Ministero dell'Istruzione e del Merito
ISTITUTO PROFESSIONALE INDUSTRIA E ARTIGIANATO
"Ostilio Ricci"
Sede Centrale – Via S D'Acquisto, 71 - 63900 Fermo - Cod. fisc. 81006180442
Tel. 0734/228829 - www.ipsiafermo.edu.it e-mail: apri02000q@istruzione.it

Prot. n. 17162
Fermo, 23/10/2026

Agli Assistenti Amministrativi
Agli Assistenti Tecnici
Bacheca Segreteria Digitale
Sito Internet Istituzionale

Oggetto: **protezione dei dati personali ai sensi del Regolamento UE 2016/679 e del D.Lgs. n. 196/2003, come modificato dal D.Lgs. n. 101/2018 - designazione delle persone autorizzate al trattamento Struttura operativa: Area Segreteria e Area Tecnica**

LA DIRIGENTE

1. VISTO il Regolamento UE 2016/679 (di seguito "GDPR") con particolare riguardo agli artt. 5, 24, 29 e 32, par. 4;
2. VISTO il Decreto Legislativo 30 giugno 2003, n. 196, *"Codice in materia di protezione dei dati personali"*, come modificato dal Decreto Legislativo 10 agosto 2018, n. 101, nel seguito indicato sinteticamente come *Codice*, ed in particolare l'art. 2-quaterdecies (attribuzione di funzioni e compiti a soggetti designati);
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 dalla scrivente Dirigente dell'Istituto, in qualità di legale rappresentante dello stesso;
5. CONSIDERATO che le SS.LL. prestano servizio presso questo Istituto come Assistenti Amministrativi, addetti alla Struttura operativa: Area Segreteria, e come Assistenti Tecnici, addetti ai laboratori, ferma restando ogni responsabilità civile e penale;

DESIGNA

le SS.LL. quali

PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI PERSONALI

(art. 29 GDPR e art. 2-quaterdecies del Codice)

in relazione alle operazioni di elaborazione di dati personali, su supporto cartaceo e/o elettronico, ai quali le SS.LL. hanno 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 addetti alla Segreteria amministrativa della scuola e ai laboratori** le SS.LL. sono autorizzate alle operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modifica, comunicazione (nei soli casi autorizzati dal titolare del trattamento), selezione, estrazione, cancellazione di dati, connesse alle seguenti funzioni e attività dalle SS.LL. esercitate:

DIDATTICA

- Gestione archivi elettronici alunni e genitori inclusa anagrafe nazionale alunni del Ministero;
- Trattamento pratiche iscrizione e trasferimenti alunni;
- Gestione elettronica e digitale fascicoli personali alunni e archivio contenente documentazione sensibile;

Documento informatico firmato digitalmente da ANNAMARIA BERNARDINI ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate

- Gestione delle certificazioni e della documentazione relativa ad alunni con disabilità, DSA e BES;
- Protocollazione/archiviazione registri di classe, docenti e documenti consiglio di classe;
- 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;
- Convocazione Consigli di classe, interclasse, intersezione, Gruppi;
- Gestione contributi e/o tasse scolastiche versati da alunni e genitori, anche tramite la piattaforma pagoPA;
- Adempimenti connessi alla corretta gestione del Registro infortuni;

PERSONALE
- Gestione graduatorie interne e graduatorie di Istituto;
- Tenuta documenti e registri relativi alla vita lavorativa dei dipendenti (quali ad es. assenze, convocazioni, comunicazioni, documentazione sullo stato del personale, atti di nomina dei supplenti, decreti del Dirigente);
- Gestione delle pratiche relative a malattie, infortuni, permessi ex L. 104/92 e altre condizioni di salute del personale;
- Gestione archivi elettronici e cartacei Personale ATA e Docenti;
- Gestione documentazione ore di servizio (quali ad esempio, registrazione delle ore eccedenti);

ACQUISTI E CONTABILITA'
- gestione archivi elettronici della contabilità;
- gestione stipendi e pagamenti, nonché adempimenti di carattere previdenziale;
- gestione rapporti con i fornitori;
- gestione Programma annuale e fondo di istituto;
- corretta tenuta dei registri contabili previsti dal Decreto interministeriale n. ~~44/2001~~ 129/2018 e correlata normativa vigente;
- adempimenti connessi alle gite scolastiche;

Protocollo e archivio corrispondenza ordinaria
- attività di protocollo e archiviazione della corrispondenza ordinaria;
- gestione della posta elettronica istituzionale e certificata (PEO/PEC) e delle pubblicazioni all'Albo online e in "Amministrazione trasparente";

Assistenti tecnici
- gestione materiale ed elaborati alunni;
- gestione delle postazioni informatiche dei laboratori e degli account utilizzati dagli alunni.

Si rende noto, a tal fine, che le operazioni sopra descritte vanno rigorosamente effettuate tenendo presenti le istruzioni operative che seguono:

1. il trattamento dei dati personali cui le SS.LL. sono autorizzate 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 e successive modificazioni;
2. il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali della scuola;

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;
4. 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 del trattamento. Si raccomanda particolare attenzione alla tutela del diritto alla riservatezza degli interessati (persone fisiche a cui afferiscono i dati personali);
5. 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;
6. 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 trattamento;
7. le eventuali credenziali di autenticazione (codice di accesso e parola chiave per accedere ai computer e ai servizi web) attribuite alle SS.LL. 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. In caso di smarrimento e/o furto, bisogna darne immediata notizia secondo quanto previsto al successivo punto 27;
8. nel caso in cui per l'esercizio delle attività sopra descritte sia inevitabile l'uso di supporti rimovibili (quali ad esempio chiavi 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; ove possibile, i dati memorizzati su tali supporti vanno protetti con cifratura o password;
9. si ricorda inoltre che i supporti rimovibili contenenti categorie particolari di dati (art. 9 GDPR) e/o dati relativi a condanne penali e reati (art. 10 GDPR), se non utilizzati, vanno distrutti o resi inutilizzabili;
10. si ricorda inoltre che l'accesso agli archivi contenenti categorie particolari di dati o dati relativi a condanne penali e reati è permesso solo alle persone autorizzate e soggetto a continuo controllo secondo le regole definite dalla scrivente;
11. durante i trattamenti i documenti contenenti dati personali vanno mantenuti in modo tale da non essere alla portata di vista di persone non autorizzate;
12. al termine del trattamento occorre custodire i documenti contenenti dati personali all'interno di archivi/cassetti/armadi muniti di serratura;
13. i documenti della scuola contenenti dati personali non possono uscire dalla sede scolastica, né essere copiati, se non dietro espressa autorizzazione del titolare del trattamento;
14. in caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati, la persona autorizzata dovrà 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;
15. 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;
16. all'atto della consegna di documenti contenenti dati personali la persona autorizzata dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta;
17. 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

18. il trattamento dei dati personali va effettuato esclusivamente con le postazioni di lavoro e gli strumenti forniti dall'Istituzione scolastica. L'eventuale utilizzo di dispositivi personali (pc, notebook, tablet, smartphone), anche in caso di lavoro agile, è consentito solo previa autorizzazione e a condizione che i dispositivi abbiano un sistema operativo aggiornato e aggiornabile, ossia ancora supportato dal produttore e destinatario degli aggiornamenti di sicurezza, un software antivirus regolarmente licenziato e costantemente aggiornato, credenziali di accesso personali e blocco automatico dello schermo; sui dispositivi personali i dati non vanno memorizzati localmente;
19. non è consentito installare software, estensioni o applicazioni sulle postazioni di lavoro senza autorizzazione; in caso di allontanamento dalla postazione occorre bloccare lo schermo e, al termine della sessione di lavoro, disconnettersi dagli applicativi (SIDI, NoiPA, gestionali di segreteria, protocollo informatico); le credenziali di accesso agli applicativi ministeriali e gestionali non possono essere condivise con colleghi, nemmeno temporaneamente;
20. le comunicazioni via e-mail vanno effettuate esclusivamente con gli account istituzionali; negli invii a più destinatari esterni gli indirizzi vanno inseriti nel campo "Ccn" (copia conoscenza nascosta); occorre prestare la massima attenzione ai messaggi sospetti (phishing): non aprire allegati o collegamenti di provenienza dubbia, non comunicare credenziali in risposta a richieste ricevute via e-mail, telefono o messaggio e segnalare subito eventuali anomalie;
21. è vietato utilizzare, per la conservazione, la condivisione o la trasmissione di dati personali, strumenti non messi a disposizione o non autorizzati dall'Istituzione scolastica (ad es. servizi di messaggistica istantanea, account di posta elettronica personali, servizi cloud personali), nonché inserire dati personali di alunni, famiglie o personale in servizi di intelligenza artificiale generativa o in altre applicazioni online non autorizzate;
22. la pubblicazione di atti e documenti all'Albo online e nella sezione "Amministrazione trasparente" del sito istituzionale deve rispettare il principio di minimizzazione: vanno pubblicati solo i dati personali necessari e pertinenti rispetto alla finalità, oscurando quelli non indispensabili; non devono mai essere pubblicati dati relativi alla salute o alla condizione di disabilità (ad es., nelle graduatorie, le precedenze ex L. 104/92 vanno indicate senza riferimento alla condizione sanitaria) né dati relativi a condanne penali e reati; i documenti vanno rimossi alla scadenza del periodo di pubblicazione previsto;
23. le certificazioni mediche, la documentazione relativa ad alunni con disabilità, DSA e BES e i dati relativi a malattie, infortuni e condizioni di salute del personale e degli alunni vanno conservati separatamente dagli altri documenti, in fascicoli o cartelle ad accesso limitato, e consultati solo da chi ne abbia necessità per i compiti assegnati; nelle comunicazioni ordinarie va indicata, ove possibile, la sola assenza e non la relativa causa;
24. le richieste di accesso agli atti (L. 241/1990), di accesso civico e le istanze con cui gli interessati esercitano i diritti previsti dagli artt. 15-22 GDPR (accesso, rettifica, cancellazione, ecc.) vanno trasmesse tempestivamente alla Dirigente Scolastica, che ne cura il riscontro anche con il supporto del DPO; non vanno fornite informazioni su alunni o personale, in particolare per telefono, a soggetti di cui non siano state verificate l'identità e la legittimazione;
25. i documenti e i fascicoli vanno conservati per i tempi previsti dal massimario di conservazione e scarto e dalla normativa archivistica; lo scarto avviene solo secondo le procedure previste, previa autorizzazione della competente Soprintendenza archivistica, e i documenti cartacei da eliminare vanno distrutti con il distruggidocumenti o con modalità equivalenti, non gettati nei comuni contenitori dei rifiuti;

26. gli Assistenti Tecnici, nella gestione dei laboratori, verificano che sulle postazioni utilizzate dagli alunni non restino memorizzati dati personali (elaborati, credenziali, file scaricati) oltre il tempo necessario e che gli interventi di manutenzione non comportino l'accesso a dati personali non necessari; l'eventuale attribuzione di funzioni di amministratore di sistema è oggetto di specifica designazione;
27. qualsiasi violazione dei dati personali, anche solo sospetta (ad es. invio di e-mail o documenti a destinatari errati, smarrimento o furto di documenti, chiavi o dispositivi contenenti dati, accesso non autorizzato a uffici, archivi o agli applicativi gestionali e ministeriali), va segnalata immediatamente alla Dirigente Scolastica e al Responsabile della Protezione dei Dati (DPO), per consentire all'Istituto di valutarne la notifica al Garante entro 72 ore (artt. 33 e 34 GDPR);
28. alla cessazione del rapporto di lavoro o dell'incarico (ad es. termine della supplenza, trasferimento), le SS.LL. sono tenute a restituire i documenti e gli eventuali supporti contenenti dati personali in loro possesso e a non conservarne copie; gli accessi agli applicativi vengono contestualmente disattivati;
29. le SS.LL. sono tenute a partecipare alle iniziative di formazione in materia di protezione dei dati personali organizzate dall'Istituto.

La violazione delle presenti istruzioni può comportare responsabilità disciplinare, oltre alle responsabilità civili e penali previste dalla normativa vigente.
Il Responsabile della Protezione dei Dati (DPO) dell'Istituto è la società Tecnob S.r.l. (referente sig. Dino Elisei), con sede in Via Direttissima del Conero, 39/41 – 60021 Camerano (AN), contattabile all'indirizzo e-mail dpo@tecnob.it, PEC amministrazione@pec.tecnob.it, tel. 071 9202848.
La presente designazione ha validità per tutta la durata del rapporto di lavoro con l'Istituto e sostituisce le precedenti. Le SS.LL. sono tenute a confermarne la presa visione secondo le modalità indicate dall'Ufficio del personale.

IL DIRIGENTE SCOLASTICO
Prof.ssa Annamaria Bernardini
(Firmato digitalmente)