

Istituto Comprensivo Statale "Alto Casertano"

Istruzione del primo ciclo nei comuni di

**ROCCAMONFINA-ROCCAD'EVANDRO-CONCA DELLA CAMPANIA-
GALLUCCIO-SAN PIETRO INFINE-TORA E PICCILLI**

Via S. Lucia,10 - 81035- ROCCAMONFINA (CE) - Tel. 0823/677280

ceic8be00b@istruzione.it ceic8be00b@pec.istruzione.it <http://www.icaltocasertano.edu.it>

Codice meccanografico CEIC8BE00B ☒ Codice Fiscale 95022400618

IL DIRIGENTE

1. **VISTO** il Regolamento UE 2016/679 GDPR;
2. **VISTO** il Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", nel seguito indicato sinteticamente come Codice;
3. **CONSIDERATO** che questo Istituto è titolare del trattamento dei dati personali di alunni, genitori, personale dipendente, fornitori, e qualunque altro soggetto che abbia rapporti con l'Istituto medesimo e che a questo conferisca, volontariamente o per obbligo, propri dati personali;
4. **CONSIDERATO** che la titolarità del trattamento dei dati personali è esercitata dallo scrivente Dirigente dell'Istituto, in qualità di legale rappresentante dello stesso;
5. **CONSIDERATO** che gli Assistenti Amministrativi prestano servizio presso questo Istituto, ferma restando ogni responsabilità civile e penale;
6. **CONSIDERATO** che il GDPR 679/2016 richiede che il titolare organizzi la propria struttura designando Responsabili, soggetti autorizzati e responsabile della protezione dei dati;

DESIGNA L'ASSISTENTE AMMINISTRATIVO

Nome	Cognome	Codice Fiscale

AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI

in relazione alle operazioni di elaborazione di dati personali, su supporto cartaceo e/o elettronico, ai quali ha accesso nell'espletamento delle funzioni e dei compiti assegnati nell'ambito del rapporto

di lavoro con questa istituzione scolastica e disciplinati dalla normativa in vigore e dai contratti di settore. In particolare, in qualità di addetto alla Segreteria amministrativa della scuola è incaricato delle operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modifica, comunicazione (nei soli casi autorizzati dal titolare o dal responsabile del trattamento), selezione, estrazione di dati, connesse alle seguenti funzioni e attività esercitate:

- alunni e tutori
- gestione archivi elettronici alunni e tutori;
- gestione archivi cartacei con fascicoli personali alunni;
- consultazione documenti e registri di attestazione dei voti e di documentazione della vita scolastica dello studente, nonché delle relazioni tra scuola e famiglia quali ad esempio richieste, istanze e corrispondenza con le famiglie;
- gestione contributi e/o tasse scolastiche versati da alunni e genitori;
- adempimenti connessi alla corretta gestione del Registro infortuni;
- adempimenti connessi ai viaggi di istruzione e visite guidate;
- personale ATA e Docenti;
- gestione archivi elettronici Personale ATA e Docenti;
- gestione archivi cartacei Personale ATA e Docenti;
- tenuta documenti e registri relativi alla vita lavorativa dei dipendenti (quali ad esempio assenze, convocazioni, comunicazioni, documentazione sullo stato del personale, atti di nomina dei supplenti, decreti del Dirigente);
- contabilità e finanza;
- gestione archivi elettronici della contabilità;
- gestione stipendi e pagamenti, nonché adempimenti di carattere previdenziale;
- gestione documentazione ore di servizio (quali ad esempio, registrazione delle ore eccedenti);
- gestione rapporti con i fornitori di beni e servizi;
- gestione Programma annuale, fondo di istituto, fondi comunitari e fondi derivanti da altri progetti, concorsi, ecc.;
- corretta tenuta dei registri contabili previsti dal Decreto interministeriale n. 129/2018 e correlata normativa vigente;
- attività di protocollo e archiviazione della corrispondenza ordinaria;

- attività organi collegiali;
- eventuale operazione di consultazione e estrazione dati dai verbali degli organi collegiali;
- tutte le attività che prevedono trattamento dati nell'ambito delle mansioni di lavoro.

Questo istituto nell'ambito dell'attività di mappatura dei trattamenti operati ne ha individuato 10 diseguito elencati. Su quelli spuntati è concessa l'autorizzazione al trattamento.

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 dirigente, docente, educativo ed ATA e 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	<input type="checkbox"/>
4	Attività propedeutiche all'avvio dell'anno scolastico, ai corsi, e a tutte le attività formative. I dati sono forniti dagli alunni, dalle famiglie, dalle persone ai fini della frequenza dei corsi di studi nelle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandi e scuole speciali.	<input type="checkbox"/>
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 ed orientamento, di scrutini ed esami, valutazione periodica e finale, per le attività di orientamento e per la certificazione delle competenze	<input type="checkbox"/>
7	Rapporti scuola-famiglie-altri soggetti: gestione del contenzioso. Il trattamento dei dati concernenti tutte le attività connesse alla instaurazione di contenzioso (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce, all'autorità giudiziaria, etc.) con gli alunni e con le famiglie, e tutte le attività relative alla difesa in giudizio delle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandi e scuole speciali.	<input type="checkbox"/>
8	Rapporti con i fornitori di beni e servizi. Il trattamento dei dati concernenti tutte le attività connesse alla instaurazione di rapporti di fornitura di beni e servizi, albo fornitori, gestione della rotazione, manifestazioni di interesse, e similari	<input type="checkbox"/>

I trattamenti devono essere eseguiti tenendo presenti le istruzioni operative che seguono:

1. Il trattamento dei dati personali a cui è autorizzato ad accedere deve avvenire secondo le modalità definite dalla normativa in vigore, in modo lecito e secondo correttezza e con l'osservanza - in particolare - delle prescrizioni di cui al Regolamento UE 2016/679 e al D.lgs. 196/2003;

2. il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali della scuola. L'autorizzato al trattamento agisce sotto la diretta autorità del Titolare e deve attenersi alle istruzioni da esso impartite;

3. i dati personali, oggetto dei trattamenti, devono essere esatti ed aggiornati, inoltre devono essere pertinenti, completi e non eccedenti le finalità per le quali vengono raccolti e trattati e conservati per il tempo strettamente necessario;

4. è vietato l'inserimento di documenti e files con dati particolari (sensibili) degli alunni, delle famiglie o di altre persone nelle cartelle condivise locali. La conservazione e gestione dei documenti su repository esterne è ammessa solo con pseudonimizzazione e crittografia dei dati. Il trattamento dei dati deve avvenire nell'ambito di una struttura organizzativa adeguata al rischio, in applicazione

delle regole di sicurezza minime AGID e delle valutazioni effettuate in sede di redazione del piano di sicurezza dei dati;

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 responsabile o dal titolare del trattamento. Si raccomanda particolare *Documenti Firmati digitalmente ai sensi del Codice Amministrazione Digitale e norme ad esso connesse.*

attenzione alla tutela del diritto alla riservatezza degli interessati e di consultare il regolamento approvato da questo Istituto e/o di consultare il titolare, il responsabile o il responsabile della protezione dei dati RPD/DPO in caso di dubbi, sempre prima di effettuare qualunque comunicazione dati a terzi.

6. si ricorda che l'obbligo di mantenere la dovuta riservatezza in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico, deve permanere in ogni caso, anche quando sia venuto meno l'incarico stesso;

7. i trattamenti andranno effettuati rispettando le misure di sicurezza predisposte nell'istituzione scolastica. in ogni operazione di trattamento andrà garantita la massima riservatezza e custodia degli atti e dei documenti contenenti dati personali che non andranno mai lasciati incustoditi o a disposizione di terzi non autorizzati ad accedervi, prendervi visione o ad effettuare qualsivoglia operazione. Si invita alla lettura periodica del piano di sicurezza predisposto da questo istituto. Il piano, infatti, costantemente aggiornato contiene tra l'altro le procedure di sicurezza da seguire, istruzioni e procedure operative per il personale, indicazione dei soggetti a cui possono essere comunicati i dati.

8. le credenziali di autenticazione (codice di accesso e parola chiave per accedere ai computer e ai servizi web) attribuite sono personali e devono essere custodite con cura e diligenza; non possono essere messe a disposizione né rivelate a terzi; non possono essere lasciate incustodite, né in libera visione, aggiornate con cadenza trimestrale, essere sufficientemente complesse e non riconducibili alla persona. In caso di smarrimento e/o furto, bisogna darne immediata notizia al responsabile, al titolare e al Responsabile della protezione dei dati RPD/DPO. Programmare, avvalendosi delle credenziali conservate dal custode delle password, una immediata e tempestiva sostituzione delle credenziali di accesso smarrite o rubate.

9. Nel caso in cui per l'esercizio delle attività sopra descritte sia inevitabile l'uso di supporti rimovibili (quali ad esempio Pendrive USB, CD-ROM, ecc.), su cui sono memorizzati dati personali, essi vanno custoditi con cura, né messi a disposizione o lasciati al libero accesso di persone non autorizzate. Al fine di garantire idonea protezione da rischio di smarrimento o furto è necessario che i dati su supporti rimovibili o comunque esterni (drive, cloud) siano pseudonimizzati e/o crittografati.

10. si ricorda inoltre che i supporti rimovibili contenenti dati particolari (sensibili e/o giudiziari) se non utilizzati vanno distrutti o resi inutilizzabili;

11. si ricorda inoltre che l'accesso agli archivi contenenti dati particolari (sensibili e/o giudiziari) è permesso solo alle persone autorizzate e soggetto a continuo controllo secondo le regole definite dallo scrivente;

12. i documenti contenenti dati personali durante i trattamenti vanno mantenuti in modo tale da non essere alla portata di vista di persone non autorizzate;

13. al termine del trattamento occorre custodire i documenti contenenti dati personali all'interno di archivi/cassetti/armadi muniti di serratura;

14. i documenti della scuola contenenti dati personali non possono uscire dalla sede scolastica, né copiati, se non dietro espressa autorizzazione del responsabile o dal titolare del trattamento;

15. in caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati, l'incaricato dovrà verificare che non vi sia possibilità da parte di terzi, anche se dipendenti non incaricati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento;

16. le comunicazioni agli interessati (persone fisiche a cui afferiscono i dati personali) dovranno avvenire in forma riservata; se effettuate per scritto dovranno essere consegnate in contenitori chiusi;

17. all'atto della consegna di documenti contenenti dati personali l'incaricato dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta;

18. in caso di comunicazioni elettroniche ad alunni, colleghi, genitori, personale della scuola o altri soggetti coinvolti per finalità istituzionali, queste (comunicazioni) vanno poste in essere seguendo le indicazioni fornite dall'Istituzione scolastica e avendo presente la necessaria riservatezza delle comunicazioni stesse e dei dati coinvolti;

Documento Firmato digitalmente ai sensi del Codice Amministrazione Digitale e norme ad esso connesse.

19. Attenersi alle disposizioni ulteriori del titolare, del responsabile o del responsabile della protezione dei dati;

20. Per la corretta applicazione del GDPR 679/2016 e del DLGS 196/2003 tutto il personale ha ricevuto o riceverà, secondo il calendario degli eventi formativi predisposto, idonea formazione.

21. Regole di Gestione della Videoconferenza o partecipazione a lezioni in modalità sincrona. La registrazione della videoconferenza può essere effettuata a condizione che il file relativo sia accessibile esclusivamente al personale scolastico a cui si riferiscono, accessibile con le opportune credenziali di autenticazione. Il relatore deve informare preventivamente i partecipanti alla videoconferenza attraverso disclaimer o indicazioni verbali che la diffusione delle immagini può comportare, responsabilità di natura civile e penale. Il Video **non può** essere oggetto di divulgazione. E' vietato pertanto la pubblicazione su altri siti o canali Social anche dell'Istituto non dedicati alla formazione a distanza con gestione degli accessi; è vietato, altresì, anche consentire a persone diverse da quelle indicate la visione del video attraverso l'invio di link tramite mail o altri canali aggirando le regole di accesso e gestione della piattaforma utilizzata.

22. Regole di Gestione di sistemi di messaggistica istantanea (WhatsApp, Telegram, Signal, ecc.). Si sconsiglia vivamente la gestione congiunta di gruppi. I messaggi dovrebbero essere inviati sempre con modalità broadcast. Il numero di telefono è un dato personale, la condivisione dello stesso deve essere preceduta da informativa e richiesta di consenso in quanto l'uso di queste applicazioni potrebbe comportare passaggi informazioni di testo e multimediali che per contenuti ed immagini siano in opposizione con le finalità pubbliche del servizio, portare disturbo, numerosità elevata di messaggi classificabile come spam etc.

Il Personale dovrà attenersi a quanto previsto nel Regolamento emanato dal Consiglio di Istituto e a tutte le misure tecniche e organizzative legate alla sicurezza adottate. Nuove istruzioni operative ad integrazione, modifica o sostituzione, potranno essere formulate dal Titolare in seguito agli audit effettuati ai sensi del principio di privacy by design e by default nel corso dell'intera durata del rapporto

Istruzioni operative ulteriori per il rispetto del GDPR 679/2016 in caso di utilizzo di postazioni informatiche, applicazioni in cloud e sistemi di comunicazione digitali.

Postazioni informatiche:

- Accesso ai portali in Cloud con un PC o notebook sul quale è installato
 - il sistema operativo Windows 11, Windows, 10 o Windows 8;
 - un software antivirus e antimalware;
 - Gestione delle credenziali di accesso con password complesse di almeno 14 caratteri, caratteri speciali, numeri, maiuscole e minuscole.

Procedure di accesso in remoto nei portali in cloud:

- NON SALVARE le password di accesso;
- Effettuare il logout alla fine di ogni sessione di lavoro;
- Accesso esclusivo alla visualizzazione delle informazioni personali presenti nelle piattaforme in cloud. (Assicurarsi che nessuno anche tra familiari ed amici possa visualizzare le informazioni a video. In caso di momentaneo allontanamento dalla postazione effettuare il logout dalle piattaforme. Spegnere la postazione di lavoro e/o utilizzare alti strumenti tecnici (screen saver con password) in modo da impedire la visualizzazione di documenti con dati personali presenti.

Documentazione Analogica (cartacea)

- Dati personali contenuti in documenti assolutamente necessari allo svolgimento delle mansioni affidate al di fuori della struttura dell'Istituto devono essere gestite con la massima attenzione per garantirne la conservazione e la protezione per il periodo strettamente necessario allo svolgimento delle mansioni affidate.

Documento Firmato digitalmente ai sensi del Codice Amministrazione Digitale e norme ad esso connesse.

Documentazione Digitale

- Utilizzo di pendrive con CRITTOGRAFIA per il salvataggio di eventuale documentazione utile al lavoro fuori sede. In alternativa alla Crittografia si può applicare la pseudonimizzazione.

Accesso Remoto

Il Titolare ha individuato, con la collaborazione dell'Amministrazione di Sistema, sistemi per l'accesso remoto alle postazioni di lavoro site nell'Istituzione Scolastica che hanno requisiti tali da garantire misure di sicurezza adeguate (teamviewer, logmein, supremo, desktop remoto) etc.

Il titolare provvederà all'acquisto delle licenze necessarie ed alla formazione, per il tramite dell'amministratore di sistema, all'uso delle tecnologie adottate.

All'amministratore di sistema viene affidato anche il compito di, valutata la struttura informatica preesistente dell'Istituto, realizzare connessione protette VPN per una gestione ottimizzata degli accessi da remoto. Nel caso venissero utilizzate tecnologie e strumenti diversi verranno fornite dal titolare gli accessi e le istruzioni operative.

Si ricorda che l'art 4 della legge 300/70 Statuto dei Lavoratori vieta i controlli a distanza sui

lavoratori, le tecnologie utilizzate tuttavia potrebbero tenere log degli accessi effettuati con data e ora e indirizzo IP o id client per ragioni legate alla sicurezza.

Ai sensi dell'art 13 del GDPR 679/2016 verranno pubblicate sul sito web dell'Istituto le privacy policy delle tecnologie adottate al fine di consentire a tutti gli utilizzatori di avere ben chiare le modalità di gestione, conservazione e trasmissione delle informazioni veicolate.

Il Dirigente Scolastico
Dott.ssa Maddalena Di Cerbo

_____,li_____

Per ricevuta: _____