Ministero dell'Istruzione e del Merito
ISTITUTO COMPRENSIVO DI OME
Scuola dell'Infanzia Statale di BRIONE – POLAVENO
Scuola Primaria Statale di BRIONE - MONTICELLI BRUSATI - OME – POLAVENO
Scuola Secondaria 1° gr. Statale di MONTICELLI BRUSATI - OME – POLAVENO
Via Valle, 7 - 25050 OME (BS) – BSIC81100Q@istruzione.it – tel. 030-652121 – fax 030-68528

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI
DEL PERSONALE SCOLASTICO (DOCENTI E PERSONALE ATA)
(ai sensi degli artt. 13 e 14 del Regolamento UE 2016/679 - GDPR)

1. Titolare del Trattamento e Responsabile della Protezione dei Dati (DPO)

- **Titolare del trattamento**: Istituto comprensivo di Ome, con sede in OME C.F. 80048360178 nella persona della Dirigente Scolastica *pro tempore* Elisabetta Zani.
  Contatti: e-mail bsic81100q@istruzione.it| PEC bsic81100q@pec.istruzione.it | Tel. 030/652121

- **Responsabile della Protezione dei Dati (RPD/DPO)**: Gianfausto Vincenzi, contattabile all'indirizzo e-mail / PEC: rpd@vincenzi.com / g.vincenzi@legalmail.it

2. Categorie di Dati Personali Trattati

L'Istituzione Scolastica tratta i seguenti dati del personale docente, educativo e ATA:

1. **Dati anagrafici, identificativi e di contatto**: nome, cognome, codice fiscale, residenza, recapiti telefonici, e-mail istituzionale e personale, estremi dei documenti di identità, fotografia (per tesserino/badge di servizio).
2. **Dati di carriera, economici e previdenziali**: titoli di studio e professionali, stato di servizio, curriculum vitae, coordinate bancarie (IBAN), dati previdenziali, presenze/assenze, orari di servizio, provvedimenti amministrativi e disciplinari.
3. **Categorie particolari di dati (art. 9 GDPR)**:
   - *Dati relativi allo stato di salute*: certificati medici, idoneità alla mansione, visite fiscali, documentazione L. 104/1992, infortuni sul lavoro, permessi per malattia/congedi speciali;
   - *Dati di appartenenza sindacale*: trattenute sindacali, permessi per attività sindacali;
   - *Dati giudiziari (art. 10 GDPR)*: casellario giudiziale e carichi pendenti (es. certificato antipedofilia ex D.Lgs. 39/2014), procedimenti penali in corso.

3. Finalità e Basi Giuridiche del Trattamento

Il trattamento dei dati personali del dipendente è effettuato dall'Istituzione Scolastica per il perseguimento delle seguenti **finalità specifiche**:

A. Gestione del rapporto di lavoro e adempimenti amministrativo-contabili

Firmato digitalmente da ZANI ELISABETTA

1. **Instaurazione, gestione ed estinzione del rapporto di lavoro**: gestione delle graduatorie, stipula e registrazione dei contratti individuali, tenuta ed evoluzione del fascicolo personale, ricostruzioni di carriera, trasferimenti, comandi, mobilità e cessazioni dal servizio.

2. **Trattamento economico, fiscale, previdenziale e assistenziale**: liquidazione delle competenze fisse e accessorie (compensi per attività aggiuntive, MOF, straordinari), trasmissione flussi a NoiPA, adempimenti fiscali (es. CU, modello 770) e previdenziali/assistenziali verso INPS e altri enti preposti.

3. **Gestione delle assenze e del personale supplente**: ricezione e registrazione delle richieste di ferie, permessi, congedi straordinari o parentali, gestione delle supplenze brevi e saltuarie e relative comunicazioni agli organi competenti.

4. **Adempimenti in materia di salute e sicurezza sul lavoro (D.Lgs. 81/2008)**: sorveglianza sanitaria, visite del medico competente per l'accertamento dell'idoneità alla mansione, denunce di infortunio sul lavoro (INAIL) e nomina delle figure di prevenzione/emergenza.

B. Organizzazione dei servizi, rilevazione presenze e riconoscimento

5. **Rilevazione delle presenze e dell'orario di lavoro**: gestione delle timbrature (tramite lettori di badge o sistemi digitali interni) e compilazione dei fogli di presenza, al solo scopo della verifica del rispetto dell'orario di servizio e del calcolo delle indennità/compensi spettanti, escludendo qualunque forma di controllo a distanza non consentita dalla legge.

6. **Utilizzo del cartellino/badge identificativo**: esposizione e uso del tesserino/cartellino di riconoscimento durante il servizio, finalizzato a garantire l'identificabilità del personale operante all'interno dei locali scolastici nei confronti di studenti, famiglie e terzi (in conformità all'art. 55-novies del D.Lgs. 165/2001 e alle disposizioni datoriali/ordini di servizio).

C. Gestione delle attività didattiche, collegiali ed extra-didattiche

7. **Organizzazione e coordinamento delle attività didattiche**: predisposizione dell'orario settimanale delle lezioni, calendarizzazione delle attività collegiali (Consigli di Classe, Collegio Docenti, colloqui con le famiglie), verbalizzazione delle sedute e pianificazione delle supplenze interne.

8. **Gestione delle attività extra-didattiche, uscite didattiche e viaggi di istruzione**: designazione e gestione degli elenchi dei docenti/personale accompagnatore, organizzazione della logistica (biglietteria, alberghi, trasporti), rilascio degli incarichi e comunicazioni funzionali con le agenzie di viaggio o le strutture ospitanti.

D. Gestione degli strumenti di lavoro, piattaforme web e infrastrutture digitali

9. **Assegnazione e gestione degli account istituzionali**: erogazione delle credenziali per l'accesso alla rete scolastica, alla casella di posta elettronica istituzionale (@dominio.edu.it), alla suite di produttività (es. Google Workspace for Education / Microsoft 365) e ai servizi cloud ad uso scolastico.

10. **Utilizzo del Registro Elettronico e dei gestionali web-based**: accesso e compilazione del registro di classe e del professore (firme, voti, note, assenze), trasmissione di circolari e comunicazioni interne, adozione di piattaforme per la gestione documentale e la dematerializzazione della segreteria.

11. **Sicurezza informatica e continuità dei sistemi**: tenuta dei log di accesso e di sistema, gestione dei profili di autorizzazione e protezione dell'infrastruttura IT scolastica da accessi non autorizzati o minacce informatiche.

Basi Giuridiche di Riferimento

I trattamenti sopra elencati trovano legittimazione nelle seguenti basi giuridiche (ai sensi degli artt. 6, 9 e 10 del GDPR):

- **Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri** (*art. 6, par. 1, lett. e, GDPR*), con specifico riferimento al D.Lgs. 297/1994 (Testo Unico Scuola), alla L. 107/2015, al D.P.R. 275/1999 e alle norme sull'autonomia scolastica;
- **Adempimento di un obbligo legale al quale è soggetto il Titolare** (*art. 6, par. 1, lett. c, GDPR*), in conformità al D.Lgs. 165/2001 (es. art. 55-novies per il cartellino identificativo), al D.Lgs. 81/2008 (sicurezza sul lavoro), alle norme fiscali, tributarie e ai Contratti Collettivi Nazionali di Lavoro (CCNL Comparto Istruzione e Ricerca);
- **Esecuzione del contratto di lavoro** (*art. 6, par. 1, lett. b, GDPR*) e adozione delle relative misure organizzative e operative interne;
- **Gestione degli obblighi in materia di diritto del lavoro, sicurezza e protezione sociale** (*art. 9, par. 2, lett. b, GDPR*), per il trattamento di dati particolari (es. assenze per malattia, congedi ex L. 104/1992, adesioni a trattenute sindacali);
- **Sorveglianza sanitaria e medicina del lavoro** (*art. 9, par. 2, lett. h, GDPR*), per i dati gestiti nell'ambito dei compiti del Medico Competente;
- **Adempimenti e verifiche previsti dalla legge sui precedenti penali** (*art. 10 GDPR*), in particolare per l'acquisizione del casellario giudiziale e del certificato antipedofilia ex D.Lgs. 39/2014.

(per le finalità istituzionali e connesse al rapporto di pubblico impiego non è richiesto il consenso dell'interessato).

4. Utilizzo di Sistemi e Strumenti di Intelligenza Artificiale (IA)

Nell'ambito della digitalizzazione e dell'efficientamento dei processi amministrativi, l'Istituzione Scolastica può avvalersi di applicativi e piattaforme dotate di funzionalità di **Intelligenza Artificiale (IA)** (es. elaborazione del linguaggio naturale, categorizzazione documentale, supporto alla redazione di atti, sintesi e trascrizione, gestione del protocollo e dei flussi di segreteria).
In merito a tali trattamenti, si forniscono le seguenti garanzie:

1. **Supporto operativo e non decisorio (*Human-in-the-loop*)**: I sistemi di IA fungono esclusivamente da supporto materiale e operativo alle attività della segreteria e della dirigenza. **È escluso qualsiasi processo decisionale basato unicamente sul trattamento automatizzato (art. 22 GDPR)**; ogni atto, provvedimento o comunicazione finale rimane sottoposto alla verifica, valutazione e firma del personale umano autorizzato.
2. **Divieto di controllo a distanza e valutazione delle prestazioni**: Gli strumenti di IA non sono in alcun modo impiegati per la profilazione, il monitoraggio o la valutazione delle prestazioni lavorative, del rendimento o del comportamento del dipendente, in piena conformità con l'art. 4 della Legge n. 300/1970 (Statuto dei Lavoratori) e l'art. 114 del D.Lgs. 196/2003.
3. **Protezione dei dati e divieto di addestramento modelli**: I dati personali e i documenti inseriti

negli applicativi di IA istituzionali vengono trattati all'interno di ambienti protetti e contrattualmente vincolati (accordi ex art. 28 GDPR). **I dati del personale non vengono utilizzati dai fornitori tecnologici per l'addestramento o il miglioramento di modelli linguistici generali/LLM di terzi.**

4. **Minimizzazione e riservatezza**: L'immissione di documenti nei flussi assistiti da IA avviene previa adozione di misure di minimizzazione o pseudonimizzazione, escludendo l'inserimento non necessario di categorie particolari di dati (dati sanitari, giudiziari o sindacali).
5. **Valutazione d'impatto (DPIA / FRIA)**: L'adozione di soluzioni di IA è preceduta da un'analisi dei rischi per i diritti e le libertà fondamentali degli interessati e dall'adozione di apposite policy interne di utilizzo.

5. Modalità del Trattamento e Misure di Sicurezza

Il trattamento dei dati personali del dipendente è improntato ai principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, integrità e riservatezza (art. 5 del GDPR).

I trattamenti sono effettuati mediante:

- Supporti cartacei: fascicoli, registri e documenti fisici custoditi in locali, uffici o armadi dotati di serratura e ad accesso controllato, accessibili esclusivamente al personale formalmente autorizzato;
- Strumenti informatici e telematici: postazioni di lavoro, piattaforme gestionali scolastiche, registri digitali, sistemi di posta elettronica istituzionale e ambienti di collaborazione/archiviazione (sia su infrastrutture locali sia su servizi cloud qualificati per la Pubblica Amministrazione).

Misure Tecniche e Organizzative di Sicurezza (art. 32 GDPR)

L'Istituzione Scolastica adotta adeguate misure tecniche e organizzative per garantire un livello di sicurezza commisurato ai rischi di distruzione, perdita, modifica, accesso non autorizzato o divulgazione accidentale o illecita dei dati, tra cui:

1. Gestione degli accessi e autenticazione:
    - Attribuzione di profili di autorizzazione differenziati e limitati alle sole funzioni strettamente necessarie alle mansioni assegnate (*principio del privilegio minimo*);
    - Accesso ai sistemi informatici e alle piattaforme mediante credenziali individuali, con obbligo di custodia diligente, policy di complessità delle password e, ove supportata, autenticazione a più fattori (MFA) o identità digitale (SPID/CIE);
2. Protezione dei canali e dei dati:
    - Adozione di protocolli di cifratura e connessioni protette per la trasmissione dei dati e l'accesso agli applicativi web;
    - Segmentazione logica dei dati e applicazione di misure di pseudonimizzazione o minimizzazione ove opportuno;
3. Resilienza, continuità operativa e tracciamento:

- Procedure periodiche di backup dei dati e piani di ripristino per garantire la disponibilità delle informazioni in caso di incidenti tecnici o fisici;
- Registrazione e monitoraggio dei log di accesso e delle operazioni di sistema a fini di sicurezza informatica e contrasto agli accessi non autorizzati;
- Impiego e aggiornamento costante di sistemi di protezione perimetrale e antivirus/antimalware;

4. Istruzione del personale e governance interna:
   - Formazione e aggiornamento continuo del personale autorizzato in materia di protezione dei dati, corretta gestione dei documenti e sicurezza informatica;
   - Formalizzazione di atti di autorizzazione/istruzioni operative interne per il personale docente e ATA e stipula di accordi vincolanti sul trattamento dei dati (ex art. 28 GDPR) con tutti i fornitori esterni di servizi digitali.

Tutti i trattamenti automatizzati o assistiti da applicativi digitali rispettano i principi di *privacy by design* e *privacy by default* (art. 25 GDPR).

6. Destinatari e Categorie di Destinatari dei Dati Personali

I dati personali non saranno diffusi o comunicati a soggetti terzi indeterminati, ma potranno essere trasmessi esclusivamente a soggetti determinati per le sole finalità istituzionali, amministrative, organizzative e contrattuali sopra indicate, nel rispetto dei principi di necessità e proporzionalità.

I destinatari appartengono alle seguenti categorie:

A. Enti, Istituzioni e Autorità Pubbliche (Titolari autonomi del trattamento)

La comunicazione a tali soggetti avviene in adempimento di precisi obblighi normativi, regolamentari o di cooperazione istituzionale:

1. Ministero dell'Istruzione e del Merito (MIM), Uffici Scolastici Regionali (USR) e Uffici di Ambito Territoriale (USP), per la gestione delle carriere, graduatorie, mobilità, organici e flussi informativi tramite il portale SIDI;
2. Ministero dell'Economia e delle Finanze (MEF) – Portale NoiPA, per la gestione stipendiale, le liquidazioni delle competenze accessorie e i relativi conguagli fiscali/previdenziali;
3. Enti previdenziali, assistenziali e assicurativi (INPS, INAIL), per la gestione delle posizioni contributive, pensionistiche, delle domande di congedo/permesso e per le denunce obbligatorie di infortunio sul lavoro o malattia professionale;
4. Amministrazione Finanziaria e Agenzia delle Entrate, per gli adempimenti fiscali di sostituto d'imposta (es. CU, Modello 770);
5. Aziende Sanitarie Locali (ASST/ATS) e Strutture Sanitarie Pubbliche, per gli adempimenti in materia di tutela della salute e le verifiche d'ufficio sulle certificazioni mediche;
6. Autorità Giudiziaria, Organi di Polizia Giudiziaria e Forze dell'Ordine, per la verifica dei carichi pendenti/casellario (es. certificato antipedofilia ex D.Lgs. 39/2014) o a seguito di formale richiesta nell'ambito di indagini;

7. Avvocatura dello Stato, Ufficio per i Procedimenti Disciplinari (UPD) e Organi di Giustizia Amministrativa/Ordinaria, in caso di procedimenti disciplinari o contenziosi legali;

8. Organizzazioni Sindacali e Rappresentanze Sindacali Unitarie (RSU), limitatamente ai dati aggregati o strettamente necessari per l'informativa preventiva e consuntiva sulle materie previste dalla contrattazione collettiva nazionale (CCNL), escludendo comunque la trasmissione di dati relativi alla salute o all'adesione sindacale individuale.

B. Soggetti Privati e Fornitori di Servizi Esterni (Responsabili del Trattamento ex art. 28 GDPR)

I dati possono essere trattati da società e professionisti esterni formalmente designati dall'Istituzione Scolastica quali Responsabili del Trattamento ai sensi dell'art. 28 del GDPR, vincolati al rispetto di rigorose istruzioni operative e misure di sicurezza:

1. Fornitori di software gestionali e applicativi per la scuola: società che gestiscono il Registro Elettronico, i pacchetti per la segreteria digitale, il protocollo informatico, la gestione documentale e la conservazione a norma;

2. Provider di servizi Cloud e piattaforme di produttività didattica/amministrativa (es. Google Workspace for Education, Microsoft 365, infrastrutture cloud certificate ACN/AgID);

3. Fornitori e gestori di sistemi e applicativi basati su Intelligenza Artificiale integrati nei flussi operativi di segreteria e documentali (con clausole vincolanti che inibiscono l'uso dei dati scolastici per l'addestramento dei modelli);

4. Istituto Bancario / Tesoreria Scolastica, per l'accredito dei pagamenti relativi a compensi accessori, rimborsi spese o missioni;

5. Medico Competente e società di sorveglianza sanitaria, per la programmazione e lo svolgimento delle visite mediche periodiche e preventive ex D.Lgs. 81/2008 (**il Medico opera per le cartelle sanitarie come autonomo titolare**, mentre il fornitore del servizio organizzativo/logistico opera quale responsabile);

6. Società di manutenzione e assistenza informatica / Amministratori di sistema esterni, per la gestione, sicurezza e continuità operativa dell'infrastruttura hardware e di rete dell'Istituto;

7. Agenzie di viaggio, strutture ricettive, vettori di trasporto e guide turistiche, limitatamente ai soli dati anagrafici e di contatto del personale docente e ATA formalmente incaricato dell'accompagnamento e vigilanza degli studenti durante uscite didattiche, visite e viaggi di istruzione.

C. Soggetti Autorizzati al Trattamento (Interni all'Istituzione Scolastica)

I dati personali sono trattati esclusivamente da personale dipendente dell'Istituto (personale di segreteria, collaboratori del Dirigente, figure di sistema, DSGA) formalmente autorizzato e istruito al trattamento ai sensi dell'art. 29 del GDPR e dell'art. 2-quaterdecies del D.Lgs. 196/2003, ciascuno nell'ambito delle mansioni e dei profili di autorizzazione assegnati.

D. Diffusione dei Dati Personali

I dati personali del personale non sono soggetti a diffusione indiscriminata.

La pubblicazione di dati sul sito web istituzionale dell'Istituto (es. sezione *"Amministrazione Trasparente"* o Albo Online) è limitata esclusivamente alle informazioni la cui pubblicità sia

espressamente imposta dalla legge (es. D.Lgs. 33/2013, compensi per incarichi conferiti, curriculum vitae dei titolari di posizioni organizzative, provvedimenti conclusivi), procedendo all'oscuramento (*omissis*) di dati personali non pertinenti, recapiti privati, dati particolari o riferimenti bancari.

7. Trasferimento dei Dati Extra-UE

I dati sono conservati su server ubicati all'interno dell'Unione Europea. Qualora l'utilizzo di specifici servizi digitali (es. suite cloud o strumenti di produttività) comporti il transito di dati verso Paesi extra-SEE, tale trasferimento avviene esclusivamente verso Paesi destinatari di decisioni di adeguatezza della Commissione Europea oppure sulla base di Clausole Contrattuali Standard (SCC) con idonee misure tecniche supplementari.

8. Periodo di Conservazione dei Dati

I dati personali sono conservati per il tempo strettamente necessario al conseguimento delle finalità per cui vengono trattati, in conformità agli obblighi di legge sul pubblico impiego e alle disposizioni per la conservazione e lo scarto degli archivi delle Istituzioni Scolastiche:

- Fascicolo personale e stato matricolare: sono conservati illimitatamente all'interno dell'archivio storico dell'Istituzione Scolastica, costituendo documentazione essenziale per la ricostruzione della carriera, i diritti pensionistici e la memoria amministrativa;
- Documenti contabili, fiscali e contrattuali: sono conservati per 10 anni dalla chiusura del relativo esercizio finanziario o dalla cessazione dell'efficacia dell'atto, fatti salvi eventuali contenziosi o prescrizioni interruttive;
- Certificazioni sanitarie, assenze e pratiche temporanee: sono conservate per il periodo strettamente necessario alla definizione del procedimento amministrativo e previdenziale di competenza, dopodiché vengono eliminate o trasmesse agli enti competenti;
- Dati e documenti elaborati tramite strumenti di IA e gestionali di segreteria: seguono i medesimi tempi di conservazione previsti per i procedimenti amministrativi a cui afferiscono. Le memorie temporanee di elaborazione (*cache/prompt log*) degli strumenti digitali vengono cancellate periodicamente secondo le policy di sicurezza adottate;
- Log di accesso ai sistemi e alle piattaforme digitali: sono conservati per un periodo non superiore a quello prescritto dalle linee guida di sicurezza (di norma 6-12 mesi), salvo specifiche esigenze di indagine da parte dell'Autorità Giudiziaria.

Decorsi i termini di conservazione previsti dalla normativa e dal piano di scarto archivistico, i dati vengono cancellati, distrutti o resi anonimi in modo irreversibile.

9. Diritti dell'Interessato

In qualità di interessato, il dipendente ha diritto di esercitare in qualsiasi momento i diritti previsti dagli articoli 15-22 del GDPR:

- **Accesso** ai propri dati personali e ricezione di copia;
- **Rettifica** o integrazione dei dati inesatti o incompleti;
- **Cancellazione** dei dati (*diritto all'oblio*), nei limiti in cui non sussista un obbligo di legge di conservazione;
- **Limitazione** del trattamento nei casi previsti dall'art. 18 GDPR;
- **Opposizione** al trattamento per motivi legittimi connessi alla propria situazione particolare (art.

21 GDPR);

- **Diritto di non essere sottoposto a decisioni automatizzate** (art. 22 GDPR), inclusa la facoltà di richiedere l'intervento umano per qualsiasi elaborazione assistita da IA.

Le istanze per l'esercizio dei diritti possono essere inoltrate al Dirigente Scolastico (Titolare) o al RPD/DPO ai recapiti indicati al punto 1.

Resta salvo il diritto di proporre reclamo all'Autorità Garante per la Protezione dei Dati Personali (www.garanteprivacy.it) o ricorso dinanzi all'Autorità Giudiziaria.

Documento elaborato con il supporto di Gemini IA
Indirizzato e supervisionato dal DPO

Ome, 8 settembre 2026