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, ___/___/_____

Agli Assistenti Amministrativi
dell’Istituto Comprensivo “Romagnoli – Solito” Gela

OGGETTO: Designazione/Autorizzazione degli Assistenti Amministrativi 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’l’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 agli Assistenti Amministrativi (Personale ATA), quale categoria omogenea, affinché il trattamento dei dati personali avvenga esclusivamente per finalità istituzionali e nei limiti delle mansioni effettivamente svolte. Le presenti istruzioni si applicano a tutte le attività di segreteria e amministrative svolte sotto l’autorità del Titolare e, per gli aspetti organizzativi e gestionali di competenza, del Direttore dei Servizi Generali e Amministrativi (DSGA), quale referente interno.

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 amministrative e di segreteria (didattica, personale, contabilità, protocollo, rapporti con utenza e fornitori), gli Assistenti Amministrativi possono venire a conoscenza e/o trattare dati personali relativi ad alunni, famiglie, personale scolastico, fornitori e altri interessati;

RITENUTO necessario definire in modo uniforme istruzioni operative e misure di riservatezza e sicurezza applicabili agli Assistenti Amministrativi, anche in relazione all’utilizzo di sistemi informativi, protocollo informatico, posta elettronica istituzionale/PEC, gestione documentale e pubblicazioni istituzionali (Albo online/Amministrazione Trasparente);

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, gli Assistenti Amministrativi in servizio presso

l'Istituto (a tempo indeterminato o determinato, supplenze e incarichi a tempo), 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 amministrative dell'Istituto. A titolo esemplificativo e non esaustivo rientrano nell'ambito: dati anagrafici e di contatto di alunni e famiglie; dati relativi a iscrizioni, carriera scolastica, frequenza, servizi e adempimenti amministrativi; dati relativi al personale scolastico (gestione presenze/assenze, fascicoli personali, incarichi, adempimenti retributivi e previdenziali); dati di fornitori e operatori economici (contratti, ordini, CIG/CUP, fatture e pagamenti); atti e corrispondenza soggetti a protocollazione e gestione documentale. Quando indispensabili, possono essere trattate categorie particolari di dati ex art. 9 GDPR (es. certificazioni sanitarie, disabilità, DSA/BES, idoneità al lavoro, provvedimenti assistenziali) e, nei casi previsti dalla normativa di settore, dati giudiziari/penali ex art. 10 GDPR, sempre secondo le procedure interne e nel rispetto delle misure di sicurezza previste.

È fatto divieto di effettuare trattamenti non pertinenti alle mansioni affidate, eccedenti rispetto alle finalità istituzionali o svolti con modalità difformi dalle istruzioni impartite, dalle procedure interne e dalle policy organizzative/informatiche dell'Istituto. In particolare, è vietato: accedere a fascicoli o informazioni non necessari (principio del "need to know"); estrarre o conservare copie ulteriori di documenti senza effettiva necessità; utilizzare strumenti o account non autorizzati; trasmettere dati personali senza una preventiva verifica del presupposto giuridico e della legittimazione del destinatario; trattare dati in luoghi o modalità tali da favorire l'accesso da parte di soggetti non autorizzati (es. documenti lasciati incustoditi, stampe non ritirate, postazioni non bloccate).

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, nonché la condivisione pubblica di documenti o contenuti idonei a identificare studenti, famiglie o personale. Ogni comunicazione o condivisione deve avvenire solo verso soggetti legittimati, per finalità di servizio e mediante canali istituzionali, limitando i dati al minimo indispensabile (principio di minimizzazione) ed evitando la trasmissione di informazioni eccedenti o non necessarie.

Le attività di pubblicazione istituzionale (Albo online e Amministrazione Trasparente) devono essere effettuate esclusivamente nei limiti previsti dalla normativa, applicando rigorosamente i principi di pertinenza, non eccedenza e minimizzazione, e adottando, ove necessario, misure di oscuramento/omissis e accorgimenti idonei a ridurre i rischi di indicizzazione e riutilizzo improprio. È necessario porre particolare attenzione alla

pubblicazione di dati riferiti a minori e alle categorie particolari di dati (art. 9 GDPR) o dati ex art. 10 GDPR, che devono essere esclusi o oscurati salvo casi eccezionali espressamente previsti e gestiti secondo istruzioni specifiche del Titolare. Devono inoltre essere rispettati i tempi di permanenza online, le regole di rimozione/archiviazione e le procedure interne di verifica preventiva, assicurando la corretta gestione delle versioni dei documenti (evitando, ad esempio, la pubblicazione di file "non ripuliti" da metadati o informazioni non visibili immediatamente ma comunque presenti nel documento).

In caso di dubbio sulla pubblicabilità di un atto o sui dati da oscurare, l'Assistente Amministrativo deve sospendere la pubblicazione e richiedere indicazioni al DSGA o al Dirigente Scolastico.

3. PRINCIPI E ISTRUZIONI OPERATIVE OBBLIGATORIE

In considerazione della natura delle attività svolte dagli Assistenti Amministrativi (gestione della segreteria didattica e del personale, protocollazione e gestione documentale, corrispondenza istituzionale/PEC, pratiche contabili e contrattuali, rapporti con l'utenza e con soggetti terzi legittimati), il trattamento dei dati personali richiede particolare attenzione e l'adozione di comportamenti uniformi, coerenti con i principi di protezione dei dati e con le misure di sicurezza definite dall'Istituto. Le presenti istruzioni operative, impartite ai sensi dell'art. 29 GDPR e dell'art. 32, par. 4 GDPR, hanno la finalità di garantire che i dati siano trattati solo per finalità istituzionali, con accessi limitati al necessario e con adeguate cautele nella gestione quotidiana di documenti cartacei e digitali.

Ogni operazione di trattamento deve essere effettuata nel rispetto del principio del "minimo privilegio" (accesso ai soli dati indispensabili) e del principio di minimizzazione (trattare e comunicare solo ciò che è necessario), assicurando riservatezza e tracciabilità delle attività, anche quando si opera in condizioni di urgenza o in presenza di richieste dell'utenza. Le seguenti prescrizioni sono da intendersi obbligatorie, si applicano a tutte le attività di ufficio e costituiscono regole operative minime cui attenersi nello svolgimento delle mansioni:

- trattare i dati personali nel rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione, esattezza, limitazione della conservazione e riservatezza;
- accedere esclusivamente ai dati necessari (principio del "need to know") e secondo i profili di accesso assegnati;
- utilizzare solo credenziali personali, mantenerle segrete, non condividerle e adottare le misure richieste (es. cambio periodico, MFA ove previsto);
- gestire protocollazione, fascicolazione, archiviazione e conservazione dei documenti secondo le procedure interne, evitando duplicazioni non necessarie;
- custodire con diligenza documenti e fascicoli (cartacei e digitali), prevenendo l'accesso di persone non autorizzate (armadi chiusi, scrivanie libere, attenzione a stampe e scanner);

- adottare misure di sicurezza fisiche e logiche (blocco schermo, postazioni presidiate, password robuste, attenzione a USB/supporti rimovibili);
- utilizzare canali istituzionali per comunicazioni e trasmissioni (posta istituzionale/PEC, protocollo), verificando destinatari e allegati prima dell'invio;
- non comunicare a terzi dati personali se non nei casi consentiti e secondo le procedure (es. richieste degli interessati, accesso agli atti, interlocuzioni con enti legittimati);
- in caso di richieste privacy (diritti degli interessati) o richieste complesse di accesso/copia documenti, informare tempestivamente DSGA/Dirigente e attenersi alle istruzioni, evitando riscontri autonomi non autorizzati.

Il trattamento deve avvenire preferibilmente mediante gli strumenti e i servizi informatici istituzionali (es. protocollo informatico/gestione documentale, posta elettronica istituzionale e PEC, piattaforme ministeriali e gestionali, segreteria digitale/Archimede, albo online e amministrazione trasparente). È vietato utilizzare account personali, servizi non autorizzati o canali informali (es. chat/social personali) per trattare o condividere dati personali. L'uso di dispositivi personali per finalità istituzionali è consentito solo se espressamente autorizzato e nel rispetto delle misure di sicurezza previste.

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

In ambito scolastico la maggior parte dei trattamenti amministrativi di dati personali è svolta in esecuzione di compiti di interesse pubblico e per l'adempimento di obblighi legali cui è soggetto l'Istituto (es. gestione iscrizioni e carriera scolastica, tenuta di registri e fascicoli, adempimenti contabili e contrattuali, gestione del personale, protocollazione e gestione documentale, comunicazioni istituzionali verso famiglie e amministrazioni, adempimenti verso Ministero/USR/enti pubblici). In tali ipotesi, il trattamento è effettuato sulla base delle pertinenti disposizioni normative e regolamentari e non richiede, di regola, il consenso dell'interessato, fermo restando l'obbligo di assicurare la corretta informazione agli interessati e il rispetto dei principi di minimizzazione, esattezza, limitazione della conservazione 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 facoltative, progetti e attività extrascolastiche non obbligatorie, pubblicazione di immagini/video e altri contenuti identificativi, servizi opzionali o comunicazioni non obbligatorie), gli Assistenti Amministrativi devono attenersi rigorosamente alle istruzioni dell'Istituto, verificare che siano stati rispettati i presupposti previsti (informativa, completezza della modulistica, soggetti firmatari, eventuali limiti e revocabilità) e utilizzare esclusivamente la modulistica e le procedure formalmente approvate dal Titolare. In tali circostanze, è vietato procedere con iniziative autonome o con modulistica non autorizzata: in caso di dubbi sulla necessità del consenso o sulla corretta base giuridica da applicare, l'Assistente Amministrativo deve sospendere l'attività e richiedere

indicazioni al DSGA/Dirigente e, se del caso, al RPD/DPO, al fine di garantire uniformità di comportamento e tutela rafforzata, soprattutto quando sono coinvolti minori o categorie particolari di dati.

5. RISERVATEZZA E OBBLIGO DI SEGRETO

Il Personale ATA, e in particolare gli Assistenti Amministrativi, 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 dal supporto utilizzato (verbale, cartaceo o digitale) e dall'ambito di riferimento (segreteria didattica, segreteria del personale, contabilità, protocollo e gestione documentale, rapporti con utenza e soggetti terzi). L'obbligo di riservatezza riguarda, a titolo esemplificativo, dati relativi a studenti e famiglie, fascicoli e pratiche amministrative, dati del personale scolastico, informazioni di natura contabile e contrattuale, corrispondenza istituzionale e ogni ulteriore informazione che, anche indirettamente, consenta l'identificazione degli interessati o la conoscenza di aspetti della loro vita personale.

È fatto divieto di divulgare, comunicare o rendere accessibili tali informazioni a soggetti non autorizzati, anche all'interno dell'Istituto, salvo che ciò sia strettamente necessario per finalità di servizio e nel rispetto del principio del "need to know". Il Personale è tenuto a prestare particolare attenzione nella gestione quotidiana di documenti e fascicoli (es. protocolli, fascicoli personali, registri, atti e provvedimenti), evitando conversazioni o scambi informali che possano comportare esposizione indebita di informazioni, soprattutto in luoghi accessibili al pubblico o in presenza dell'utenza. Analogo obbligo si applica all'uso degli strumenti digitali: è vietata qualsiasi condivisione tramite canali non istituzionali (es. chat o social personali) e deve essere evitata l'esposizione accidentale di dati (es. schermi visibili a terzi, stampe lasciate su dispositivi condivisi, documenti archiviati in modo non protetto). Tale obbligo permane anche dopo la cessazione del rapporto di lavoro o collaborazione, per tutto il tempo necessario a garantire la tutela della riservatezza degli interessati e nei limiti previsti dalla normativa vigente. Eventuali richieste di accesso, rilascio copie, comunicazione o pubblicazione di dati e documenti dovranno essere gestite esclusivamente tramite i canali istituzionali dell'Istituto e secondo le procedure previste, senza iniziative personali.

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. *violazione dei dati personali* o *data breach*), anche solo potenziale, deve essere segnalato senza ritardo e comunque immediatamente non appena conosciuto. Rientrano, a titolo esemplificativo: invio di PEC/email (o allegati) al destinatario errato; comunicazione non autorizzata di dati a soggetti non legittimati; caricamento o condivisione accidentale di

documenti su piattaforme non autorizzate o con permessi errati; smarrimento, furto o sottrazione di registri, fascicoli, stampe, chiavette USB, notebook o smartphone utilizzati per finalità di servizio; accessi anomali o sospetto furto/compromissione di credenziali; accesso non autorizzato a fascicoli cartacei o digitali; pubblicazione involontaria di dati su Albo online/Amministrazione Trasparente o su altri canali istituzionali; malfunzionamenti o blocchi che impediscano l'accesso a dati e documenti necessari per lo svolgimento dell'attività. La segnalazione deve essere effettuata immediatamente al Dirigente Scolastico e al DSGA e/o ai referenti interni individuati (es. Referente privacy), e per conoscenza al RPD/DPO ai recapiti istituzionali, fornendo tutte le informazioni utili, anche in forma sintetica: data e ora dell'evento, descrizione dell'accaduto, strumenti coinvolti, tipologia di dati interessati, categorie di interessati, eventuali destinatari non autorizzati, prime misure adottate per contenere l'evento (es. richiesta di cancellazione, revoca condivisioni, blocco account, cambio password) ed eventuali evidenze disponibili. È fatto obbligo di non intraprendere iniziative autonome che possano aggravare l'evento o comprometterne la gestione (es. ulteriori inoltri, tentativi non coordinati di ripristino, comunicazioni esterne), ma di attenersi alle indicazioni del Titolare e dei referenti incaricati, al fine di consentire la tempestiva valutazione dell'incidente, l'adozione delle misure di mitigazione e, se del caso, l'effettuazione delle comunicazioni previste dalla normativa (inclusa l'eventuale notifica all'Autorità Garante e/o la comunicazione 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 degli Assistenti Amministrativi 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 (es. firma digitale su circolare interna) 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 degli Assistenti Amministrativi quale “persona autorizzata al trattamento” (art. 29 GDPR). Il presente registro è compilato dal personale per attestare la presa visione dell’atto e delle istruzioni operative.

N.	Cognome e Nome	Ufficio/Area	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				