ISTITUTO COMPRENSIVO “ROMAGNOLI – SOLITO” GELA (CL)

in Via Volturno, 28- 93012 Gela (CL)
Cod. Mecc.: CLIC83200Q
Tel. 0933930934 - E-mail: clic83200q@istruzione.it t - PEC: clic83200q@pec.istruzione.it
Sito web: https://istitutocomprensivoromagnoligela.edu.it/

Gela, ___/___/_____

Al Personale Docente
dell’Istituto Comprensivo “Romagnoli – Solito” Gela

OGGETTO: Designazione/Autorizzazione del Personale Docente quale “persona autorizzata al trattamento” e istruzioni operative (art. 29 Reg. UE 2016/679 - GDPR; art. 32, par. 4 GDPR; art. 2-quaterdecies D.Lgs. 196/2003).

Il sottoscritto Prof. Gianfranco Mancuso, Dirigente Scolastico pro tempore dell’Istituto Comprensivo “Romagnoli – Solito” Gela (CL) in qualità di legale rappresentante e Titolare del trattamento dei dati personali trattati nell’ambito delle attività istituzionali, con il presente atto DESIGNA/AUTORIZZA e impartisce istruzioni operative al Personale Docente, quale categoria omogenea, affinché il trattamento dei dati personali avvenga esclusivamente per finalità istituzionali e nei limiti delle mansioni effettivamente svolte.

VISTI gli artt. 5, 24, 29 e 32 del Regolamento (UE) 2016/679;

VISTI gli artt. 2-quaterdecies e 2-quinquiesdecies del D.Lgs. 196/2003 e s.m.i., per quanto compatibili;

CONSIDERATO che, nello svolgimento delle attività didattiche, educative e connesse funzioni organizzative, il Personale Docente può venire a conoscenza e/o trattare dati personali relativi ad alunni, famiglie, personale scolastico e altri interessati;

RITENUTO necessario definire in modo uniforme istruzioni operative e misure di riservatezza e sicurezza applicabili al Personale Docente, anche in relazione all’utilizzo di strumenti digitali e piattaforme istituzionali;

DISPONE quanto segue.

1. PERSONALE AUTORIZZATO

Con il presente atto, il Titolare autorizza e istruisce, ai sensi dell’art. 29 GDPR e dell’art. 2-quaterdecies del D.Lgs. 196/2003, il Personale Docente in servizio presso l’Istituto (a tempo indeterminato o determinato, supplenti brevi, docenti di sostegno, docenti incaricati di funzioni/attività aggiuntive o progettuali), quale “personale autorizzato al trattamento”. L’autorizzazione opera nei limiti delle mansioni effettivamente svolte, dei profili di accesso assegnati e delle istruzioni interne tempo per tempo vigenti.

2. AMBITO DI APPLICAZIONE E LIMITI

L'autorizzazione riguarda esclusivamente i trattamenti di dati personali strettamente necessari all'espletamento delle attività istituzionali e didattiche dell'Istituto, nel rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione dei dati, limitazione della conservazione e riservatezza. A titolo esemplificativo e non esaustivo rientrano nell'ambito: dati anagrafici e di contatto di alunni e famiglie; dati relativi a frequenza, attività didattiche, valutazioni, esiti, registri e verbali; documentazione connessa a inclusione e bisogni educativi (BES/DSA, PDP, PEI) e, quando indispensabili, categorie particolari di dati ai sensi dell'art. 9 GDPR (es. dati sulla salute/disabilità), trattati secondo le procedure interne e con specifiche cautele (accessi limitati, riservatezza, conservazione protetta). Nei casi previsti dalla normativa di settore, possono essere trattati anche eventuali dati relativi a condanne penali e reati ex art. 10 GDPR, esclusivamente nei limiti delle competenze istituzionali e delle istruzioni impartite.

È fatto divieto di effettuare trattamenti non pertinenti alle mansioni affidate, eccedenti rispetto alle finalità istituzionali o svolti con modalità difformi dalle istruzioni operative, incluse le policy e i regolamenti interni. In particolare, è vietato: accedere a dati non necessari; acquisire o conservare copie ulteriori di documenti senza necessità; utilizzare canali o strumenti non autorizzati; comunicare informazioni a soggetti non legittimati o senza idonea verifica dei presupposti. Ogni comunicazione di dati deve avvenire esclusivamente verso destinatari legittimati e con strumenti istituzionali, adottando cautele adeguate (verifica del destinatario, limitazione degli allegati, eventuale oscuramento dei dati non necessari).

È altresì vietata la diffusione di dati personali (anche tramite canali digitali, piattaforme non istituzionali o social network) salvo che ciò sia previsto da norme o espressamente autorizzato dal Titolare secondo le procedure interne. Rientrano nella "diffusione", a titolo esemplificativo, la pubblicazione su siti web, bacheche digitali, social, gruppi/ chat non istituzionali e la condivisione pubblica di immagini, video, elaborati o altri contenuti idonei a identificare gli interessati. Eventuali attività di pubblicazione o comunicazione esterna devono rispettare il principio di minimizzazione, prevedere (ove necessario) idonee basi giuridiche e/o consensi e utilizzare esclusivamente canali e modalità approvate dall'Istituto, con particolare attenzione ai dati di minori e alle informazioni idonee a rivelare condizioni di salute, situazioni di fragilità o altri profili meritevoli di tutela rafforzata.

3. PRINCIPI E ISTRUZIONI OPERATIVE OBBLIGATORIE

Ai sensi dell'art. 29 GDPR e dell'art. 32, par. 4 GDPR, il Personale autorizzato è tenuto a trattare i dati personali esclusivamente nell'ambito delle attività istituzionali dell'Istituto e nel rispetto delle istruzioni impartite dal Titolare, delle procedure interne e delle policy organizzative e informatiche vigenti. Le presenti indicazioni hanno l'obiettivo di garantire un trattamento corretto, sicuro e tracciabile, riducendo i rischi di accessi non autorizzati, perdite di riservatezza, errori di comunicazione e trattamenti eccedenti, con particolare attenzione ai dati riferiti a minori e alle categorie di dati che richiedono tutele rafforzate.

In particolare, ciascun autorizzato è tenuto ad adottare comportamenti coerenti con il principio del "minimo privilegio" (accesso solo a ciò che serve) e a mantenere un livello costante di attenzione nella gestione quotidiana di registri, documenti, comunicazioni e strumenti digitali, anche in relazione alle attività svolte fuori sede o in modalità ibrida. Le

seguenti istruzioni operative sono da intendersi obbligatorie e si applicano sia al trattamento su supporto cartaceo sia al trattamento mediante strumenti informatici:

- trattare i dati personali nel rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione, esattezza, limitazione della conservazione e riservatezza;
- accedere esclusivamente ai dati necessari e utilizzare solo credenziali personali, mantenendole segrete e non condividendole;
- custodire con diligenza registri, verifiche, elaborati, fascicoli e documenti (cartacei e digitali), evitando l'accesso da parte di persone non autorizzate;
- adottare misure di sicurezza fisiche e logiche (es. blocco schermo, password robuste, conservazione in armadi chiusi, attenzione a stampe e fotocopie);
- non comunicare a terzi dati personali se non nei casi consentiti e secondo le procedure (es. comunicazioni scuola-famiglia e interlocuzioni con enti pubblici legittimati).

Il trattamento deve avvenire preferibilmente mediante gli strumenti e i servizi informatici istituzionali (es. registro elettronico, posta istituzionale, piattaforme didattiche adottate dall'Istituto). È vietato utilizzare account personali, servizi non autorizzati o canali informali (es. chat/social personali) per trattare o condividere dati di studenti o famiglie. L'uso di dispositivi personali per finalità istituzionali è consentito solo se espressamente autorizzato e nel rispetto delle misure di sicurezza previste.

La violazione delle presenti istruzioni, oltre a poter determinare rischi e responsabilità in materia di protezione dei dati personali, può costituire inosservanza dei doveri d'ufficio e comportare l'attivazione delle conseguenti misure organizzative e disciplinari previste dalla normativa e dal CCNL di riferimento, ferma restando ogni ulteriore responsabilità nei casi previsti.

4. TRATTAMENTI BASATI SU OBBLIGO DI LEGGE/INTERESSE PUBBLICO E, OVE PREVISTO, CONSENSO

In ambito scolastico la maggior parte dei trattamenti di dati personali avviene in esecuzione di compiti di interesse pubblico e per l'adempimento di obblighi legali cui è soggetto l'Istituto, connessi all'organizzazione del servizio di istruzione e formazione, alla gestione della carriera scolastica e alla tutela dei diritti degli studenti. Pertanto, tali trattamenti non richiedono, di regola, il consenso dell'interessato, fermo restando l'obbligo di garantire trasparenza mediante idonea informativa, nonché il rispetto dei principi di minimizzazione, correttezza e sicurezza.

Nei soli casi in cui, per specifiche attività non strettamente riconducibili alle finalità istituzionali obbligatorie, sia prevista l'acquisizione di un consenso (a titolo esemplificativo: iniziative progettuali facoltative, attività extrascolastiche non obbligatorie, partecipazione a eventi esterni, realizzazione e pubblicazione di fotografie/filmati o altri contenuti idonei a identificare gli studenti, utilizzo di immagini per comunicazione istituzionale secondo procedure interne), il Personale Docente deve attenersi rigorosamente alle istruzioni dell'Istituto, verificare che siano stati rispettati i presupposti previsti (informativa, modulistica, eventuali limiti e revocabilità) e utilizzare esclusivamente la modulistica e le procedure formalmente approvate dal Titolare.

In tali ipotesi è comunque necessario adottare cautele rafforzate, soprattutto in presenza di minori e di eventuali categorie particolari di dati (es. informazioni sulla salute o su situazioni di fragilità), evitando qualsiasi iniziativa autonoma o difforme dalle procedure interne e assicurando che la pubblicazione o comunicazione avvenga soltanto tramite canali istituzionali autorizzati e nel rispetto del principio di minimizzazione.

5. RISERVATEZZA E OBBLIGO DI SEGRETO

Il Personale Docente è tenuto alla massima riservatezza in relazione a tutte le informazioni e ai dati personali conosciuti, acquisiti o comunque trattati per ragioni di servizio, indipendentemente dalla forma in cui tali informazioni sono disponibili (verbale, cartacea o digitale). L'obbligo di riservatezza comprende, a titolo esemplificativo, dati relativi a studenti e famiglie, situazioni personali e scolastiche, valutazioni, provvedimenti, documentazione amministrativa e didattica, nonché ogni informazione idonea a rivelare condizioni di salute, disabilità, bisogni educativi speciali o altre circostanze meritevoli di tutela rafforzata.

È fatto divieto di divulgare, comunicare o rendere accessibili tali informazioni a soggetti non autorizzati, anche all'interno dell'Istituto, salvo che ciò sia necessario per finalità di servizio e nel rispetto del principio del "need to know". Il Personale è altresì tenuto ad adottare comportamenti coerenti con tale obbligo anche in contesti informali (es. conversazioni in luoghi pubblici, chat, social network, gruppi di messaggistica), evitando qualunque forma di esposizione indebita o identificabilità degli interessati.

Tale obbligo permane anche dopo la cessazione del rapporto di lavoro o collaborazione, per tutto il tempo necessario in relazione alle finalità di tutela della riservatezza e nei limiti previsti dalla normativa vigente, fermo restando che eventuali richieste di accesso, comunicazione o pubblicazione di dati e documenti dovranno essere gestite esclusivamente attraverso i canali istituzionali dell'Istituto e secondo le procedure previste.

La violazione dell'obbligo di riservatezza può determinare l'attivazione delle misure organizzative e disciplinari previste, nonché eventuali ulteriori responsabilità nei casi stabiliti dalla legge.

6. SEGNALAZIONE INCIDENTI E VIOLAZIONI (DATA BREACH)

Qualsiasi evento, anomalia o sospetto incidente che possa comportare perdita, accesso non autorizzato, divulgazione, alterazione o indisponibilità di dati personali (c.d. *data breach*), anche solo potenziale, deve essere segnalato senza ritardo e comunque immediatamente non appena conosciuto. Rientrano, a titolo esemplificativo: invio di email/PEC o allegati al destinatario errato; caricamento o condivisione non autorizzata di documenti su piattaforme digitali; smarrimento, furto o sottrazione di registri, fascicoli, chiavette USB, notebook o smartphone utilizzati per finalità di servizio; accessi anomali o sospetto furto/compromissione di credenziali; pubblicazione involontaria di dati su canali web o bacheche digitali; malfunzionamenti o blocchi che impediscano l'accesso a dati e documenti necessari.

La segnalazione deve essere effettuata immediatamente al Dirigente Scolastico e/o ai referenti interni individuati (es. DSGA/Referente privacy o altra figura incaricata), e per conoscenza al RPD/DPO ai recapiti istituzionali, fornendo tutte le informazioni utili (anche

in forma sintetica), quali: data e ora dell'evento, descrizione dell'accaduto, tipologia di dati coinvolti, categorie di interessati, eventuali destinatari non autorizzati, misure già adottate per limitare l'impatto (es. richiesta di cancellazione, revoca accessi, cambio password) e ogni ulteriore elemento disponibile.

Il Personale è tenuto a non intraprendere iniziative autonome che possano aggravare l'evento o comprometterne la gestione (es. ulteriori inoltri, tentativi non coordinati di ripristino, comunicazioni esterne), ma ad attenersi alle istruzioni fornite dal Titolare e dai referenti incaricati, al fine di consentire la tempestiva valutazione dell'evento e, se del caso, l'adozione delle misure previste dalla normativa (incluse eventuali comunicazioni all'Autorità Garante e/o agli interessati nei termini di legge).

7. DURATA, AGGIORNAMENTO, REVOCA E CONSEGUENZE IN CASO DI INOSSERVANZA

La presente designazione decorre dalla data di efficacia indicata a protocollo e resta valida fino a revoca o cessazione del rapporto di servizio. Il Titolare del trattamento può in qualsiasi momento aggiornare, integrare o revocare le presenti istruzioni (anche in relazione a nuove piattaforme, procedure o misure di sicurezza), nonché modificare i profili di accesso assegnati. Il mancato rispetto delle presenti istruzioni può comportare conseguenze disciplinari e ulteriori responsabilità previste dalla normativa vigente.

8. CONTATTI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD/DPO) E PRESA VISIONE

Per chiarimenti in materia di protezione dei dati personali e per segnalazioni inerenti alla privacy, il Responsabile della Protezione dei Dati (RPD/DPO) dell'Istituto è: Cer.Med. s.r.l. – nella persona del dott. Marco Lo Brutto – E-mail: rpd.privacy@gmail.com – PEC: cermed@legalmail.it.

Il presente atto è portato a conoscenza del Personale Docente tramite circolare interna/area riservata o mediante sottoscrizione del Registro di presa visione (Allegato 1), che costituisce evidenza dell'avvenuta informazione e consegna delle istruzioni operative. Il registro può essere integrato o sostituito da evidenza equivalente di presa visione purché sia garantita la tracciabilità dei nominativi e della data.

Il Dirigente Scolastico

Prof. Gianfranco Mancuso

(firma digitale o autografa)

ALLEGATO 1 - REGISTRO DI PRESA VISIONE

Designazione/Autorizzazione del Personale Docente quale “persona autorizzata al trattamento” (art. 29 GDPR). Il presente registro è compilato dai docenti per attestare la presa visione dell’atto e delle istruzioni operative.

N.	Cognome e Nome	Qualifica/Plesso	Data	Firma per presa visione
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				