Ministero dell'Istruzione, dell'Università e della Ricerca
UFFICIO SCOLASTICO REGIONALE PER LA CAMPANIA
ISTITUTO COMPRENSIVO S.GIOVANNI A PIRO "T. GAZA"
VIA CENOBIO, 4/B
84070 SAN GIOVANNI A PIRO (SA)
Codice Fiscale: 84001740657 Codice Meccanografico: SAIC815005

LETTERA DI INCARICO
A PERSONA AUTORIZZATA AL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 29 DEL GDPR

Premesso che:
- Il Regolamento Europeo 2016/679 del 27 aprile 2016 (c.d. GDPR – *General Data Protection Regulation*) stabilisce le norme relative alla protezione delle persone fisiche, con riguardo al trattamento dei loro dati personali, nonché alla libera circolazione di essi;
- Il Regolamento Europeo 2016/679, individuando i soggetti preposti al trattamento dei dati personali, annovera le "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare" (art. 4 n. 10 GDPR);
con la presente lettera:

La dott.ssa Maria Teresa Tancredi C.F. TNCMTR70L50E409G nella persona del suo legale rappresentante pro tempore, con sede in Via Cenobio 4/B, 84070 San Giovanni a Piro (SA), in qualità di **Titolare del trattamento** dei dati ex artt. 24 ss. GDPR

NOMINA quale
PERSONA AUTORIZZATA E INCARICATA AL TRATTAMENTO DEI DATI PERSONALI

Nome _____

Cognome _____

C.F. _____

Nato/a _____ il _____

ai sensi e per gli effetti del Regolamento Europeo 2016/679.

Con la presente lettera, l'incaricato viene autorizzato ed istruito a trattare i dati personali dei quali verrà a conoscenza durante lo svolgimento della propria mansione lavorativa prestata in virtù del regolare contratto di lavoro stipulato con il Titolare.

Il trattamento autorizzato deve avvenire nel rispetto dei principi, dei diritti, dei doveri e degli adempimenti predisposti dal Regolamento 2016/679: pertanto, sulla base di tale normativa, impartite le seguenti **ISTRUZIONI atte a garantire un corretto, lecito e trasparente trattamento di tutti i dati personali ai quali l'incaricato avrà accesso.**
Le istruzioni costituiscono parte integrante della presente lettera di incarico.

1) **TRATTAMENTO DEI DATI PERSONALI**

L'incaricato è autorizzato al **trattamento dei dati personali solo ed esclusivamente nei limiti delle finalità inerenti lo svolgimento delle proprie mansioni contrattuali previste dal contratto di lavoro sottoscritto con il Titolare.** Al riguardo, il trattamento deve sempre essere adeguato, pertinente e limitato a tali finalità.

L'incaricato deve prestare particolare attenzione all'esattezza dei dati trattati e provvedere, inoltre, all'aggiornamento degli stessi. Coerentemente a questo scopo, devono essere rispettate e seguite tutte le misure ragionevoli e indispensabili per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

I dati oggetto del trattamento al quale è autorizzato l'incaricato sono i seguenti:

	Tipologia dato trattato	**Finalità trattamento**
x	Personali comuni	Raccolta nomi per mensa raccolta nominativi allievi archiviazione
x	Particolari ex art. 9 GDPR	
x	Giudiziari ex art. 10 GDPR	

2) **COMUNICAZIONE E DIFFUSIONE DEI DATI**

La comunicazione dei dati trattati è consentita solo all'interno dell'*equipe* lavorativa del Titolare e, comunque, nei limiti della stretta indispensabilità e pertinenza rispetto alle mansioni lavorative svolte.

La comunicazione è altresì consentita verso soggetti esterni espressamente e preventivamente individuati dal Titolare.

È vietato effettuare riprese fotografiche o video durante l'espletamento delle proprie mansioni, senza previa autorizzazione del Titolare.

Qualora vi sia autorizzazione, il trattamento delle immagini, è sottoposto alle medesime istruzioni e misure di sicurezza previste dal presente incarico.

3) **MISURE DI SICUREZZA**

La persona autorizzata al trattamento dei dati personali è tenuta ad osservare tutte le misure di protezione e sicurezza - già predisposte dal titolare, nonché quelle che in futuro verranno adottate -, di tipo organizzativo e tecnico, atte garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento e, quindi al contempo, volte ad evitare qualsiasi violazione dei dati personali come la perdita, l'accesso non autorizzato e/o il trattamento non consentito.

- **Misure di sicurezza organizzative**

L'incaricato al trattamento dei dati è tenuto a frequentare corsi di formazione e di aggiornamento finalizzati ad illustrare quanto disciplinato dal Regolamento Europeo e da tutta la normativa in materia di privacy, con particolare attenzione agli adempimenti richiesti dalla normativa.

La persona autorizzata deve, in ogni caso, rispettare le regole di condotta contenute dal regolamento interno appositamente predisposto dal Titolare per garantire sul luogo di lavoro la corretta applicazione del Regolamento Europeo.

Al riguardo, con riferimento agli strumenti di lavoro (così come indicati nel codice regolamento interno, si precisa che è vietato ogni loro utilizzo non inerente all'attività lavorativa in quanto, lo stesso, potrebbe contribuire a determinare la perdita, la distruzione o un errato impiego dei dati personali oggetto del trattamento autorizzato.

A titolo esemplificativo, l'incaricato non può creare nuove ed autonome banche dati contenenti dati personali, salva preventiva autorizzazione del titolare.

- **Misure di sicurezza tecniche:**

Sistemi informatici- misure minime

La postazione informatica non va lasciata incustodita, permettendo il libero accesso ai dati. **Le proprie credenziali di autenticazione devono essere riservate; in particolare, ciascun computer dev'essere protetto da una password alfanumerica di almeno otto caratteri, associata ad una parola chiave o ad uno username**. Né la password, né la parola chiave, né lo username possono essere associabili alla persona autorizzata al trattamento dei dati personali. La password dev'essere rinnovata ogni tre mesi.

Una volta ultimato il trattamento tramite lo strumento informatico, è obbligatorio uscire dall'applicazione che consente il trattamento stesso.

Tutti i supporti magnetici utilizzati vanno risposti negli archivi a ciò preposti; i supporti non più utilizzati possono essere eliminati solo dopo che i dati contenuti sono stati resi effettivamente inutilizzabili.

Qualora sorgessero esigenze aziendali, il Titolare potrà accedere ai dati trattati dall'incaricato e agli strumenti informatici in dotazione al medesimo, mediante l'intervento dell'Amministratore di Sistema o del Responsabile addetto ai sistemi IT.
Gli strumenti informatici e telematici messi a disposizione (esempio computer, smartphone, software, navigazione web, e-mail, così come altri strumenti indicati nel regolamento interno costituiscono strumenti di lavoro da utilizzare esclusivamente per l'esecuzione delle mansioni affidate.
L'incaricato può accedere soltanto agli archivi informatici strettamente inerenti alla mansione svolta.
A tal fine, l'accesso ad alcuni archivi verrà consentito esclusivamente a chi, in virtù della mansione svolta, abbia necessità di consultarli, aggiornarli, implementarli, ecc..
La persona autorizzata non può installare ed utilizzare programmi informatici non autorizzati dal titolare, o privi di licenza che ne legittimi l'uso; in particolare, non può scaricare della rete internet alcun programma applicativo, né per un proprio uso personale, né se destinato allo svolgimento della propria mansione (salva autorizzazione del titolare).
Non è altresì consentito l'uso di supporti magnetici personali, (es. chiavette USB, CD, hardisk), senza l'approvazione del titolare del trattamento.
Non è consentito alcun trasferimento di dati archiviati nei server aziendali, o presenti in qualsiasi altro strumento di lavoro, mediante l'utilizzo di supporti magnetici personali, posta elettronica, *cloud* ad uso personale, o altri strumenti ancora.

Trattamenti cartacei

Nell'osservanza del principio di stretta pertinenza e indispensabilità del trattamento rispetto alle mansioni svolte, la persona autorizzata può accedere soltanto agli inerenti archivi di banche dati cartacei.
La persona autorizzata è tenuta a custodire i dati conservati negli archivi, in modo tale da impedirne l'accesso a persone prive di autorizzazione.
Una volta effettuato il trattamento e comunque ogni volta che la persona autorizzata si allontani dalla sua postazione di lavoro, i documenti cartacei devono essere riordinati nell'archivio appositamente predisposto dal titolare e, comunque, non lasciati nella disponibilità di terze parti.
Allo scopo di accedere agli archivi materializzati, alla persona autorizzata vengono consegnate le chiavi di accesso, da conservare con cura, oppure viene indicato il luogo protetto dove possono essere reperite/riposte.
Nello specifico:
- qualora i documenti riportanti dati personali siano riposti in armadi dotati di serratura, le chiavi non possono essere affidate a terzi non autorizzati, oppure lasciate nella serratura, ma devono essere custodite in un luogo non visibile;
- qualora i documenti riportanti dati personali siano archiviati su scaffali non protetti da qualsivoglia barriera fisica, la persona autorizzata deve curarsi di chiudere a chiave la porta del locale dove gli scaffali stessi sono collocati, non deve affidare la chiave a terzi non autorizzati, oppure lasciarla nella serratura, ma deve custodirla in un luogo non visibile.
Là dove vi siano archivi con porta a vetri e non costituiti da armadi dotati di serratura, i documenti devono comunque essere coperti o girati, in modo tale da non rendere possibile la lettura a terzi non autorizzati.
I documenti non possono essere portati al di fuori del luogo di lavoro, salvo i casi di comunicazione a terzi preventivamente individuati ed autorizzati del titolare come destinatari.
Eventuali copie riprodotte devono essere riposte anch'esse nell'apposito archivio, oppure essere distrutte, in modo tale da non permetterne la lettura a terze parti.
Fermo restando tutto quanto esposto nella presente lettera, per qualsiasi altra regola di condotta si rinvia integralmente al codice deontologico/regolamento interno/policy aziendale adottato dal Titolare.

4) RESPONSABILITÀ

L'incaricato, in caso di violazione delle istruzioni qui impartite (o quelle alle quali in ogni caso si rimanda in quanto contenute nel regolamento interno) potrà essere ritenuto responsabile di eventuali danni al trattamento dei dati per il quale è stato incaricato e, per tali motivazioni, potrà essere soggetto all'applicazione di sanzioni disciplinari.

5) DEFINIZIONI DI LEGGE

L'art. 4 n. 1) del Regolamento definisce il **dato personale** come "*qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

L'art. 4 n. 2) del Regolamento definisce il **trattamento** come "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme 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*".

L'art. 4 n. 6) del Regolamento definisce l'**archivio** come *"qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico"*.

L'art. 4 n. 7) del Regolamento definisce il **titolare del trattamento** come *"la persona fisica o giuridica, l'autorità pubblica, il servizio o al organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali"*.

L'art. 4 n. 11) del Regolamento definisce il **consenso** come "*qualsiasi manifestazione di volontà libera, specifica, informata, inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*".

L'art. 4 n. 12) del Regolamento definisce il la **violazione dei dati personali** come *"la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso dei dati personali trasmessi, conservati o comunque trattati"*.

L'art. 32 del Regolamento comprende, fra le **misure di sicurezza tecniche ed organizzative** applicabili, *"la pseudonimizzazione e la cifratura dei dati personali, la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento"*.

Luogo_____, data_____

Il Titolare del Trattamento

_____

L'incaricato al Trattamento

_____