



Ufficio Scolastico Regionale per il Lazio
Istituto Comprensivo di Lariano
Scuola dell'Infanzia – Primaria – Secondaria di I grado
Via Urbano IV n. 3 – 00076 Lariano (Rm)
XXXIX Distretto Scolastico - Ambito Territoriale 15
C.F. 95002200582 - Codice Meccanografico RMIC8BR004
Indirizzo P.E.O rmic8br004@istruzione.it Indirizzo Pec RMIC8BR004@PEC.ISTRUZIONE.IT
tel. 06/96498742
Sito Internet: <http://www.comprensivolariano.edu.it>

DESIGNAZIONE A SOGGETTO AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI (DSGA) – Funzionario EQ (art. 29 e art. 32, par. 4, Regolamento UE 2016/679 – art. 2-quaterdecies D.Lgs. 196/2003)

IL DIRIGENTE SCOLASTICO

1. **VISTO** il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (di seguito "GDPR"), con particolare riguardo agli artt. 4, n. 10), 5, 24, 29 e 32, par. 4;
2. **VISTO** il D.Lgs. 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", come modificato dal D.Lgs. 10 agosto 2018, n. 101, e in particolare l'art. 2-quaterdecies (attribuzione di funzioni e compiti a soggetti designati) e gli artt. 2-sexies e 2-octies (trattamento di categorie particolari di dati e di dati relativi a condanne penali e reati per motivi di interesse pubblico rilevante);
3. **VISTI** il Regolamento (UE) 2024/1689 ("AI Act"), come modificato dal Regolamento (UE) 2026/1744 dell'8 luglio 2026, con particolare riguardo agli artt. 4, 5 e 50; la Legge 23 settembre 2025, n. 132; nonché le "Linee guida per l'introduzione dell'Intelligenza Artificiale nelle Istituzioni scolastiche", allegate al D.M. n. 166 del 9 agosto 2025;
4. **VISTO** il Regolamento d'Istituto per l'utilizzo dei sistemi di intelligenza artificiale e il Piano d'Istituto per l'IA;
5. **CONSIDERATO** che questo Istituto è titolare del trattamento dei dati personali di alunni, genitori ed esercenti la responsabilità genitoriale, personale dipendente, fornitori e di qualunque altro soggetto che abbia rapporti con l'Istituto medesimo e che a questo conferisca, volontariamente o per obbligo, propri dati personali;
6. **CONSIDERATO** che le funzioni di titolare del trattamento sono esercitate dallo scrivente Dirigente scolastico, in qualità di legale rappresentante dell'Istituto;
7. **VISTO** il CCNL del comparto Istruzione e Ricerca vigente, con particolare riferimento all'ordinamento professionale del personale ATA e all'inquadramento nell'Area dei Funzionari e dell'Elevata Qualificazione per il conferimento dell'incarico di Direttore dei servizi generali e amministrativi (DSGA)- Funzionario EQ;
8. **CONSIDERATO** che il DSGA-Funzionario EQ, per l'espletamento delle proprie funzioni, ha necessità di venire a conoscenza e di trattare la generalità dei dati personali gestiti dai servizi amministrativi dell'Istituto — riferiti ad alunni, famiglie, personale, fornitori e altri soggetti che intrattengono rapporti con l'Istituto — ivi comprese categorie particolari di dati e dati relativi a condanne penali e reati, nei limiti di quanto strettamente necessario, fermi restando gli obblighi e le responsabilità civili e penali;
9. **CONSIDERATO** che l'art. 2-quaterdecies del Codice consente al titolare di prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la sua autorità, e che ai sensi degli artt. 29 e 32, par. 4, GDPR chiunque agisca sotto l'autorità del titolare e abbia accesso a dati personali può trattarli soltanto su istruzione del titolare medesimo;

10. **VISTA** la designazione del Responsabile della protezione dei dati (RPD/DPO): Attilio Milli, contattabile ai recapiti: dpo@gdpristruzione.it.

DESIGNA

la Direttrice dei servizi generali e amministrativi Funzionario EQ, Gioia Mancini (codice fiscale: MNCGIO61D45A449T), quale **SOGGETTO AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI**

in relazione alle operazioni di trattamento di dati personali, su supporto cartaceo e/o con strumenti elettronici, ai quali ha accesso nell'espletamento delle funzioni e dei compiti assegnati nell'ambito del rapporto di lavoro con questa Istituzione scolastica, disciplinati dalla normativa vigente e dai contratti collettivi di settore. La presente designazione costituisce formale autorizzazione a trattare i dati personali relativi a tutti i trattamenti di competenza dei servizi generali e amministrativo-contabili dell'Istituto, a eccezione di quelli espressamente riservati al titolare, con le operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modifica, selezione, estrazione e comunicazione (quest'ultima nei soli casi previsti da norme di legge o di regolamento o autorizzati dal titolare). In particolare:

Sovrintendenza ai servizi e coordinamento del personale ATA

- sovrintendenza, con autonomia operativa, ai servizi generali amministrativo-contabili e cura della relativa organizzazione (art. 3 D.L. 129/2018), con accesso agli archivi elettronici e cartacei di tutte le aree della segreteria (didattica e alunni, personale, contabilità e finanza, protocollo e affari generali);
- coordinamento del personale ATA, nell'ambito delle direttive del Dirigente scolastico, anche ai fini della corretta applicazione delle procedure organizzative e delle istruzioni operative impartite dal Titolare; eventuali inosservanze, anomalie o criticità in materia di trattamento dei dati sono tempestivamente segnalate al Titolare;

Gestione amministrativa, contabile e negoziale

- gestione del personale docente e ATA (fascicoli, assenze, stato giuridico ed economico), di stipendi, compensi accessori e adempimenti fiscali e previdenziali;
- attività negoziale e rapporti con i fornitori di beni e servizi (art. 44 D.L. 129/2018); gestione del Programma annuale, del fondo d'istituto, dei fondi comunitari (PNRR, PON) e di altri progetti; corretta tenuta dei registri contabili previsti dal D.L. 129/2018;
- gestione documentale, protocollo informatico e conservazione digitale a norma; supporto alle attività degli organi collegiali; pubblicazioni all'albo on line e nella sezione Amministrazione trasparente, nel rispetto delle istruzioni di cui al punto dedicato;
- gestione delle pratiche riguardanti alunni e famiglie che comportano categorie particolari di dati o dati ex art. 10 GDPR (disabilità, DSA/BES, certificati medici, denunce di infortunio all'INAIL, contenzioso), nei limiti di quanto strettamente indispensabile;

Supporto al titolare negli adempimenti in materia di protezione dei dati

- supporto operativo al Titolare nella predisposizione, tenuta e aggiornamento del registro delle attività di trattamento (art. 30 GDPR) e del registro interno delle violazioni dei dati personali (art. 33, par. 5, GDPR), ferma restando la responsabilità del Titolare per i relativi adempimenti;
- supporto organizzativo al Titolare affinché agli interessati siano rese le informative di cui agli artt. 13 e 14 GDPR e il personale riceva gli atti di designazione, le istruzioni operative e gli aggiornamenti pertinenti alle mansioni svolte;
- nell'ambito dell'attività negoziale, cura gli adempimenti amministrativi necessari affinché, quando un fornitore tratta dati personali per conto dell'Istituto, siano acquisiti e formalizzati gli atti previsti dall'art. 28 GDPR e gli ulteriori documenti richiesti dal Titolare; collabora inoltre alla corretta formalizzazione degli incarichi alle figure tecniche secondo le determinazioni del Titolare;

- collaborazione con il Titolare, con il Responsabile della protezione dei dati e con le figure tecniche competenti nell'attuazione delle misure tecniche e organizzative di cui all'art. 32 GDPR, nella gestione operativa delle violazioni di dati personali e nella raccolta delle informazioni necessarie alle valutazioni d'impatto di cui all'art. 35 GDPR, che restano di competenza del Titolare;
- cura dell'applicazione del piano di conservazione e scarto della documentazione e dei tempi di conservazione definiti dal titolare per ciascun trattamento;
- proposta al titolare, in relazione ai compiti assegnati, dell'impiego di adeguate risorse umane, tecniche ed economiche.

Nell'ambito del Registro delle attività di trattamento vigente dell'Istituto, predisposto ai sensi dell'art. 30 GDPR, sono riportati di seguito i trattamenti potenzialmente pertinenti alle funzioni del DSGA-Funzionario EQ e ai servizi generali amministrativo-contabili. **L'autorizzazione è individuale ed è concessa esclusivamente per i trattamenti effettivamente pertinenti alle funzioni esercitate e contrassegnati (☑) dal Titolare.**

N.	Trattamento	Autorizzato
1	Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro, del personale dipendente dell'Amministrazione centrale e periferica del Ministero dell'istruzione e del merito, e dirigente, docente, educativo ed ATA, dei collaboratori esterni e dei soggetti che intrattengono altri rapporti di lavoro diversi da quello subordinato. Il trattamento concerne tutti i dati relativi alle procedure per la selezione e il reclutamento, all'instaurazione, alla gestione e alla cessazione del rapporto di lavoro.	☑
2	Gestione del contenzioso e procedimenti disciplinari. Il trattamento dei dati concerne tutte le attività relative alla difesa in giudizio del Ministero e delle istituzioni scolastiche ed educative nel contenzioso del lavoro e amministrativo, nonché quelle connesse alla gestione degli affari penali e civili.	☑
3	Organismi collegiali e commissioni istituzionali. Il trattamento dei dati necessario per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero e dell'ordinamento scolastico (organi rappresentativi del personale, degli studenti, delle famiglie e delle associazioni sindacali).	☑
4	Attività propedeutiche all'avvio dell'anno scolastico, ai corsi e a tutte le attività formative. I dati sono forniti dagli alunni, dalle famiglie e dalle persone ai fini della frequenza dei corsi di studi nelle istituzioni scolastiche di ogni ordine e grado.	☑
5	Attività educativa, didattica e formativa, e di valutazione. Il trattamento dei dati necessari all'espletamento delle attività educative, didattiche e formative, curricolari ed extracurricolari, di valutazione e orientamento, di scrutini ed esami, valutazione periodica e finale, e per la certificazione delle competenze.	☑
6	Scuole non statali (trattamento non utilizzato nella scuola statale; si riporta per continuità di numerazione).	—
7	Rapporti scuola-famiglie-altri soggetti: gestione del contenzioso. Il trattamento dei dati concernenti le attività connesse all'instaurazione di contenzioso (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce all'autorità giudiziaria, ecc.) con gli alunni e con le famiglie, e le attività relative alla difesa in giudizio delle istituzioni scolastiche.	☑
8	Rapporti con i fornitori di beni e servizi. Il trattamento dei dati concernenti le attività connesse all'instaurazione di rapporti di fornitura di beni e servizi, albo fornitori, gestione della rotazione, manifestazioni di interesse e similari.	☑
9	Rapporti con enti e associazioni. Il trattamento dei dati concernenti le attività connesse all'instaurazione di rapporti con enti pubblici, assimilati e associazioni.	☑
10	Videosorveglianza. Il trattamento dei dati concernenti le attività di gestione, conservazione dei dati e gestione degli accessi ai sistemi di videosorveglianza.	☐

ISTRUZIONI OPERATIVE

I trattamenti devono essere eseguiti nel rispetto delle istruzioni operative che seguono, impartite ai sensi degli artt. 29 e 32, par. 4, GDPR:

1. il trattamento dei dati personali cui è autorizzato ad accedere deve avvenire secondo le modalità definite dalla normativa vigente, in modo lecito e secondo correttezza, nel rispetto dei principi di cui all'art. 5 GDPR e con l'osservanza, in particolare, delle prescrizioni del Regolamento (UE) 2016/679 e del D.Lgs. 196/2003;
2. il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali della scuola; il soggetto autorizzato agisce sotto la diretta autorità del titolare e deve attenersi alle istruzioni da questo impartite;
3. i dati personali oggetto dei trattamenti devono essere esatti e aggiornati; devono inoltre essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali vengono raccolti e trattati (principio di minimizzazione), e conservati per il tempo strettamente necessario;
4. è vietato collocare documenti o file contenenti categorie particolari di dati (art. 9 GDPR) o dati relativi a condanne penali e reati (art. 10 GDPR) in aree di archiviazione condivise ad accesso generalizzato. L'uso di repository, servizi cloud o spazi documentali esterni è ammesso esclusivamente se fornito o autorizzato dall'Istituto e configurato secondo le misure tecniche e organizzative definite dal Titolare;
5. è vietata qualsiasi forma di diffusione e comunicazione dei dati personali trattati che non sia strettamente funzionale allo svolgimento dei compiti affidati e autorizzata dal titolare. Si raccomanda particolare attenzione alla tutela della riservatezza degli interessati e di consultare il regolamento approvato dall'Istituto e/o il titolare o il Responsabile della protezione dei dati in caso di dubbi, prima di comunicare dati a terzi;
6. l'obbligo di riservatezza sulle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico permane in ogni caso anche dopo la cessazione dell'incarico stesso;
7. i trattamenti vanno effettuati nel rispetto delle misure tecniche e organizzative di sicurezza adottate dall'Istituto ai sensi dell'art. 32 GDPR. In ogni operazione di trattamento va garantita la massima riservatezza e custodia di atti e documenti contenenti dati personali, che non vanno mai lasciati incustoditi o a disposizione di terzi non autorizzati ad accedervi, prenderne visione o effettuare qualsivoglia operazione. Si invita alla lettura periodica delle procedure di sicurezza e delle istruzioni operative predisposte dall'Istituto, costantemente aggiornate;
8. le credenziali di autenticazione attribuite sono personali e devono essere custodite con cura e diligenza; non possono essere condivise, messe a disposizione o rivelate a terzi, né lasciate incustodite o in libera visione. In caso di smarrimento, furto o sospetta compromissione occorre darne immediata notizia al Titolare secondo le procedure dell'Istituto e provvedere all'immediata sostituzione; ove resa disponibile dall'Istituto, l'autenticazione a più fattori deve essere attivata e utilizzata;
9. l'uso di supporti rimovibili (chiavi USB, dischi esterni, ecc.) per memorizzare dati personali è ammesso solo quando necessario e autorizzato. I supporti devono essere custoditi con cura e, se contengono categorie particolari di dati (art. 9 GDPR) o dati relativi a condanne penali e reati (art. 10 GDPR), devono essere cifrati secondo le misure e le procedure definite dall'Istituto;
10. i supporti rimovibili contenenti categorie particolari di dati e/o dati giudiziari, se non più utilizzati, vanno distrutti o resi inutilizzabili;
11. l'accesso agli archivi contenenti categorie particolari di dati o dati giudiziari è consentito solo alle persone autorizzate ed è soggetto a controllo secondo le regole definite dal titolare;
12. durante i trattamenti i documenti contenenti dati personali vanno mantenuti in modo tale da non essere alla portata di vista di persone non autorizzate;
13. al termine del trattamento i documenti contenenti dati personali vanno custoditi all'interno di archivi, cassette o armadi muniti di serratura;
14. i documenti e i dati personali non possono essere trasferiti, duplicati o trattati al di fuori degli ambienti, dei dispositivi e dei servizi autorizzati dall'Istituto, salvo quanto espressamente previsto dalle procedure organizzative e di sicurezza adottate dal Titolare;

15. in caso di allontanamento anche temporaneo dalla postazione di lavoro, o comunque dal luogo dove vengono trattati i dati, occorre bloccare la sessione di lavoro (disconnessione e/o salvaschermo con password) e verificare che non vi sia possibilità da parte di terzi, anche se dipendenti non autorizzati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento;
16. le comunicazioni agli interessati devono avvenire in forma riservata; se effettuate per iscritto, devono essere consegnate in plico chiuso;
17. all'atto della consegna di documenti contenenti dati personali occorre assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento con delega in forma scritta;
18. le comunicazioni elettroniche ad alunni, colleghi, genitori, personale della scuola o altri soggetti coinvolti per finalità istituzionali vanno effettuate esclusivamente tramite gli account e i canali istituzionali, seguendo le indicazioni fornite dall'Istituzione scolastica e garantendo la necessaria riservatezza delle comunicazioni stesse e dei dati coinvolti;
19. **postazioni di lavoro:** l'accesso ai gestionali e ai portali in cloud deve avvenire esclusivamente da postazioni con sistema operativo supportato dal produttore e costantemente aggiornato, dotate di software antivirus/antimalware attivo; le password non vanno salvate nei browser su postazioni condivise; al termine di ogni sessione di lavoro occorre effettuare il logout dalle piattaforme e, in caso di allontanamento, attivare il blocco schermo con password;
20. **lavoro e accesso da remoto:** l'accesso ai sistemi dell'Istituto e il trattamento di dati al di fuori della sede sono ammessi esclusivamente tramite strumenti, dispositivi e canali autorizzati dal Titolare e nel rispetto delle procedure di sicurezza adottate dall'Istituto; è vietato utilizzare software di controllo remoto, servizi cloud o strumenti di condivisione non autorizzati. Gli eventuali documenti cartacei autorizzati fuori sede devono essere custoditi con particolare attenzione e per il tempo strettamente necessario;
21. **riunioni e colloqui a distanza:** le riunioni in videoconferenza per finalità istituzionali si svolgono esclusivamente sulle piattaforme autorizzate dall'Istituto. Qualsiasi registrazione è ammessa soltanto quando espressamente autorizzata, necessaria rispetto alla finalità istituzionale e gestita secondo le indicazioni del Titolare; è vietata ogni diffusione o condivisione con soggetti non autorizzati;
22. **messaggistica istantanea:** le comunicazioni di servizio contenenti dati personali vanno effettuate esclusivamente tramite i canali istituzionali; è vietato l'uso di applicazioni di messaggistica su account personali (WhatsApp, Telegram e simili) per trasmettere dati personali di alunni, famiglie o personale, ivi compresi elenchi, recapiti e documenti;
23. **pubblicazioni sul sito istituzionale:** nella predisposizione di atti destinati all'albo on line o alla sezione Amministrazione trasparente devono essere rispettati i principi di liceità, minimizzazione e limitazione della finalità, nonché gli specifici obblighi e limiti di pubblicazione previsti dalla normativa vigente. Prima della pubblicazione devono essere omessi o oscurati i dati personali non pertinenti o eccedenti e non devono essere diffusi dati appartenenti a categorie particolari, salvo che una specifica disposizione normativa lo consenta nei limiti strettamente necessari;
24. **dispositivi e servizi:** per il trattamento dei dati personali vanno utilizzati esclusivamente i dispositivi, gli account e i servizi (posta elettronica, piattaforme, spazi cloud) forniti o espressamente autorizzati dall'Istituto. È vietato salvare o trasferire dati personali di alunni e famiglie su account personali, spazi cloud privati o applicazioni di messaggistica non autorizzate; l'eventuale uso di dispositivi personali (BYOD) è ammesso solo se previamente autorizzato e nel rispetto delle misure di sicurezza indicate dall'Istituto;
25. **sicurezza informatica:** non vanno aperti messaggi di posta elettronica, allegati o collegamenti di provenienza incerta o sospetta (phishing) e non va installato software non autorizzato; gli aggiornamenti di sicurezza delle risorse informatiche e degli applicativi vanno curati direttamente o segnalati all'amministratore di sistema; ogni anomalia, accesso sospetto o malfunzionamento va segnalato tempestivamente all'amministratore di sistema e al titolare;

26. **violazioni di dati personali (data breach):** chiunque venga a conoscenza di una violazione, anche solo sospetta, dei dati personali (perdita, furto o smarrimento di dispositivi o documenti, accesso non autorizzato, invio errato di comunicazioni, alterazione o indisponibilità di dati) è tenuto a segnalare immediatamente e comunque senza ingiustificato ritardo al Titolare, attraverso i canali previsti dalla procedura di gestione delle violazioni adottata dall'Istituto, affinché possano essere effettuate le valutazioni e gli eventuali adempimenti di cui agli artt. 33 e 34 GDPR; il RPD/DPO è coinvolto secondo quanto previsto dalla procedura interna;
27. **utilizzo di sistemi di intelligenza artificiale: nell'impiego di sistemi di IA nei compiti amministrativi e nell'esercizio delle funzioni di sovrintendenza, il soggetto autorizzato si attiene al Regolamento d'Istituto per l'IA, alle procedure interne e alle seguenti prescrizioni:**
- a) è consentito l'uso dei soli sistemi di IA espressamente autorizzati dal Titolare e inseriti nell'elenco degli strumenti approvati dall'Istituto, con account istituzionali e nelle configurazioni definite dall'amministrazione;
 - b) è vietato inserire dati personali di alunni, famiglie, personale o fornitori – e, a maggior ragione, categorie particolari di dati (art. 9 GDPR) o dati relativi a condanne penali e reati (art. 10 GDPR) – in sistemi di IA non autorizzati, anche se gratuiti o utilizzati tramite account personali. Nei sistemi autorizzati i dati devono comunque essere limitati a quanto strettamente necessario, privilegiando ove possibile dati anonimi o adeguatamente de-identificati;
 - c) non è consentito delegare a sistemi di IA decisioni che producano effetti giuridici o incidano in modo significativo sugli interessati. L'IA può essere utilizzata esclusivamente come supporto, nel rispetto delle competenze e delle responsabilità proprie dell'amministrazione; ogni output deve essere sottoposto a effettiva verifica umana prima di essere utilizzato in atti, comunicazioni o procedimenti;
 - d) gli output dei sistemi di IA (testi, bozze di atti, calcoli, riepiloghi o classificazioni) devono essere verificati criticamente sotto il profilo della correttezza, completezza, riservatezza e pertinenza. Gli eventuali obblighi di trasparenza previsti dalla normativa in materia di IA sono applicati nei casi e secondo le modalità effettivamente pertinenti al sistema e all'uso concreto;
 - e) eventuali malfunzionamenti, incidenti, risultati anomali o usi impropri dei sistemi di IA devono essere segnalati tempestivamente al Titolare e, secondo le procedure dell'Istituto, al referente per l'IA e al RPD/DPO;
 - f) nell'ambito dell'attività negoziale, cura la raccolta della documentazione necessaria alla valutazione dei fornitori e dei sistemi di IA destinati all'uso nell'Istituto e, ove il fornitore tratti dati personali per conto della scuola, cura gli adempimenti amministrativi necessari alla formalizzazione dell'art. 28 GDPR secondo le determinazioni del Titolare; collabora inoltre alla tenuta dell'elenco degli strumenti di IA autorizzati;
 - g) nell'ambito del coordinamento del personale ATA, richiama il personale al rispetto delle istruzioni e delle procedure adottate dall'Istituto per l'uso dei sistemi di IA e segnala tempestivamente al Titolare eventuali utilizzi non autorizzati, anomalie o criticità rilevate;
 - h) il soggetto autorizzato partecipa alle iniziative di alfabetizzazione in materia di IA predisposte dall'Istituto in relazione agli strumenti concretamente utilizzati e alle funzioni esercitate.
28. attenersi alle ulteriori istruzioni impartite dal Titolare del trattamento o dai soggetti da esso formalmente incaricati; il Responsabile della protezione dei dati (RPD/DPO) resta riferimento per consulenza e chiarimenti in materia di protezione dei dati personali;
29. partecipare alle attività di formazione e aggiornamento predisposte dall'Istituto in materia di protezione dei dati personali, sicurezza informatica e, ove pertinente alle funzioni e agli strumenti utilizzati, alfabetizzazione in materia di intelligenza artificiale, attenendosi alle istruzioni e alle procedure organizzative ricevute;

30. la presente designazione ha validità per la durata del servizio prestato presso questo Istituto e cessa automaticamente alla cessazione, a qualunque titolo, del rapporto con l'Istituzione scolastica, ovvero in caso di revoca o modifica da parte del titolare; restano fermi gli obblighi di riservatezza di cui al punto 6.

Il presente modello è firmato, protocollato e conservato agli atti.

Lariano 23/09/2026

Il Dirigente Scolastico

Prof.ssa Fermina Tardiola

(firma digitale ai sensi del D.Lgs. 82/2005)