FUTURA LA SCUOLA PER L'ITALIA DI DOMANI

Finanziato dall'Unione europea NextGenerationEU — Ministero dell'Istruzione e del Merito — Italiadomani

ISTITUTO D'ISTRUZIONE SUPERIORE "B. RUSSELL"
Liceo Scientifico Liceo delle Scienze Umane e Liceo Classico "Omero"
Via Gatti, 16 - 20162 Milano tel. 02/6430051/52
www.iis-russell.edu.it C.M. MIIS03900T C.F. 80125870156- Codice univoco UFO7CZ
MIIS03900T@istruzione.it - MIIS03900T@pec.istruzione.it

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

Documento redatto ai sensi degli artt. 13 e 14 del Regolamento (UE) 2016/679 (GDPR) e della normativa nazionale ed europea vigente.

1. Quadro normativo di riferimento

Il trattamento dei dati personali presso l'Istituzione scolastica avviene nel rispetto del seguente corpus normativo:

- **Regolamento (UE) 2016/679 (GDPR)**;
- **D.lgs. 196/2003**, come modificato dal **D.lgs. 101/2018**;
- **Linee guida del Garante per la protezione dei dati personali in ambito scolastico** (provvedimento 26 marzo 2020 e aggiornamenti FAQ 2022–2024);
- **Provvedimento Garante 8 aprile 2010** e successivi chiarimenti su **videosorveglianza**;
- **Decisione di adeguatezza della Commissione europea del 10 luglio 2023** (EU-US Data Privacy Framework);
- **Reg. (UE) 2021/915** e **Decisione Commissione UE 2021/914** sulle **Clausole Contrattuali Standard (SCC)** per trasferimenti extra-UE;
- **Reg. (UE) 2022/2555 (Direttiva NIS2)**, recepita in Italia con **Legge 28 giugno 2024, n. 90 (Legge sulla cybersicurezza nazionale)**;
- **Reg. (UE) 2841/2023 (Cybersecurity Act II)**, che rafforza gli obblighi in materia di resilienza e certificazione dei servizi digitali;

- **Reg. (UE) 2022/2065 (Digital Services Act – DSA)** e **Reg. (UE) 2022/1925 (Digital Markets Act – DMA)**, applicabili ai grandi fornitori di servizi digitali (es. Google, Microsoft) utilizzati in ambito scolastico;
- **Linee guida AgID sulla sicurezza ICT e sulla conservazione digitale dei documenti scolastici** (det. n. 371/2021 e aggiornamenti 2023–2024);
- **Piano Triennale per l'Informatica nella PA 2022–2024 (AgID – Dipartimento per la trasformazione digitale)**;
- **Linee guida ENISA 2024–2025 sulla protezione dei minori online e sulla sicurezza delle piattaforme cloud in ambito educativo**;
- **Codice dei contratti pubblici** (D.lgs. 36/2023), per quanto riguarda i rapporti con fornitori ICT.

2. Titolare del trattamento

L'Istituzione scolastica, nella persona del Dirigente Scolastico pro tempore.

- **Sede**: VIA FRANCESCO GATTI, 16
- **Telefono**: 026430051
- **E-mail**: miis03900t@istruzione.it
- **PEC**: miis03900t@pec.istruzione.it

3. Responsabile della Protezione dei Dati (RPD/DPO)

Dott. Gabriele Mencarini – Diemme Informatica S.r.l.

- Sede legale e operativa: Via Enrico Mattei 721/E – 55100 Lucca (LU)
- C.F./P.IVA: 02115770469
- PEC: contabilitadiemme@pec.it
- Email: amministrazione@diemmeinformatica.com – dpo@diemmeinformatica.com
- Tel: 0583 491734 – Cell. 349 5740739

4. Finalità del trattamento

I dati personali degli alunni e delle famiglie sono trattati per:

1. **Gestione iscrizioni e carriera scolastica** (art. 6, par.1, lett. e GDPR);
2. **Esecuzione attività istituzionali** di istruzione, formazione e valutazione (art. 6, par.1, lett. e GDPR);

3. **Servizio Pago in Rete** (art. 6, par.1, lett. c GDPR – obbligo ex D.L. 76/2020 conv. L. 120/2020);
4. **Servizio mensa e servizi accessori** (art. 6, par.1, lett. e GDPR);
5. **Somministrazione/auto-somministrazione farmaci** (previo consenso esplicito: art. 6, par.1, lett. a e art. 9, par.2, lett. a GDPR);
6. **Adempimenti di legge** (obblighi fiscali, amministrativi, contabili, statistici, sanitari);
7. **Documentazione e diffusione di attività scolastiche**:
    - per finalità istituzionali (sito, registro elettronico, Google Workspace for Education), su base di compito di interesse pubblico;
    - per finalità divulgative (giornalini, social istituzionali, album fotografici), solo con consenso;
8. **Trasferimento fascicolo scolastico ad altri istituti** (art. 6, par.1, lett. e GDPR);
9. **Difesa in sede giudiziaria e gestione del contenzioso** (art. 6, par.1, lett. f GDPR);
10. **Videosorveglianza** (Provv. Garante 8 aprile 2010; art. 6, par.1, lett. f GDPR);
11. **Utilizzo di piattaforme digitali e cloud** (Google Workspace for Education, registro elettronico, piattaforme DDI), nel rispetto del DSA/DMA e delle norme su trasferimento dati extra-UE.

5. Base giuridica

- Art. 6, par.1, lett. c ed e GDPR – obbligo legale e compiti di interesse pubblico;
- Art. 9, par.2, lett. g GDPR – dati particolari per finalità scolastiche;
- Art. 6, par.1, lett. a GDPR – consenso (immagini divulgative, farmaci, attività extracurricolari non obbligatorie);
- Art. 6, par.1, lett. f GDPR – legittimo interesse (videosorveglianza, difesa diritti).

6. Categorie di dati trattati

- **Dati comuni**: anagrafici, identificativi, fiscali, scolastici;
- **Dati particolari (art. 9 GDPR)**: sanitari (certificati, disabilità, vaccinazioni, L.104/1992), convinzioni religiose (es. scelta IRC), dati sensibili per bisogni educativi speciali;
- **Dati giudiziari (art. 10 GDPR)**: eventuali provvedimenti giudiziari rilevanti per l'attività scolastica.

7. Modalità di trattamento e sicurezza informatica

Il trattamento avviene in forma cartacea e digitale, con misure tecniche e organizzative adeguate (art. 32 GDPR).
In materia di sicurezza informatica, dal 2024–2025 sono state introdotte novità significative:

- **Reg. UE 2841/2023** e **L. 90/2024 (NIS2 Italia)**: obbligo per le PA, comprese le scuole, di adottare un **Sistema di Gestione della Sicurezza delle Informazioni (ISMS)** conforme agli standard internazionali (ISO/IEC 27001 e 27701);
- **Piano Triennale ICT PA 2022–2024 (AgID)**: obbligo di garantire backup cifrati, disaster recovery e continuità operativa;
- **Linee guida AgID 2023–2024**: rafforzamento autenticazione a più fattori (MFA) per accesso a registro elettronico e piattaforme cloud;
- **ENISA Cybersecurity Recommendations 2024**: specifiche raccomandazioni per la protezione dei minori online e la gestione sicura dei servizi cloud educativi;
- **DSA/DMA**: obblighi di trasparenza e responsabilità dei grandi fornitori digitali (Google, Microsoft) anche nei confronti delle scuole;
- **Legge 90/2024**: obbligo di segnalare eventuali incidenti di sicurezza (data breach o cyberattacchi) all'ACN (Agenzia per la Cybersicurezza Nazionale) e al Garante Privacy entro 72 ore.

Le principali misure adottate dalla scuola includono:

- autenticazione forte (SPID/CIE per i genitori, MFA per docenti e personale);
- cifratura dei dati sensibili e dei backup;
- segmentazione della rete interna e firewall dedicati;
- monitoraggio log e sistemi anti-intrusione (IDS/IPS);
- formazione continua del personale (art. 39 GDPR e Linee guida AgID).

---

8. Conservazione dei dati

- Dati scolastici e amministrativi: per la durata della carriera scolastica e oltre, secondo i piani di conservazione MiC.
- Dati multimediali: fino a revoca consenso o cancellazione dai sistemi.
- Videosorveglianza: massimo 7 giorni (salvo proroga per indagini).
- Log informatici: conservati secondo obblighi AgID e normativa cybersecurity (min. 6 mesi per incident detection).

---

9. Comunicazione e destinatari dei dati

- Personale scolastico autorizzato (art. 29 GDPR);
- Responsabili esterni (art. 28 GDPR): fornitori IT, cloud provider (Google Ireland Ltd.), consulenti, manutentori;
- Enti pubblici: MIM, MEF, INPS, INAIL, Regioni, Comuni, AUSL, forze dell'ordine;
- Istituti bancari e assicurativi per gestione sinistri/pagamenti;
- Agenzie viaggio e strutture ricettive per uscite didattiche.

---

10. Trasferimento extra UE

I dati possono essere trasferiti in Paesi terzi, in particolare con l'utilizzo di Google Workspace for Education:

- verso Paesi coperti da **decisioni di adeguatezza** (es. EU-US Data Privacy Framework, luglio 2023);
- in assenza, con **Clausole Contrattuali Standard (Decisione 2021/914)** e misure supplementari (cifratura end-to-end, data localization).

---

11. Diritti degli interessati

Ai sensi degli artt. 15–22 GDPR, gli interessati hanno diritto a: accesso, rettifica, cancellazione, limitazione, portabilità, opposizione e revoca del consenso.

È sempre possibile proporre reclamo al Garante Privacy (www.garanteprivacy.it).

---

12. Conclusioni operative

L'Istituto, in linea con le novità normative 2024–2025, ha rafforzato il proprio modello di protezione dei dati:

- aggiornamento delle informative e dei registri dei trattamenti;
- adozione di misure di sicurezza ICT conformi a NIS2 e Reg. 2841/2023;
- implementazione di procedure di gestione e notifica dei **data breach**;
- piani di formazione annuale per tutto il personale (art. 39 GDPR);
- verifica costante dei fornitori di servizi digitali alla luce del DSA/DMA.
