTO COMPRENSIVO STATALE "FILIPPO MAZZEI"**
Via Don Lorenzo Milani 2/4, 59016 - Poggio a Caiano (PO)
*e-mail:* poic81000b@istruzione.it, PEC: poic81000b@pec.istruzione.it
Sito Web: https://www.icfilippomazzei.edu.it
*Tel.* 055/8778366 – *C.F.84032620480*