



ISTITUTO COMPRENSIVO DI SCUOLA PRIMARIA E SECONDARIA
DI PRIMO GRADO BASSA VAL DI SOLE "GIOVANNI CICCOLINI"

Via Taddei de Mauris, 4 - 38027 MALÉ (TN)

Codice Fiscale: 92013860223 - Tel. 0463/901237 - Fax 0463/902866

E-mail: segr.ciccolini.male@scuole.provincia.tn.it

PEC: ic.bassavaldisole@pec.provincia.tn.it



FUTURA PNRR ISTRUZIONE **LA SCUOLA
PER L'ITALIA DI DOMANI**



Finanziato
dall'Unione europea
NextGenerationEU



Ministero dell'Istruzione
e del Merito

icbvs/2026/4.1/pg

Numero di protocollo associato al documento come metadato (DPCM 3.12.2013, art. 20). Verificare l'oggetto della PEC o i files allegati alla medesima. Data di registrazione inclusa nella segnatura di protocollo. Negli esemplari cartacei segnatura di protocollo in alto a sinistra (da citare nella risposta)

Egregio Signore/Gentile Signora

LETTERA DI INCARICO AL TRATTAMENTO DEI DATI E RELATIVE ISTRUZIONI (art. 29 del Regolamento UE 769/2016)

L'Istituto IC Bassa Val di Sole "G. Ciccolini", (d'ora in poi "**Titolare**"), con sede in Via Taddei de Mauris 4, 38027 Malé (TN), quale titolare del trattamento dei dati personali (d'ora in poi "**Dati**"), svolto nell'ambito della propria attività

premessi che:

- nell'ambito dell'attività svolta dal Titolare, svolge mansioni che comportano il trattamento di dati personali;
- il Regolamento UE 679/2016 recante disposizioni per la "*protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*" prevede che il trattamento di dati personali, come definiti all'art. 4 del Regolamento, avvenga in modo lecito, corretto e trasparente, adeguato, pertinente, compatibile e limitato a quanto necessario rispetto alle finalità per le quali i dati sono stati raccolti ed in maniera tale da garantire un'adeguata sicurezza, sia sotto il profilo dell'integrità degli stessi sia sotto quello della sicurezza;
- l'art. 4 prevede espressamente l'esistenza di "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare e del responsabile";
- l'art. 29 stabilisce che chiunque agisca sotto l'autorità del titolare o del responsabile del trattamento ed abbia accesso a dati personali non possa trattare tali dati se non è istruito in tal senso dal titolare del trattamento;
- il medesimo obbligo viene ribadito al paragrafo 4 dell'art. 32 che, invece, al suo paragrafo 1 stabilisce in capo al titolare del trattamento l'obbligo di "mettere in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio".

Tutto ciò premesso, con il presente atto

**È NOMINATO AUTORIZZATO AL TRATTAMENTO DEI DATI NELL'AMBITO DELLE
MANSIONI A LEI ATTRIBUITE**

Al fine di garantire un trattamento conforme alle previsioni normative ed una adeguata tutela dei diritti degli interessati, dovrà trattare ed elaborare i dati ai quali ha accesso solo per lo svolgimento delle Sue funzioni, garantendo la riservatezza, integrità e la disponibilità dei dati ed attenendosi alle seguenti istruzioni:

1. trattare i dati di cui viene a conoscenza **esclusivamente nell'ambito dello svolgimento delle Sue funzioni e per operazioni necessarie alle finalità del trattamento per cui sono stati raccolti e successivamente trattati**, in modo lecito e secondo correttezza, astenendosi, senza preventiva autorizzazione, dal creare nuove banche dati o operare nuovi trattamenti e verificando che i dati siano pertinenti e non eccedenti le finalità per le quali sono stati raccolti e successivamente trattati, secondo le indicazioni ricevute dal Titolare; potrà trovare tutti riferimenti all'ambito di trattamento di dati che Le è consentito all'interno dell'organizzazione, nel sistema di gestione nonché nella mappa degli accessi alle informazioni che verranno mantenuti aggiornati nel tempo;
2. mantenere la riservatezza opportuna e necessaria affinché il trattamento dei dati, nell'attività affidata, sia effettuato in conformità alle disposizioni del Reg. UE 679/2016 e volte alla prevenzione da parte del titolare dei crimini informatici e del trattamento illecito di dati;
3. trattare e conservare i dati nel rispetto delle misure di sicurezza prevista dal Reg. UE 679/2016, dal Regolamento privacy dell'Istituto, delle istruzioni di seguito specificate e di quelle ulteriori impartite dal Titolare; in particolare, conservare i documenti contenenti dati particolari (ex dati sensibili e giudiziari) che Le sono affidati ai fini del trattamento, sempre e solo negli appositi contenitori muniti di serratura;
4. l'archiviazione di documenti contenenti dati particolari deve avvenire in locali ad accesso controllato (es. controllo a vista da parte del personale), salvo per gli archivi già dotati di strumenti adeguati al controllo degli accessi;
5. se incaricato della raccolta dei dati, prima di procedervi, dovrà sempre fornire l'apposita informativa all'interessato e, laddove necessario, raccogliere l'eventuale consenso al trattamento dei dati;
6. la raccolta dei dati deve essere effettuata con la massima cura, verificando con l'Interessato la completezza e l'esattezza degli stessi;
7. inserire, se preventivamente autorizzato, i dati nel sistema informatico;
8. Garantire all'interessato l'esercizio dei diritti sui propri dati che il Reg. UE 679/2016 gli riconosce (es: di accesso, di rettifica, di limitazione, di portabilità, di opposizione, ecc.); in caso di richieste in tal senso dovrà utilizzare l'apposita procedura predisposta dal Titolare;
9. conservare i supporti informatici e/o cartacei contenenti i dati, in modo da evitare che siano accessibili a persone terze e/o non autorizzate al trattamento dei dati o che potrebbero essere oggetto di danneggiamenti intenzionali e/o accidentali;
10. in particolare, con riguardo ai trattamenti senza l'ausilio di strumenti elettronici, i documenti cartacei, contenenti i dati, devono essere custoditi nei locali e/o archivi predisposti dal Titolare;
11. i documenti cartacei, contenenti i dati, dovranno essere prelevati dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni, senza lasciarli incustoditi e, in caso di allontanamento dall'ufficio, riponendoli in un luogo sicuro che dia sufficienti garanzie di protezione da accessi non autorizzati;
12. non devono essere effettuate, per uso privato, copie di documenti contenenti dati personali;
13. eventuali fotocopie non devono essere lasciate incustodite presso le stampanti;
14. laddove autorizzato e qualora sia necessario distruggere documenti contenenti dati, la distruzione definitiva deve avvenire in modo controllato ed in modalità tale da assicurare il non riutilizzo/la non leggibilità dei dati, ad esempio utilizzando gli appositi apparecchi "distruggi documenti"; in ogni caso non devono essere gettati documenti contenenti dati senza aver provveduto a renderne illeggibile il contenuto;
15. non utilizzare eventuali fotocopie o stampe di documenti contenenti dati personali come carta per appunti;
16. al termine del trattamento, gli atti e documenti vanno restituiti agli interessati o distrutti o resi inutilizzabili, salvo sia necessario conservarli per adempiere ad obblighi di legge a carico del Titolare;
17. con riferimento al trattamento con modalità elettroniche, dovrà sempre essere utilizzato il codice identificativo personale e una parola chiave (o password) che dovrà essere da Lei modificata **almeno ogni tre mesi**. La parola chiave da Lei scelta deve essere composta da almeno otto caratteri alfanumerici, non dovrà contenere riferimenti agevolmente riconducibili a Lei, non dovrà essere uguale ad una delle ultime

5 già utilizzate e non dovrà essere basata su parole di uso comune (nomi di luoghi, personaggi, mesi, giorni della settimana, ecc.); dovrà assicurare segretezza e diligente custodia della parola chiave adottando le necessarie cautele, evitando di annotarla su supporti facilmente accessibili (post-it, blocco appunti, ecc.). Nel caso si voglia mantenerne traccia scritta, per propria memoria, essa dovrà essere conservata in luogo sicuro;

18. Le credenziali d'autenticazione saranno disattivate col venir meno dell'incarico che Le consente l'accesso ai dati personali o per mancanza d'utilizzo per più di sei mesi;
19. nell'utilizzo di pc condivisi assicurarsi di uscire dal sistema operativo, chiudendo la sessione di lavoro avviata con le proprie credenziali;
20. in caso di allontanamento, anche temporaneo, dal posto di lavoro, non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di lavoro, al fine di evitare trattamenti non autorizzati;
21. i PC in dotazione agli Autorizzati, pur protetti contro gli attacchi dei virus informatici mediante appositi programmi, rimangono potenzialmente esposti ad aggressioni di virus non conosciuti e per ridurre le probabilità del verificarsi di tali attacchi è necessario che vengano osservate le seguenti regole:
 - a) controllare che il programma antivirus installato sia aggiornato periodicamente e sia attivo;
 - b) chiudere correttamente i programmi in uso;
 - c) prestare la massima attenzione nell'utilizzo dei supporti di origine esterna (per es. chiavi USB, dischi esterni ecc.), verificando con l'ausilio del programma antivirus in dotazione ogni supporto magnetico, prima dell'esecuzione dei file in esso contenuti, avvertendo immediatamente per iscritto il responsabile dell'area IT nel caso di anomalie;
 - d) non utilizzare supporti elettronici di provenienza incerta;
 - e) non modificare le configurazioni impostate sul proprio PC, spegnere lo stesso al termine della giornata di lavoro e porre la necessaria attenzione sulle eventuali notifiche di sicurezza;
 - f) usare correttamente e solo per esigenze di lavoro i servizi di posta elettronica e di Internet;
 - g) alla verifica di un malfunzionamento del PC sospendere ogni operazione, e contattare immediatamente il responsabile dell'area IT;
 - h) tutti i dati devono essere salvati sul server rispettando quanto previsto dal sistema di gestione e dalla mappa degli accessi alle informazioni;
 - i) non aprire files e/o siti non pertinenti allo svolgimento delle Sue mansioni, sospetti o di dubbia provenienza;
 - j) non scaricare o installare applicazioni/software che non siano state preventivamente approvate e autorizzate
 - k) prestare attenzione ai messaggi di posta elettronica ed ai file, programmi e oggetti allegati, ricevuti da mittenti sconosciuti o comunque sospetti;
22. accedere unicamente alle banche dati necessarie per lo svolgimento delle mansioni e degli incarichi che Le sono stati assegnati e non creare nuove banche dati;
23. evitare di portare fuori dall'Istituto supporti informatici o cartacei contenenti dati, salvo casi eccezionali che dovranno essere preventivamente autorizzati dal Titolare ed in tal caso custodire costantemente detti supporti, non perdendoli mai di vista;
24. in caso si verifichi o si sospetti un incidente di sicurezza/violazione di dati dovrà essere data immediata comunicazione al Titolare seguendo l'apposita procedura e, in caso di incidente/anomalia informatico (anche solo sospetto), contattare il referente informatico;
25. non comunicare dati di qualsiasi natura provenienti dagli archivi/banche dati aziendali senza la preventiva autorizzazione del Titolare;
26. non diffondere e/o utilizzare dati di qualsiasi natura oltre i limiti di quanto sia necessario alle finalità del trattamento e senza la preventiva specifica autorizzazione scritta del Titolare; i dati relativi alla salute degli interessati non possono **mai** essere diffusi;
27. segnalare al Titolare eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle già menzionate misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati;
28. osservare scrupolosamente tutte le istruzioni e tutte le misure di sicurezza sopra elencate, quelle già in atto e risultanti dalle procedure adottate dal Titolare e quelle che verranno successivamente adottate ed

impartite dal Titolare, nonché ogni ulteriore specifica istruzione che Le verrà impartita in relazione a determinati trattamenti;

Il Titolare si riserva la facoltà di impartire ulteriori istruzioni scritte in qualsiasi momento, ad integrazione o in sostituzione di quelle iniziali. Quali istruzioni provenienti dal Titolare del trattamento, le stesse si intendono automaticamente vincolanti per il destinatario e da questi ben comprese senza necessità di alcuna specifica formale accettazione.

La formazione è un requisito previsto come obbligatorio dal GDPR ed il Titolare considera di grande importanza la collaborazione di tutti al fine di garantire la conformità al GDPR delle attività di trattamento che vengono svolte presso le varie aree funzionali.

Lei è tenuto a partecipare a tutte le attività formative in materia di protezione dei dati personali (privacy & cybersecurity) che vengono erogate dal Titolare e/o da terzi fornitori della stessa. Tali attività potranno ad esempio essere erogate tramite sessioni d'aula, distribuzione via e-mail o consegna cartacea di circolari o altri materiali documentali, sessioni on-line interattive. Lei è tenuto a leggere immediatamente tali documenti ed a chiedere spiegazioni al Titolare nel caso in cui abbia qualsiasi dubbio circa il contenuto degli stessi.

La presente nomina decade automaticamente nel caso di cessazione, per qualsiasi motivo del rapporto con Lei in essere.

Il Titolare è inoltre a disposizione per fornire ogni eventuale ulteriore informazione, istruzione, documentazione, chiarimento e/o supporto utile all'osservanza delle prescrizioni sopra indicate.

Con la sottoscrizione della presente lettera di incarico Lei si obbliga sin d'ora, in ogni caso, a rispettare tutte le istruzioni impartite dal Titolare ed a garantire la massima riservatezza in relazione a tutti i dati trattati su istruzione del Titolare, in veste di titolare e/o responsabile del trattamento.

Per ricevuta e presa visione
L'Autorizzato

Per assunzione dell'obbligo di riservatezza
L'Autorizzato

IL DIRIGENTE DELL'ISTITUZIONE

Nicola Parzian

Firmato digitalmente. Questa nota, se trasmessa in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, predisposto e conservato presso questa Amministrazione in conformità alle regole tecniche (artt. 3 bis, c. 4 bis, e 71 D.Lgs. 82/2005). La firma autografa è sostituita dall'indicazione a stampa del nominativo del responsabile (art. 3 D.Lgs. 39/1993).