
Informativa sul trattamento dei dati personali

Utilizzo dell'Intelligenza Artificiale

Ai sensi degli artt. 13-14 del Regolamento UE 2016/679 (GDPR)

Destinatari: personale docente e personale ATA

1. Titolare del trattamento

Denominazione	ISTITUTO TECNICO SETTORE TECNOLOGICO
Sede legale	Via Mauro Leone, 105 – 80038 Pomigliano D’Arco (NA)
Codice meccanografico	NATF040003
Codice fiscale	80104010634
Email	NATF040003@istruzione.it
PEC	NATF040003@pec.istruzione.it
Telefono	+39 081 884 1350
Dirigente Scolastico	Nome e cognome: Carmela Mosca

2. Responsabile della Protezione dei Dati (DPO)

Data Protection Officer (DPO): Giovanni Notaro

3. Oggetto dell'informativa

La presente informativa illustra le modalità di trattamento dei dati personali del personale scolastico (docenti e ATA) nell'ambito dell'utilizzo di strumenti di intelligenza artificiale per finalità didattiche, organizzative e amministrative.

4. Finalità del trattamento

I dati personali del personale vengono trattati per le finalità che seguono.

A. Gestione delle attività didattiche con supporto IA

- preparazione di materiali didattici personalizzati;
- creazione di verifiche e prove di valutazione;
- elaborazione di contenuti per le diverse discipline;
- supporto alla programmazione didattica;
- generazione di risorse per l'inclusione di studenti BES e DSA.

B. Gestione delle attività amministrative con supporto IA

- redazione di circolari e comunicazioni istituzionali;
- elaborazione di documenti amministrativi standard;
- traduzione di comunicazioni per utenza non italofona;
- ottimizzazione dei processi gestionali;
- risposte automatizzate a quesiti ricorrenti.

C. Formazione professionale

- monitoraggio della partecipazione e delle competenze acquisite;
- certificazione dei percorsi formativi;
- valutazione dell'efficacia della formazione.

D. Governance e monitoraggio

- gestione delle richieste di autorizzazione di nuovi strumenti IA;
- tracciamento dell'utilizzo degli strumenti autorizzati;
- rilevazione dei dati per i KPI (Key Performance Indicators);
- audit di conformità normativa;
- reporting periodico agli organi collegiali.

5. Base giuridica del trattamento

Il trattamento dei dati personali del personale si fonda sulle basi giuridiche che seguono.

Art. 6, par. 1, lett. b GDPR: esecuzione del contratto

Trattamento necessario all'esecuzione del contratto di lavoro e degli obblighi contrattuali.

Art. 6, par. 1, lett. c GDPR: obbligo legale

Adempimento di obblighi normativi:

- Regolamento UE 2024/1689 (AI Act), art. 4: obbligo di formazione dei deployers;
- D.Lgs. 165/2001: obblighi del pubblico dipendente;
- CCNL Comparto Istruzione e Ricerca: obblighi di formazione e di aggiornamento.

Art. 6, par. 1, lett. e GDPR: interesse pubblico

Svolgimento delle funzioni istituzionali dell'amministrazione scolastica.

6. Categorie di dati personali trattati

Dati anagrafici e di contatto

- nome, cognome;
- codice fiscale;
- ruolo e qualifica;
- email istituzionale;
- recapiti telefonici, se forniti;
- plesso o sede di servizio.

Dati relativi all'attività professionale

- disciplina di insegnamento o mansione amministrativa;
- competenze digitali (autovalutazione DigComp Edu);
- partecipazione a corsi di formazione IA;
- certificazioni digitali possedute;
- utilizzo di strumenti IA autorizzati (tipologia, frequenza, finalità);
- richieste di autorizzazione di nuovi strumenti presentate;
- materiali didattici prodotti con supporto IA (metadati, non contenuti riservati).

Dati generati dall'uso di strumenti IA

- log degli accessi agli strumenti autorizzati (data, ora, durata);

-
- tipologia delle operazioni effettuate;
 - output generati, solo per finalità di controllo qualità e non per la valutazione del personale.

Dati che NON vengono trattati

Dati sensibili (salute, orientamento politico, religioso o sindacale).

Dati biometrici.

Dati di geolocalizzazione.

Contenuti personali non professionali.

7. Modalità del trattamento

Il trattamento avviene con strumenti informatici e telematici, mediante:

- piattaforme IA autorizzate (White List pubblicata);
- sistemi di gestione della formazione;
- database interni per il monitoraggio degli utilizzi;
- registro degli strumenti IA;
- dashboard google moduli KPI.

Le modalità organizzative e logiche correlate alle finalità garantiscono:

- sicurezza e confidenzialità dei dati;
- protezione da accessi non autorizzati;
- integrità e disponibilità dei dati;
- tracciabilità delle operazioni.

8. Obblighi del personale come utilizzatore di strumenti IA

Il personale docente e ATA, nell'utilizzo di strumenti di intelligenza artificiale, è tenuto a rispettare gli obblighi che seguono.

Obblighi generali

1. Utilizzo esclusivo di strumenti autorizzati

Utilizzare unicamente strumenti inseriti nella White List pubblicata sul sito web istituzionale. L'utilizzo di strumenti non autorizzati costituisce violazione delle procedure e può comportare responsabilità disciplinare.

2. Partecipazione alla formazione obbligatoria

Completare il percorso formativo AI Literacy Base (6 ore) entro i termini stabiliti (100% del personale entro dicembre 2026). La mancata partecipazione costituisce inadempimento degli obblighi contrattuali.

3. Supervisione umana integrale

Validare sempre gli output generati dai sistemi IA prima dell'utilizzo con gli studenti o nei documenti ufficiali. La responsabilità finale sui contenuti resta del dipendente e non può essere delegata all'IA.

4. Dichiarazione dell'uso dell'IA

Dichiarare esplicitamente quando i materiali didattici o i documenti sono stati elaborati con il supporto dell'IA, secondo le modalità previste dal Regolamento d'Istituto.

5. Rispetto delle procedure autorizzative

Presentare richiesta formale al Gruppo di Lavoro IA per ogni nuovo strumento che si intende utilizzare, inviando email al referente IA.

Prescrizioni specifiche in materia di privacy

6. Divieto assoluto di inserimento di dati sensibili degli studenti

È vietato inserire in qualsiasi strumento IA:

- nomi e cognomi degli studenti;
- codici fiscali;
- diagnosi mediche o certificazioni DSA nominative;
- situazioni familiari, sociali o economiche personali;
- appartenenza religiosa, etnica o politica;
- voti e valutazioni nominative complete.

7. Preferenza per dati anonimi o aggregati

Utilizzare preferibilmente dati anonimi (ad esempio "classe 3A" anziché i nominativi) o aggregati, quando possibile.

8. Minimizzazione dei dati

Inserire solo i dati strettamente necessari alla finalità specifica. Non caricare intere classi nominative se non indispensabile.

9. Credenziali personali

Utilizzare esclusivamente le proprie credenziali di accesso agli strumenti IA. È vietata la condivisione di username e password.

10. Segnalazione immediata delle criticità

Segnalare tempestivamente al Referente IA e al DPO:

- malfunzionamenti degli strumenti;
- output inappropriati o errati;
- sospette violazioni di sicurezza;
- difficoltà operative.

9. Destinatari e comunicazione dei dati

I dati personali del personale possono essere comunicati ai soggetti che seguono.

Destinatari interni all'Istituto

- Dirigente Scolastico;
- membri del Gruppo di Lavoro IA, per finalità di governance;
- Referente IA, per supporto tecnico;
- DSGA e personale amministrativo, per finalità gestionali;
- DPO, per controlli di conformità privacy.

Destinatari esterni all'Istituto

- fornitori di servizi IA autorizzati, in qualità di responsabili del trattamento con cui sono in essere contratti specifici;
- enti erogatori di formazione, per la certificazione dei percorsi;
- Ministero dell'Istruzione, USR, Ambito Territoriale, per gli adempimenti normativi;
- autorità di controllo (Garante Privacy, Autorità IA europea), in caso di ispezioni.

Non diffusione pubblica

I dati personali del personale relativi all'uso dell'IA NON sono oggetto di diffusione pubblica, salvo gli obblighi di trasparenza amministrativa previsti da normativa specifica (ad esempio per gli incarichi retribuiti).

10. Trasferimento di dati extra UE

Alcuni strumenti IA autorizzati possono comportare il trasferimento di dati personali verso paesi extra UE (ad esempio gli Stati Uniti per servizi cloud-based). In tali casi, il trasferimento avviene con garanzie adeguate:

- clausole contrattuali standard (SCC) approvate dalla Commissione Europea;
- certificazioni riconosciute (ad esempio ISO 27001, SOC 2);
- accordi internazionali vigenti.

L'elenco dettagliato degli strumenti con trasferimenti extra UE è disponibile nella White List pubblicata sul sito web, con indicazione delle garanzie specifiche.

11. Periodo di conservazione

I dati personali sono conservati per i periodi che seguono.

Dati formativi (partecipazione ai corsi, attestati)

- durata: 10 anni dalla cessazione del rapporto di lavoro;
- finalità: documentazione degli obblighi formativi, ricostruzione di carriera, gestione di eventuale contenzioso.

Dati di utilizzo degli strumenti IA (log, richieste di autorizzazione)

- durata: 5 anni dalla generazione;
- finalità: audit di conformità, tracciabilità delle decisioni, gestione di eventuale contenzioso.

Dati di monitoraggio KPI (dati aggregati anonimi)

- durata: 10 anni;
- finalità: serie storiche, valutazione diacronica delle politiche digitali.

Al termine dei periodi indicati, i dati vengono cancellati in modo sicuro e irreversibile, salvo obblighi di legge che impongano una conservazione superiore.

12. Diritti degli interessati

Il personale ha diritto di:

Art. 15 GDPR: accesso	ottenere conferma dell'esistenza di dati personali e riceverne copia;
Art. 16 GDPR: rettifica	ottenere la correzione di dati inesatti o l'integrazione di dati incompleti;
Art. 17 GDPR: cancellazione (oblio)	ottenere la cancellazione dei dati quando non sono più necessari, compatibilmente con gli obblighi di conservazione legale;
Art. 18 GDPR: limitazione	ottenere la limitazione del trattamento in presenza di specifiche condizioni;
Art. 20 GDPR: portabilità	ricevere in formato strutturato i dati forniti al titolare per trasmetterli ad altro titolare;
Art. 21 GDPR: opposizione	opporsi al trattamento per motivi connessi alla situazione particolare, salvo prevalenti motivi legittimi del titolare;
Art. 22 GDPR: decisioni automatizzate	non essere sottoposti a decisioni basate unicamente su trattamento automatizzato che producano effetti giuridici.

Modalità di esercizio dei diritti

La richiesta deve essere inviata in forma scritta a:

- Dirigente Scolastico (via email);
- DPO (via email).

Tramite i seguenti canali:

- email istituzionale;
- PEC;

Termini di risposta: 30 giorni, prorogabili di ulteriori 60 giorni in casi complessi.

13. Diritto di reclamo

In caso di ritenuta violazione dei diritti, il personale può proporre reclamo all'autorità competente.

Autorità	Garante per la Protezione dei Dati Personali
Indirizzo	Piazza Venezia n. 11, 00187 Roma
Telefono	+39 06.696771

Email	garante@gdpd.it
PEC	protocollo@pec.gdpd.it
Sito web	www.garanteprivacy.it

14. Responsabilità e sanzioni

Responsabilità professionale

L'utilizzo improprio di strumenti IA, in particolare nei casi che seguono:

- uso di strumenti non autorizzati;
- inserimento di dati sensibili degli studenti in violazione dei divieti;
- mancata supervisione degli output;
- condivisione delle credenziali;
- rifiuto della formazione obbligatoria.

Può comportare sanzioni disciplinari secondo CCNL e Codice Disciplinare:

- richiamo verbale;
- richiamo scritto;
- multa;
- sospensione dal servizio;
- nei casi più gravi: licenziamento.

Responsabilità amministrativa

In caso di danno all'amministrazione derivante da uso improprio.

Responsabilità civile e penale

In caso di violazioni che configurino reati, ad esempio violazione della privacy, diffamazione, accesso abusivo a sistemi informatici.

Responsabilità verso terzi

Per i danni causati a studenti, famiglie o altri soggetti da uso scorretto dell'IA.

15. Misure di sicurezza

Il titolare ha adottato misure tecniche e organizzative adeguate, disponibili mediante gli strumenti di google workspace ufficiali

16. Consultazione obbligatoria del DPO

Per ogni nuovo strumento IA che tratti dati personali (di studenti o di personale) è obbligatoria la consultazione preventiva del DPO, che esprime parere vincolante sulla conformità GDPR.

Il personale che propone l'adozione di un nuovo strumento deve fornire al DPO i seguenti elementi:

- documentazione tecnica del fornitore;
- informativa privacy del fornitore;
- descrizione delle finalità e dei dati trattati;
- misure di sicurezza implementate.

17. Data Protection Impact Assessment (DPIA)

Per gli strumenti IA ad alto rischio (valutazione automatizzata con effetti significativi, monitoraggio sistematico, trattamento di dati sensibili su larga scala), è obbligatoria una DPIA prima dell'implementazione.

La DPIA viene condotta dal Dirigente Scolastico con il supporto del DPO e del Gruppo di Lavoro IA, e valuta:

- necessità e proporzionalità del trattamento;
- rischi per i diritti e le libertà degli interessati;
- misure di mitigazione dei rischi;
- opportunità di procedere con l'implementazione.

18. Gestione del data breach

In caso di violazione di sicurezza che comporti accidentalmente o illegalmente la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali, si applicano gli obblighi che seguono.

Obblighi del personale

- segnalazione immediata al DPO e al Dirigente Scolastico, entro 24 ore dalla scoperta;
- descrizione dettagliata dell'incidente;
- non cancellare tracce o log utili per le indagini.

Obblighi del titolare

- valutazione della gravità con il DPO;
- notifica al Garante Privacy entro 72 ore in caso di rischio elevato;
- comunicazione agli interessati senza ritardo, in caso di rischio elevato per i diritti;

-
- documentazione nel registro delle violazioni;
 - adozione di misure correttive.

19. Trasparenza e accesso alla documentazione

Sul sito web istituzionale sono pubblicati e costantemente aggiornati i contenuti che seguono.

- Piano d'Istituto IA, in versione completa;
- Regolamento sull'uso dell'IA;
- White List degli strumenti autorizzati, con indicazione del trattamento dei dati;
- Black List degli strumenti vietati;
- Informative varie

Il personale è tenuto a consultare regolarmente la documentazione, in particolare la White List, prima di utilizzare qualsiasi strumento.

20. Aggiornamenti dell'informativa

La presente informativa può essere aggiornata in caso di:

- modifiche normative;
- adozione di nuovi strumenti;
- variazioni delle modalità di trattamento;
- evoluzioni organizzative.

Gli aggiornamenti sostanziali vengono comunicati al personale tramite:

- email istituzionale;
- circolare interna;
- pubblicazione sul sito web con evidenza delle modifiche.

Data dell'ultima versione: 20/10/2025

Versione: 1

21. Contatti

Per informazioni, chiarimenti, esercizio dei diritti o segnalazioni rivolgersi all'email scolastica:
NATF040003@istruzione.it