ISTITUTO COMPRENSIVO
BADOLATO - GUARDAVALLE
"A. MORO"
Scuola dell'infanzia, Primaria e Secondaria di primo grado
Via Nazionale snc, 88060 - Badolato (CZ) tel. 0967 814185 – fax 0967811939
Posta istituzionale: czic818007@istruzione.it – czic818007@pec.istruzione.it
sito web: www.icbadolato.edu.it
Codice meccanografico: czic818007 – codice fiscale: 97035190798

APPENDICE 22

REGOLAMENTO INTERNO PER LA PRIVACY, LA PROTEZIONE E IL TRATTAMENTO DEI DATI PERSONALI

Natura del documento

La presente Appendice integra il Regolamento d'Istituto e disciplina, in chiave organizzativa e comportamentale, i principi e le regole interne per il trattamento dei dati personali. Essa **non sostituisce** le informative rese agli interessati ai sensi degli artt. 12, 13 e 14 GDPR, il Registro delle attività di trattamento, gli atti di designazione o autorizzazione, i contratti o atti di nomina dei responsabili del trattamento, le procedure di sicurezza, le valutazioni d'impatto, né le ulteriori misure di responsabilizzazione adottate dall'Istituto

Premessa

La protezione dei dati personali costituisce parte integrante della tutela della dignità, della riservatezza, dell'identità personale e digitale di alunni, famiglie, personale e di ogni soggetto che entri in relazione con l'Istituto.

Il presente Regolamento disciplina le modalità con cui l'Istituto applica i principi di liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione, esattezza, limitazione della conservazione, integrità, riservatezza e responsabilizzazione previsti dal GDPR .

In coerenza con la natura pubblica dell'istituzione scolastica, i trattamenti necessari allo svolgimento delle funzioni istituzionali sono fondati, di regola, sull'adempimento di obblighi legali o sull'esecuzione di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri, e non sul consenso.

Indice

- Art. 1 – Oggetto, finalità e rapporto con il Regolamento d'Istituto
- Art. 2 – Fonti normative e atti di riferimento
- Art. 3 – Ambito di applicazione e categorie di interessati
- Art. 4 – Definizioni essenziali
- Art. 5 – Principi del trattamento
- Art. 6 – Ruoli privacy e responsabilità interne
- Art. 7 – Basi giuridiche, finalità e consenso
- Art. 8 – Tipologie di dati trattati
- Art. 9 – Categorie particolari di dati e dati relativi a reati
- Art. 10 – Informative e trasparenza verso gli interessati
- Art. 11 – Comunicazione, diffusione, pubblicazione e Amministrazione Trasparente
- Art. 12 – Registro elettronico, piattaforme, cloud, posta elettronica e strumenti digitali
- Art. 13 – Intelligenza artificiale e sistemi automatizzati
- Art. 14 – Immagini, audio, video, sito web e social network
- Art. 15 – Dispositivi personali, chat, fotografie e registrazioni effettuate da privati
- Art. 16 – Diritti degli interessati e accesso agli atti
- Art. 17 – Sicurezza, credenziali, documenti e gestione degli incidenti
- Art. 18 – Data breach
- Art. 19 – Valutazione d'impatto e privacy by design/by default
- Art. 20 – Responsabili esterni, fornitori e trasferimenti di dati
- Art. 21 – Conservazione, archiviazione e cancellazione
- Art. 22 – Obblighi del personale e regole di comportamento
- Art. 23 – Reclami, segnalazioni e rapporti con il RPD/DPO
- Art. 24 – Approvazione, pubblicazione e aggiornamento
- Allegato A – Matrice sintetica dei principali trattamenti
- Allegato B – Procedura interna essenziale in caso di data breach

Art. 1 – Oggetto, finalità e rapporto con il Regolamento d'Istituto

1. La presente Appendice è parte integrante del Regolamento d'Istituto e stabilisce le regole generali per il trattamento dei dati personali effettuato nell'ambito delle attività didattiche, educative, amministrative, contabili, organizzative, istituzionali e di gestione del rapporto di lavoro

2. Essa si applica a tutto il personale, agli organi collegiali, agli studenti per quanto compatibile con età e ruolo, ai collaboratori, ai tirocinanti, ai fornitori e a ogni soggetto che tratti dati personali per conto dell'Istituto
3. In caso di contrasto con norme imperative, provvedimenti dell'Autorità Garante o disposizioni ministeriali sopravvenute, prevalgono queste ultime.

Art. 2 – Fonti normative e atti di riferimento

Il presente Regolamento è redatto tenendo conto, nel testo vigente, in particolare delle seguenti fonti:

- Regolamento (UE) 2016/679 (GDPR), con particolare riferimento agli artt. 5, 6, 9, 10, 12-22, 24, 25, 28, 29, 32, 33, 34, 35, 37-39, 44 e ss.;
- D.lgs. 30 giugno 2003, n. 196, come modificato dal D.lgs. 10 agosto 2018, n. 101;
- Legge 7 agosto 1990, n. 241;
- D.lgs. 14 marzo 2013, n. 33;
- D.lgs. 7 marzo 2005, n. 82 (CAD);
- D.P.R. 8 marzo 1999, n. 275;
- D.lgs. 16 aprile 1994, n. 297;
- D.M. 7 dicembre 2006, n. 305, per quanto applicabile;
- normativa di settore in materia di istruzione, inclusione, disabilità, DSA, lavoro pubblico e conservazione documentale;
- Regolamento (UE) 2024/1689 (AI Act), per i profili applicabili:
- provvedimenti, pareri, FAQ e linee guida del Garante per la protezione dei dati personali in ambito scolastico.

Art. 3 – Ambito di applicazione e categorie di interessati

I trattamenti dell'Istituto possono riguardare, tra gli altri:

- alunni e studenti iscritti, frequentanti, trasferiti o candidati all'iscrizione;
- genitori, esercenti la responsabilità genitoriale, tutori, affidatari e delegati;
- personale dirigente, docente, educativo e ATA;
- membri degli organi collegiali;
- esperti esterni, tirocinanti, volontari e collaboratori;
- fornitori, operatori economici, professionisti, rappresentanti di enti e amministrazioni;
- utenti dei servizi digitali, visitatori e altri soggetti che interagiscono con l'Istituto.

Art. 4 – Definizioni essenziali

Ai fini del presente Regolamento si applicano le definizioni del GDPR. In particolare:

- **dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile;
- **trattamento**: qualsiasi operazione compiuta su dati personali, con o senza strumenti automatizzati;
- **categorie particolari di dati**: i dati di cui all'art. 9 GDPR;
- **dati relativi a condanne penali e reati**: i dati disciplinati dall'art. 10 GDPR;
- **titolare del trattamento**: l'Istituto scolastico, rappresentato dal Dirigente scolastico;
- **responsabile del trattamento**: il soggetto che tratta dati personali per conto del titolare ai sensi dell'art. 28 GDPR;
- **persona autorizzata**: chi tratta dati sotto l'autorità del titolare o del responsabile, su istruzioni ricevute;
- **RPD/DPO**: il Responsabile della Protezione dei Dati designato ai sensi degli artt. 37-39 GDPR ;
- **data breach**: violazione di sicurezza che comporta distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali.

Art. 5 – Principi del trattamento

Ogni trattamento deve rispettare i principi di:

- liceità, correttezza e trasparenza;
- limitazione della finalità;
- minimizzazione dei dati;
- esattezza;
- limitazione della conservazione;
- integrità e riservatezza;
- responsabilizzazione del titolare.

L'Istituto applica inoltre i principi di **protezione dei dati fin dalla progettazione** e **per impostazione predefinita**, adottando misure tecniche e organizzative adeguate al rischio e trattando solo i dati necessari per ogni specifica finalità.

Art. 6 – Ruoli privacy e responsabilità interne

6.1 Titolare del trattamento

Il Titolare del trattamento è l'Istituto scolastico, legalmente rappresentato dal Dirigente scolastico, che adotta o approva le decisioni organizzative necessarie e garantisce l'adozione delle misure di accountability.

6.2 Responsabile della Protezione dei Dati (RPD/DPO)

L'Istituto designa un RPD/DPO ai sensi degli artt. 37-39 GDPR. I dati di contatto del RPD/DPO sono pubblicati sul sito istituzionale e comunicati al Garante secondo le modalità previste .

6.3 Persone autorizzate al trattamento

Il personale docente, educativo, amministrativo e ATA tratta i dati esclusivamente nei limiti delle proprie funzioni, secondo istruzioni documentate e nel rispetto del principio di necessità.

6.4 Responsabili esterni

I fornitori di servizi informatici, registro elettronico, piattaforme cloud, conservazione digitale, assistenza tecnica e altri soggetti che trattano dati per conto della scuola sono designati, quando ne ricorrono i presupposti, responsabili del trattamento ai sensi dell'art. 28 GDPR.

Art. 7 – Basi giuridiche, finalità e consenso

1. I trattamenti necessari alle funzioni istituzionali della scuola sono effettuati, di regola, ai sensi dell'art. 6, par. 1, lett. c) ed e) GDPR e dell'art. 2-ter del Codice privacy.
2. Per le categorie particolari di dati si applicano l'art. 9 GDPR e le specifiche norme nazionali di settore.
3. Il consenso non costituisce la base giuridica generale dei trattamenti istituzionali obbligatori o necessari. Può essere richiesto solo per attività realmente facoltative, ulteriori e chiaramente distinte, quando ricorrano i presupposti di libertà, specificità, informazione, inequivocabilità e revocabilità.
4. Per i servizi della società dell'informazione offerti direttamente ai minori si applicano, quando pertinenti, le regole specifiche del GDPR e della normativa nazionale.

Art. 8 – Tipologie di dati trattati

Nel rispetto del principio di minimizzazione, l'Istituto può trattare:

- dati anagrafici, di contatto, iscrizione, frequenza, profitto e percorso scolastico;
- dati relativi ai rapporti scuola-famiglia, deleghe, autorizzazioni e comunicazioni;
- dati del personale relativi al rapporto di lavoro, stato giuridico, trattamento economico, presenze, formazione e incarichi;

- dati degli organi collegiali necessari a convocazioni, elezioni, verbalizzazioni e deliberazioni;
- dati di fornitori ed esterni necessari a contratti, acquisti, pagamenti, progetti e convenzioni;
- dati tecnici e di utilizzo dei servizi digitali nei limiti necessari alla sicurezza, all'autenticazione e alla continuità operativa.

Art. 9 – Categorie particolari di dati e dati relativi a reati

1. I dati rientranti nell'art. 9 GDPR sono trattati solo quando necessari e sulla base di una specifica previsione normativa o di altro idoneo presupposto di liceità
2. L'accesso a tali dati è limitato ai soli soggetti che ne abbiano effettiva necessità in ragione del proprio ruolo.
3. I dati relativi a condanne penali e reati sono trattati esclusivamente nei casi ammessi dall'art. 10 GDPR e dalla normativa nazionale applicabile.

Art. 10 – Informative e trasparenza verso gli interessati

L'Istituto rende agli interessati informative chiare, accessibili e aggiornate ai sensi degli artt. 12, 13 e 14 GDPR, indicando almeno:

- identità e contatti del Titolare;
- contatti del RPD/DPO;
- finalità e basi giuridiche del trattamento;
- categorie di destinatari;
- eventuali trasferimenti extra SEE;
- tempi o criteri di conservazione;
- diritti esercitabili e modalità di reclamo-

Le informative rivolte ai minori devono essere formulate con linguaggio semplice e comprensibile.

Art. 11 – Comunicazione, diffusione, pubblicazione e Amministrazione Trasparente

1. La comunicazione di dati a soggetti determinati e la diffusione a soggetti indeterminati costituiscono operazioni distinte e richiedono un autonomo presupposto di liceità.
2. La pubblicazione nella sezione "Amministrazione Trasparente" avviene esclusivamente nei casi previsti dalla legge, nel rispetto dei principi di pertinenza, minimizzazione, esattezza, durata della pubblicazione e tutela della riservatezza

3. Non devono essere pubblicati dati ulteriori rispetto a quelli strettamente necessari all'adempimento dell'obbligo normativo.
4. Gli esiti di scrutini ed esami sono resi conoscibili secondo la disciplina scolastica vigente, evitando l'inserimento di dati sulla salute, disabilità, DSA o altre informazioni non pertinenti.

Art. 12 – Registro elettronico, piattaforme, cloud, posta elettronica e strumenti digitali

L'utilizzo di registro elettronico, piattaforme didattiche, servizi cloud, sistemi di videoconferenza, archiviazione digitale e posta elettronica istituzionale è consentito solo se approvato dall'Istituto e configurato secondo i principi di minimizzazione e sicurezza

In particolare:

- devono essere attivate solo le funzionalità necessarie alle finalità istituzionali;
- gli account istituzionali non devono essere condivisi;
- le autorizzazioni devono essere profilate per ruolo e riesaminate periodicamente;
- l'uso di account personali per trattare dati scolastici deve essere evitato, salvo casi eccezionali formalmente autorizzati;
- i documenti contenenti categorie particolari di dati non devono essere inseriti in servizi non autorizzati;
- prima di attivare nuovi servizi devono essere valutati ruoli privacy del fornitore, misure di sicurezza, sub-responsabili, localizzazione dei dati ed eventuali trasferimenti internazionali.

Art. 13 – Intelligenza artificiale e sistemi automatizzati

1. L'uso di strumenti di intelligenza artificiale deve essere coerente con finalità istituzionali, protezione dei dati, sicurezza delle informazioni, non discriminazione, inclusione e supervisione umana.
2. Non devono essere inseriti in servizi di IA non autorizzati dati identificativi di studenti o personale, categorie particolari di dati, credenziali, fascicoli, PEI, PDP, informazioni disciplinari o altri contenuti riservati,
3. Prima dell'adozione istituzionale di sistemi di IA, l'Istituto verifica almeno: ruolo del fornitore, basi giuridiche, finalità, dati trattati, conservazione, uso per addestramento, trasferimenti internazionali, misure di sicurezza, diritti degli interessati e necessità di DPIA.

4. Qualora il sistema rientri tra quelli ad alto rischio ai sensi del Regolamento (UE) 2024/1689, l'Istituto applica gli obblighi previsti e garantisce adeguata supervisione umana.
5. L'Istituto promuove una adeguata alfabetizzazione del personale in materia di IA.

Art. 14 – Immagini, audio, video, sito web e social network

1. La ripresa e l'utilizzo di immagini, audio e video costituiscono trattamento di dati personali quando le persone siano identificate o identificabili.
2. La documentazione di attività scolastiche non comporta automaticamente la liceità della successiva pubblicazione online. La diffusione sul sito istituzionale o sui social network costituisce trattamento ulteriore e va valutata separatamente.
3. L'Istituto privilegia immagini non identificative, riprese di contesto, elaborati o soluzioni che riducano l'esposizione dei minori.
4. Quando il consenso rappresenti la base giuridica appropriata per attività facoltative, esso deve essere specifico, distinto per finalità e revocabile.
5. L'eventuale affidamento a fotografi, videomaker o altri soggetti esterni richiede la preventiva definizione dei ruoli privacy e, ove necessario, la designazione a responsabile del trattamento.

Art. 15 – Dispositivi personali, chat, fotografie e registrazioni effettuate da privati

1. L'uso di smartphone e dispositivi personali è disciplinato dal Regolamento d'Istituto e dalle disposizioni vigenti.
2. Foto e video effettuati da genitori o familiari durante eventi scolastici, se destinati esclusivamente all'ambito personale o familiare, restano sotto la responsabilità di chi li realizza; la successiva diffusione tramite social, siti o chat deve rispettare i diritti delle persone ritratte.
3. Chat di classe e gruppi non istituzionali non costituiscono canali ufficiali della scuola, salvo espressa adozione da parte dell'Istituto. È vietato al personale diffondere tramite tali canali dati riservati o documenti contenenti informazioni non necessarie.

Art. 16 – Diritti degli interessati e accesso agli atti

Gli interessati possono esercitare, quando applicabili, i diritti di cui agli artt. 15-22 GDPR, inclusi accesso, rettifica, cancellazione, limitazione, opposizione e i diritti relativi a decisioni automatizzate.

Tali diritti possono subire limitazioni nei casi previsti dalla legge quando il trattamento sia necessario per obblighi legali o compiti di interesse pubblico.
Il diritto di accesso ai dati personali ai sensi del GDPR è distinto:

- dall'accesso documentale ex Legge n. 241/1990;
- dall'accesso civico semplice o generalizzato ex D.lgs. n. 33/2013.

Art. 17 – Sicurezza, credenziali, documenti e gestione degli incidenti

L'Istituto e i soggetti autorizzati adottano misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, tenendo conto della natura, del contesto e delle finalità del trattamento.
In particolare, occorre:

- utilizzare password robuste e, ove disponibile, autenticazione a più fattori;
- non condividere credenziali;
- bloccare la postazione quando ci si allontana;
- evitare l'uso di supporti non controllati per dati scolastici riservati;
- verificare attentamente i destinatari prima dell'invio di e-mail;
- utilizzare il campo Ccn/Bcc nelle comunicazioni collettive quando opportuno;
- non lasciare documenti riservati in luoghi accessibili;
- conservare fascicoli e documenti secondo le regole di sicurezza e archivistiche;
- segnalare immediatamente smarrimenti, invii errati, accessi anomali, malware o altre possibili violazioni.

Art. 18 – Data breach

1. Chiunque rilevi o sospetti una violazione di dati personali deve segnalarla senza ritardo al Dirigente scolastico e ai referenti interni individuati dalla procedura, fornendo le informazioni disponibili.
2. Il Titolare valuta la violazione con il supporto del RPD/DPO, documenta l'evento e, se la violazione può presentare un rischio per i diritti e le libertà delle persone fisiche, provvede alla notifica al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore.
3. Se il rischio è elevato, l'Istituto provvede anche alla comunicazione agli interessati, nei casi e con le modalità previsti dal GDPR.

Art. 19 – Valutazione d'impatto e privacy by design/by default

Prima di introdurre trattamenti che possano presentare un rischio elevato per i diritti e le libertà delle persone, in particolare se basati su nuove tecnologie, monitoraggio sistematico, trattamenti su larga scala o sistemi di IA, l'Istituto verifica la necessità di effettuare una valutazione d'impatto sulla protezione dei dati (DPIA).

Le scelte organizzative e tecnologiche devono garantire, fin dalla progettazione e per impostazione predefinita, il trattamento del minor numero di dati necessario rispetto alla finalità perseguita.

Art. 20 – Responsabili esterni, fornitori e trasferimenti di dati

Prima di affidare servizi che comportino trattamento di dati personali, l'Istituto verifica che il fornitore presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate e stipula, ove necessario, un contratto o altro atto giuridico ai sensi dell'art. 28 GDPR.

La verifica riguarda almeno:

- oggetto, durata, natura e finalità del trattamento;
- categorie di dati e di interessati;
- misure di sicurezza;
- eventuali sub-responsabili;
- assistenza nell'esercizio dei diritti;
- supporto nella gestione dei data breach;
- tempi di conservazione;
- eventuali trasferimenti verso Paesi terzi o organizzazioni internazionali.

I trasferimenti extra SEE sono ammessi solo nel rispetto del Capo V GDPR.

Art. 21 – Conservazione, archiviazione e cancellazione

I dati personali sono conservati per il tempo previsto dalla normativa scolastica, amministrativa, contabile, archivistica e lavoristica oppure, in mancanza di un termine specifico, per il periodo necessario al perseguimento della finalità.

L'Istituto adotta criteri di conservazione documentati e provvede, quando dovuto, alla cancellazione, anonimizzazione o archiviazione secondo la disciplina applicabile.

La cancellazione non è effettuata quando la conservazione sia imposta dalla legge o necessaria per finalità di archivio istituzionale o difesa di un diritto.

Art. 22 – Obblighi del personale e regole di comportamento

Il personale è tenuto a:

- trattare i dati esclusivamente per finalità di servizio;
- mantenere la riservatezza anche dopo la cessazione del rapporto;
- non utilizzare dati scolastici per finalità personali o estranee al servizio;
- non pubblicare su profili personali contenuti riferibili ad alunni, famiglie o colleghi acquisiti per ragioni di servizio;
- non comunicare a terzi, informazioni su salute, profitto, comportamento o situazione familiare senza idoneo presupposto;
- attenersi alle istruzioni dell'Istituto e alle indicazioni del RPD/DPO.

La violazione delle presenti regole può comportare responsabilità disciplinare, amministrativa, civile o penale secondo la normativa applicabile.

Art. 23 – Reclami, segnalazioni e rapporti con il RPD/DPO

Gli interessati possono rivolgersi al Titolare o al RPD/DPO per quesiti e richieste in materia di protezione dei dati personali. È fatto salvo il diritto di proporre reclamo al Garante ai sensi dell'art. 77 GDPR.

I dati di contatto del Titolare e del RPD/DPO devono essere mantenuti aggiornati sul sito istituzionale.

Art. 24 – Approvazione, pubblicazione e aggiornamento

1. Il presente Regolamento è approvato dal Consiglio d'Istituto secondo le competenze previste dall'ordinamento scolastico.
2. Il documento è pubblicato sul sito istituzionale nella sezione dedicata al Regolamento d'Istituto e/o alla privacy.
3. Il Regolamento è soggetto a revisione periodica e ogniqualvolta intervengano modifiche normative, provvedimenti del Garante, nuovi trattamenti o significativi cambiamenti tecnologici e organizzativi.

ALLEGATO A – Matrice sintetica dei principali trattamenti

Ambito	Dati principali	Finalità	Base giuridica prevalente	Cautele
Iscrizione e carriera scolastica	Anagrafici, contatti, frequenza, profitto	Gestione del percorso scolastico	Obbligo legale / compito di interesse pubblico	Minimizzazione, accessi profilati, informative
Inclusione e salute	Dati sulla salute, disabilità, DSA, esigenze specifiche	Inclusione, sicurezza, diritto allo studio	Art. 9 GDPR + norme di settore	Accesso strettamente necessario, canali sicuri
Rapporto di lavoro	Dati anagrafici, giuridici, economici, presenze	Gestione del personale	Obblighi legali / pubblico interesse	Riservatezza, separazione funzionale
Organi collegiali	Anagrafici, cariche, verbali	Funzionamento degli organi	Obbligo legale / compito pubblico	Verbali pertinenti, limitazione diffusione
Fornitori e contratti	Anagrafici, fiscali, bancari	Acquisti, contratti, pagamenti	Obbligo legale / contratto	Verifica destinatari, pubblicazioni obbligatorie
Registro e piattaforme digitali	Account, dati didattici, log necessari	Didattica e amministrazione digitale	Compito pubblico / obbligo legale	Sicurezza, servizi minimi, art. 28 ove necessario
Immagini e video	Immagini, voce, contenuti multimediali	Documentazione o ulteriori attività	Da verificare per singola finalità	Diffusione online separata, tutela minori
IA	Prompt, contenuti, eventuali dati trattati	Supporto didattico/amministrativo autorizzato	Da verificare per ciascun uso	No dati riservati su servizi non autorizzati, DPIA se necessaria

La matrice ha carattere orientativo e deve essere coordinata con il Registro delle attività di trattamento e con le informative specifiche.

ALLEGATO B – Procedura interna essenziale in caso di data breach

Fase	Azione
1. Rilevazione	Chiunque rilevi perdita, invio errato, accesso abusivo, malware, furto di dispositivo o pubblicazione indebita avvisa immediatamente i referenti interni.
2. Contenimento	Si adottano le misure immediate necessarie a limitare la violazione senza compromettere le evidenze utili.
3. Raccolta informazioni	Vanno raccolti data/ora, sistemi coinvolti, categorie di dati, numero approssimativo di interessati, conseguenze e misure già adottate.
4. Valutazione	Il Titolare, con il supporto del RPD/DPO, valuta natura, probabilità e gravità del rischio.
5. Notifica al Garante	Se sussiste un rischio, si notifica senza ingiustificato ritardo e, ove possibile, entro 72 ore.
6. Comunicazione agli interessati	Se il rischio è elevato, si comunica agli interessati in modo chiaro, salvo ricorrano i casi di esenzione.
7. Documentazione e miglioramento	L'evento, le decisioni e le misure correttive devono essere registrati e utilizzati per il miglioramento organizzativo.

Clausola finale

Per quanto non espressamente disciplinato dal presente Regolamento, si applicano il GDPR, il Codice privacy, la normativa scolastica e amministrativa vigente, nonché i provvedimenti e le indicazioni dell'Autorità Garante per la protezione dei dati personali.

Il Dirigente Scolastico

Vittorio RUBERTO

Il presente documento è stato approvato, come da delibere riportate di seguito:

Collegio docenti:

Regolamenti allegati al PTOF - delibera n. 21 del verbale del 29/10/2026 prot. 5731 del 04/11/2026.

Consiglio di Istituto:

Regolamenti allegati al PTOF - delibera n. 29 del verbale n. 5 del 29/10/2026 prot. 5889 del 11/11/2026.