Istituto Comprensivo "Don Bosco - V. Tieri"
Via del Cantastorie snc, 87064 Cantinella di Corigliano-Rossano (CS)
Tel. 0983-80719/ 80022 – Email csic83100t@istruzione.it – C.M. CSIC83100T

Al/Alla dipendente _____

DESIGNAZIONE DEL PERSONALE DI SEGRETERIA AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI

E RELATIVE ISTRUZIONI OPERATIVE

Oggetto: autorizzazione al trattamento dei dati personali ai sensi degli artt. 29 e 32, par. 4, del Regolamento (UE) 2016/679 e dell'art. 2-quaterdecies del d.lgs. 196/2003.

IL DIRIGENTE SCOLASTICO

VISTO il Regolamento (UE) 2016/679 (GDPR), con particolare riferimento agli artt. 5, 24, 29 e 32;

VISTO il decreto legislativo 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101, e in particolare l'art. 2-quaterdecies;

CONSIDERATO che l'Istituto, quale Titolare del trattamento, deve individuare e istruire le persone che, in ragione delle mansioni affidate, trattano dati personali sotto la propria autorità;

CONSIDERATO che il **DSGA** e gli **Assistenti amministrativi**, nello svolgimento delle rispettive funzioni, trattano dati personali riferiti ad alunni e famiglie, personale, fornitori, professionisti e altri soggetti che intrattengono rapporti con l'Istituto, comprese, nei casi previsti, categorie particolari di dati e dati relativi a condanne penali e reati;

TENUTO CONTO dei principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza;

DESIGNA E AUTORIZZA

il/la dipendente _____, C.F. _____
in servizio presso l'Istituto con la qualifica sopra indicata, al trattamento dei dati personali esclusivamente per le operazioni necessarie allo svolgimento delle funzioni, dei compiti e degli incarichi attribuiti.

L'autorizzazione è limitata ai trattamenti strettamente necessari allo svolgimento delle mansioni e delle funzioni attribuite. Essa cessa o si modifica al venir meno o al variare delle funzioni che ne costituiscono il presupposto.

1. AMBITO DELL'AUTORIZZAZIONE

1.1 Il personale di segreteria può trattare, nei limiti delle mansioni assegnate, dati anagrafici e di contatto, dati relativi alla carriera scolastica e al rapporto con l'Istituto Istituto Comprensivo "Don Bosco - V. Tieri", dati del personale, dati amministrativi, contabili, fiscali, previdenziali, assicurativi, bancari e contrattuali, nonché ogni altra informazione pertinente alle attività di competenza.

1.2 L'accesso a categorie particolari di dati (ad es. salute, disabilità, appartenenza sindacale, convinzioni religiose ove rilevanti) e a dati relativi a condanne penali e reati è consentito esclusivamente quando necessario per uno specifico adempimento istituzionale e nei limiti delle informazioni che la persona autorizzata è legittimata a conoscere.

1.3 Le operazioni autorizzate possono comprendere, secondo le mansioni attribuite: raccolta, registrazione, organizzazione, consultazione, aggiornamento, estrazione, utilizzo, comunicazione ai soggetti legittimati, conservazione, archiviazione, cancellazione e distruzione secondo le procedure dell'Istituto.

1.4 L'accesso ai fascicoli, agli archivi e agli applicativi deve essere coerente con l'ufficio, il profilo di abilitazione e i compiti assegnati; non è consentita la consultazione di dati per curiosità, interesse personale o finalità estranee al servizio.

2. ISTRUZIONI GENERALI E OBBLIGO DI RISERVATEZZA

2.1 Trattare i dati esclusivamente per finalità istituzionali e nell'ambito delle attività assegnate, rispettando le istruzioni del Titolare e le procedure interne.

2.2 Mantenere il segreto d'ufficio e la massima riservatezza sulle informazioni conosciute per ragioni di servizio. L'obbligo permane anche dopo la cessazione dal servizio o dall'incarico.

2.3 Verificare, per quanto di competenza, l'esattezza e l'aggiornamento dei dati e limitare la raccolta e l'utilizzo a quanto effettivamente necessario.

2.4 Non comunicare dati a soggetti non legittimati e non diffondere dati personali, salvo i casi espressamente previsti dalla normativa o dalle procedure autorizzate dell'Istituto.

2.5 Non lasciare incustoditi fascicoli, certificazioni, elenchi, cedolini, prospetti, contratti, verbali, documenti contabili o altri atti contenenti dati personali; riporli negli archivi, armadi o sistemi previsti.

2.6 Non creare copie, archivi paralleli o esportazioni di dati non necessarie; le copie di lavoro devono essere eliminate in modo sicuro quando non più occorrenti.

3. PROTOCOLLO, FASCICOLI, PEC, E-MAIL E COMUNICAZIONI

3.1 Protocollare, classificare, fascicolare e inoltrare i documenti secondo le procedure dell'Istituto, evitando che dati riservati siano resi visibili a soggetti o uffici non competenti.

3.2 Prima dell'invio di e-mail, PEC, atti o allegati, verificare con attenzione destinatario, indirizzo, contenuto e allegati. Utilizzare i canali istituzionali e le funzionalità previste dai sistemi in uso.

3.3 Quando una comunicazione è destinata a più soggetti non legati tra loro, utilizzare modalità che non rendano indebitamente visibili gli indirizzi degli altri destinatari, salvo necessità istituzionale.

3.4 Le comunicazioni telefoniche o allo sportello devono essere rese solo dopo aver verificato, in modo proporzionato al contenuto, l'identità e la legittimazione dell'interlocutore.

3.5 All'atto della consegna di certificati, atti o documenti contenenti dati personali, verificare l'identità del richiedente e, in caso di delega, l'esistenza e la validità della delega secondo le procedure dell'Istituto.

4. SISTEMI INFORMATICI, SIDI E APPLICATIVI AMMINISTRATIVI

4.1 Utilizzare esclusivamente account, credenziali, applicativi e profili di accesso assegnati o autorizzati dall'Istituto, compresi SIDI e gli altri sistemi istituzionali o gestionali necessari alle funzioni di competenza.

4.2 Le credenziali sono personali: non devono essere comunicate, cedute o lasciate disponibili a terzi. Segnalare immediatamente smarrimento, compromissione, accessi anomali o sospetti.

4.3 Bloccare la sessione o disconnettersi quando ci si allontana dalla postazione; non lasciare documenti o schermate contenenti dati personali visibili al pubblico o a personale non autorizzato.

4.4 Non trasferire dati d'ufficio su caselle e-mail personali, servizi cloud personali, supporti o applicazioni non autorizzati. L'uso di supporti rimovibili è consentito solo quando necessario e secondo le misure stabilite dall'Istituto.

4.5 Prestare attenzione a phishing, allegati, link e richieste anomale; non installare software o estensioni non autorizzati e non disattivare le misure di sicurezza predisposte dall'Istituto.

5. DATI PARTICOLARI, PERSONALE, ALUNNI E PROCEDIMENTI RISERVATI

5.1 I documenti contenenti dati relativi alla salute, disabilità, assenze per motivi sanitari, appartenenza sindacale, procedimenti disciplinari, contenzioso o altre informazioni particolarmente riservate devono essere trattati con cautele rafforzate e resi accessibili soltanto ai soggetti competenti.

5.2 Nei procedimenti amministrativi e nella gestione dei fascicoli personali di alunni e dipendenti, evitare annotazioni o copie non necessarie e utilizzare solo le informazioni pertinenti allo specifico adempimento.

5.3 Nella predisposizione di elenchi, graduatorie, atti, determine, contratti e documenti destinati alla pubblicazione, verificare preventivamente quali dati possano essere legittimamente pubblicati e applicare, quando necessario, omissioni o oscuramenti.

6. PUBBLICAZIONE, ACCESSO AGLI ATTI E TRASPARENZA

6.1 La pubblicazione sul sito istituzionale, all'Albo online o in Amministrazione Trasparente deve avvenire esclusivamente nei casi previsti e secondo le istruzioni dell'Istituto, rispettando i principi di minimizzazione e limitazione della diffusione.

6.2 Le richieste di accesso documentale, accesso civico o altre istanze che possano coinvolgere dati di terzi devono essere gestite secondo le procedure interne, sottoponendo al Dirigente o al responsabile del procedimento i casi che richiedono valutazioni o bilanciamenti.

6.3 Prima di pubblicare o trasmettere un documento, verificare che non contenga dati personali eccedenti, firme, recapiti privati, coordinate bancarie, dati sanitari o altre informazioni non destinate alla conoscibilità del destinatario o del pubblico.

7. STRUMENTI DI INTELLIGENZA ARTIFICIALE E SERVIZI ESTERNI

7.1 Non inserire in servizi di intelligenza artificiale generativa o in altri servizi esterni non autorizzati dati personali, documenti, fascicoli, elenchi, credenziali, informazioni contabili, disciplinari, sanitarie o comunque riservate apprese per ragioni di servizio.

7.2 L'eventuale utilizzo di strumenti di IA o di servizi digitali che comportino trattamento di dati personali è consentito solo se previsto o autorizzato dall'Istituto e nel rispetto delle specifiche istruzioni impartite.

8. INCIDENTI E VIOLAZIONI DI DATI PERSONALI

8.1 Qualsiasi evento che possa comportare perdita, distruzione, alterazione, divulgazione o accesso non autorizzato a dati personali deve essere segnalato senza ritardo al Dirigente scolastico o al referente interno individuato dall'Istituto, fornendo le informazioni disponibili.

8.2 Rientrano, a titolo esemplificativo, tra gli eventi da segnalare: invio a destinatario errato, pubblicazione accidentale, smarrimento di documenti o dispositivi, credenziali compromesse, accessi anomali, malware, sottrazione di dati o indisponibilità rilevante degli archivi.

8.3 La persona autorizzata non deve comunicare autonomamente l'incidente agli interessati o al Garante, salvo specifiche istruzioni del Titolare.

9. SPECIFICHE PER IL DSGA

9.1 Il DSGA, nell'ambito delle attribuzioni proprie e delle direttive impartite dal Dirigente scolastico, coordina l'attività amministrativa e può impartire al personale amministrativo indicazioni organizzative coerenti con le presenti istruzioni e con le misure adottate dal Titolare.

9.2 Tale funzione di coordinamento non attribuisce al DSGA autonoma determinazione delle finalità e dei mezzi essenziali del trattamento e non modifica la titolarità del trattamento in capo all'Istituto.

10. DISPOSIZIONI FINALI

10.1 La presente designazione integra le disposizioni organizzative, il mansionario, gli ordini di servizio, le policy e le misure di sicurezza adottate dall'Istituto. Restano ferme eventuali istruzioni più specifiche riferite a singoli uffici, procedimenti o sistemi.

10.2 In caso di dubbio sulla liceità di una comunicazione, pubblicazione, accesso o altra operazione sui dati, il dipendente deve sospendere l'operazione non necessaria e richiedere indicazioni al Dirigente scolastico o ai soggetti interni competenti.

10.3 La violazione delle presenti istruzioni può rilevare sotto il profilo organizzativo, disciplinare e, nei casi previsti, civile, amministrativo o penale, ferme le responsabilità del Titolare per gli adempimenti di propria competenza.

Luogo _____, data _____ / _____ / _____

IL DIRIGENTE SCOLASTICO
LAURA SISCA
Firma autografa omessa ai sensi dell'art. 3,
comma 2, del D.Lgs. n. 39/1993

Firma DESIGNATO _____