Via Roma snc 67054 CIVITELLA ROVETO (AQ) - Tel. 0863 97140 Fax 0863 979095
Cod. Mecc. AQIC83900L – C.F. 90038870664
www.icenricomattei.edu.it – e-mail aqic83900l@istruzione.it – pec aqic83900l@pec.istruzione.it

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 i docenti, in servizio presso questo Istituto (in tale ambito, ai fini del presente incarico, si fanno rientrare anche i docenti esterni incaricati ufficialmente di funzioni nella scuola quali ad esempio esami, corsi, e attività integrative), per l'espletamento delle loro funzioni, hanno necessità di venire a conoscenza e di trattare dati personali relativi prevalentemente agli alunni di questa Istituzione Scolastica, fermi restando gli obblighi e le responsabilità civili e penali;

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 RPD/DPO;

DESIGNA IL DOCENTE

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 Docente è incaricato delle operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, modifica, connesse alle seguenti funzioni e attività svolte:

- alunni e genitori
- attività didattica e partecipazione agli organi collegiali;
- valutazione alunni;
- tenuta 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;

- rapporti con famiglie e alunni in situazione di disagio psico-sociale;
- ricezione di certificati medici relativi allo stato di salute degli alunni, documentazione alunni disabili, documentazione mensa/intolleranze, documentazione DSA e BES, nei limiti sempre di quanto strettamente indispensabile;
- eventuali contributi e/o tasse scolastiche versati da alunni e genitori;
- adempimenti connessi alle visite guidate e ai viaggi d'istruzione;
- conoscenza di dati relativi a professioni di fede religiosa;
- eventuali adempimenti connessi al rapporto di pubblico impiego, ad esempio la registrazione delle presenze, le attestazioni inerenti lo stato del personale, ecc.

Questo istituto nell'ambito dell'attività di mappatura dei trattamenti operati ne ha individuato 10 di seguito 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	☐
2	**Gestione del contenzioso e procedimenti disciplinari**. Il trattamento dei dati concerne tutte le attività relative alla difesa in giudizio del Ministero dell'Istruzione 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 Istruzione e dell'ordinamento scolastico. Tali organi sono rappresentativi sia del personale amministrativo e scolastico, sia 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, dalle persone ai fini della frequenza dei corsi di studi nelle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali.	☐
5	**Attività educativa, didattica e formativa**, **e di valutazione**. Il trattamento dei dati necessari all'espletamento delle attività educative, didattiche e formative, curriculari ed extracurriculari, di valutazione ed orientamento, di scrutini ed esami, valutazione periodica e finale, per le attività di orientamento e per la certificazione delle competenze	☐
6	Scuole non statali (TRATTAMENTO NON UTILIZZATO NELLA SCUOLA PUBBLICA) si riporta per numerazione	
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, educandati e scuole speciali.	☐

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	☐
9	**Rapporti con enti e associazioni**. Il trattamento dei dati concernenti tutte le attività connesse alla instaurazione di rapporti con enti pubblici, assimilati, e associazioni	☐
10	**Video Sorveglianza.** Il trattamento dei dati concernenti le attività di gestione, conservazione dati, gestione degli accessi, ai sistemi di videosorveglianza	☐

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 sono con pseudonimizzazione e crittografia dei dati. Il trattamento 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 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 removibili 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;

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 o antimalware;
    - gestione delle credenziali di accesso con password complesse di almeno 10 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 una volta si loggati e si svolgono operazioni su dati presenti nelle piattaforme in cloud. (assicurarsi che nessuno anche tra familiari ed amici possa visualizzare le informazioni a video e anche in caso di momentaneo allontanamento dalla postazione, effettuare il logout dalle piattaforme e spegnere la postazione di lavoro e/o utilizzare alti strumenti tecnici (screen saver con password) per impedire la visualizzazione di documenti con dati personali presenti anche accidentali

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.

Documentazione Digitale

- Utilizzo di pendrive con CRITTOGRAFIA per il salvataggio di eventuale documentazione utile al lavoro fuori sede. In alternativa alla Crittografia 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
LUCIA TROIANO
Documento firmato digitalmente ai sensi del Codice Amministrazione Digitale e norme ad esso connesse

_____li, _____

Per Ricevuta: _____