MANUALE PER L'USO DELL'INTELLIGENZA ARTIFICIALE A SCUOLA

IC 3 – GIUSEPPE PRATI DON PIPPO

Versione 1

DIRIGENTE SCOLASTICO Mirko Vignoli

DPO Mario Padroni

INDICE

REGOLAMENTO PER L’USO DELL’INTELLIGENZA ARTIFICIALE A SCUOLA 2

FINALITÀ 3

DEFINIZIONE E AMBITO DI APPLICAZIONE 4

NORMATIVA DI RIFERIMENTO 4

SEZIONE I – Uso dell’intelligenza artificiale da parte del personale scolastico 5

SEZIONE II – Uso dell’intelligenza artificiale da parte degli alunni della scuola primaria 8

SEZIONE III – Uso dell’intelligenza artificiale da parte degli alunni della scuola secondaria di primo grado 8

SEZIONE V – Tutela dei minori 9

SEZIONE V – Privacy, protezioni dei dai e gestione delle violazioni 9

SEZIONE VI – Responsabilità e sanzioni 10

SEZIONE VII – Regole di comportamento (netiquette) 11

SEZIONE VII – Disposizioni finali 11

ALLEGATO A 0

ELENCO DEGLI STRUMENTI DI INTELLIGENZA ARTIFICIALE AUTORIZZATI E APPROVATI 0

ALLEGATO B 8

LETTERA DI NOMINA DEL DESIGNATO 8

ALLEGATO C 14

INFORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI E INTELLIGENZA ARTIFICIALE 14

ALLEGATO D 20

LINEE GUIDA PER IL TRATTAMENTO E LA PROTEZIONE DEI DATI PERSONALI DEL PERSONALE DOCENTE 20

ALLEGATO E 30

LINEE GUIDA PER IL TRATTAMENTO E LA PROTEZIONE DEI DATI PERSONALI DEL PERSONALE AMMINISTRATIVO 30

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

REGOLAMENTO PER L'USO DELL'INTELLIGENZA ARTIFICIALE A SCUOLA

IN CONFORMITÀ AL REG. (UE) N. 2024/1689 (AI ACT) E AL REG. (UE) N. 679/2016 (GDPR)

Rev. n°	Data	Descrizione della revisione	Approvato Legale Rappresentante
01	[27/03/2026]	Prima Stesura	Elaborato e approvato dal Collegio dei Docenti con Delibera n. 27 del 10 marzo 2026 e dal Consiglio di Istituto con Delibera n. 5 del 27 marzo 2026.

VISTO

il Regolamento UE 2024/1689, ed in particolare l'art. 4 secondo il quale "I fornitori e i «deployer» dei sistemi di IA adottano misure per garantire **un livello sufficiente di alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto**, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione, nonché il contesto in cui i sistemi di IA devono essere utilizzati, **e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati.** [...] La nozione di «deployer» di cui al presente regolamento dovrebbe essere interpretata come **qualsiasi persona fisica o giuridica, compresi un'autorità pubblica**, un'agenzia o altro organismo, **che utilizza un sistema di IA sotto la sua autorità**, salvo nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale. A seconda del tipo di sistema di IA, l'uso del sistema può interessare persone diverse dal deployer."

Il presente regolamento è redatto in coerenza con le **Linee guida per l'introduzione dell'Intelligenza Artificiale nelle istituzioni scolastiche** emanate dal Ministero dell'Istruzione e del Merito con **DM n. 166/2025**, che promuovono un impiego consapevole, etico e sicuro dell'IA all'interno dell'istituzione scolastica.

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

Il documento riconosce il valore dell'IA come supporto ai processi di insegnamento e apprendimento, alla personalizzazione dei percorsi formativi e allo sviluppo delle competenze digitale degli studenti, senza sostituire il ruolo educativo del docente. Riconosce altresì funzioni utili ad alleggerire il lavoro del personale amministrativo.

Il regolamento stabilisce ambiti di utilizzo consentiti, responsabilità di docenti, studenti e personale scolastico, regole per la tutela dei dati personali, per la produzione degli elaborati, promuovendo trasparenza, rispetto delle norme e formazione della comunità scolastica.

FINALITÀ

Il presente regolamento disciplina l'utilizzo degli strumenti di Intelligenza Artificiale (IA) nell'Istituto Comprensivo IC3 - Forlì.

In accordo con le Linee guida ministeriali, l'Istituto promuove un utilizzo dell'IA che sia:

- centrato sulla persona;
- rispettoso dei diritti fondamentali;
- didatticamente significativo;
- eticamente responsabile;
- trasparente;
- conforme alle normative vigenti.

Il regolamento ha le seguenti finalità:

- garantire la sicurezza dei dati personali e della privacy
- Definire le linee guida per l'utilizzo dell'IA nella didattica e nella gestione scolastica
- promuovere un uso consapevole delle tecnologie attraverso la formazione del personale e degli studenti;
- tutelare l'apprendimento autentico degli studenti;
- prevenire usi impropri i rischi legati alla manipolazione al plagio e ai pregiudizi algoritmici;
- sviluppare competenze digitali e pensiero critico.

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

DEFINIZIONE E AMBITO DI APPLICAZIONE

- Per Intelligenza Artificiale (IA o AI) si intendono sistemi informatici capaci di generare contenuti o risposte automatiche attraverso elaborazione di dati e algoritmi, prendere decisioni o supportare attività umane con vari livelli di autonomia.
- Sono strumenti di IA software, piattaforme e applicazioni, basate su modelli di IA, incluse le tecnologie di apprendimento automatico (machine Learning), i modelli linguistici (LLM) e i sistemi di generazione di contenuti multimediali. Per esempio: chatbot conversazionali, generatori di testi, generatori di immagini, sistemi di traduzione e sintesi automatica e tutor digitali intelligenti.
- Deployer: qualsiasi soggetto (docente, studente personale scolastico) che utilizza strumenti di IA all'interno della scuola.

Il seguente regolamento si applica a tutto il personale docente e non docente, agli studenti e alle famiglie nell'ambito delle attività didattiche e amministrative della scuola.

NORMATIVA DI RIFERIMENTO

- Regolamento (UE) 2016/679 – GPDR
- Regolamento (UE) 2024-AI Act
- Decreto ministeriale n. 166 del 9 /08/ 2025 e Legge 23/09/2025, n. 132, relative alle linee guida per l'introduzione dell'intelligenza artificiale nelle istituzioni scolastiche
- Linee Guida per l'utilizzo dell'intelligenza artificiale nella Pubblica Amministrazione (AGID, versione 2023)
- Principi etici dell'Alta Autorità per l'IA della Commissione UE (2021)

Art. 1 – Principi generali (Linee guida MIM)

L'utilizzo dell'IA nell'Istituto si basa sui seguenti principi:

- **Centralità dello studente**: l'uso dell'IA deve supportare l'apprendimento del discente, sostenendo percorsi personalizzati e valorizzando potenzialità, talenti e inclinazioni individuali; deve favorire l'inclusione scolastica, attraverso interventi didattici mirati, che supportino l'integrazione, la personalizzazione dei percorsi e la prevenzione della dispersione scolastica. Gli studenti devono imparare a verificare le informazioni prodotte dall'IA, riconoscere errori e imprecisioni e comprenderne limiti e rischi.

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

- **Ruolo centrale del docente:** l'IA non può sostituire il ruolo educativo e valutativo del docente. L'adozione di strumenti di IA deve essere coerente con il piano triennale dell'offerta formativa PTOF e il patto educativo di corresponsabilità. Non deve essere utilizzata per generare discriminazioni o condizionamenti indebiti sugli studenti.
- **Supportare l'organizzazione scolastica:** può essere usata al servizio del personale amministrativo per la semplificazione e l'ottimizzazione dei processi interni attraverso strumenti digitali e automatizzati; rende più efficaci ed efficienti le comunicazioni e le attività rivolte a studenti e famiglie.
- **Promuovere la formazione** continua del personale, al fine di garantire competenze aggiornate per un uso consapevole, critico e responsabile delle nuove tecnologie.

L'Intelligenza Artificiale viene pertanto intesa come **strumento di supporto** ai processi educativi e organizzativi, che non sostituisce il ruolo centrale dello studente nell'apprendimento né quello del docente nella guida didattica.

Art. 2 – Applicazioni consentite

Sono ammessi strumenti di IA che:

- assistono nella scrittura traduzione o revisione di testi sotto supervisione didattica;
- supportano il tutoraggio per il recupero il potenziamento l'orientamento;
- generano contenuti multimediali per fini educativi (es. mappe concettuali, immagini, quiz);
- ottimizzano, processi amministrativi interni (es. automatizzazione di moduli o risposte).

SEZIONE I – Uso dell'intelligenza artificiale da parte del personale scolastico

Art. 3 – Uso dell'IA da parte dei docenti

L'attività del docente conserva priorità e valore decisionale rispetto a qualunque elaborazione prodotta da un sistema di IA. Pertanto, l'utilizzo di strumenti che prevedono AI deve essere sempre ponderato e coerente con la deontologia professionale.

- I docenti possono utilizzare strumenti di IA a supporto dell'attività didattica esclusivamente nel rispetto delle finalità educative, evitando un utilizzo passivo e non consapevole.
- L'IA può essere utilizzata per personalizzare l'insegnamento, analizzare il rendimento degli studenti ed elaborare materiali didattici, ma non deve sostituire la valutazione critica del

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

docente. È vietato l'uso per automatizzare le correzioni delle verifiche interamente senza supervisione umana.

- L'accesso e l'utilizzo di strumenti IA devono avvenire esclusivamente tramite le piattaforme e i canali ufficialmente approvati dall'Istituto e inclusi nell'apposito registro degli strumenti autorizzati.
- L'uso degli strumenti di IA da parte dei docenti deve rispettare le normative vigenti e le disposizioni della scuola, in materia di tutela della privacy.
- L'uso di IA generativa (es. chatbot, assistenti virtuali, generatori di testi o immagini) deve essere monitorato per prevenire la diffusione di informazioni inesatte o fuorvianti.
- La scelta degli strumenti deve essere coerente con quanto previsto dal PTOF in merito all'adozione dei materiali didattici e non deve comportare costi aggiuntivi per gli studenti e le famiglie salvo approvazione secondo procedure condivise.
- I docenti sono tenuti a informare preventivamente gli studenti e, ove necessario, le famiglie sull'utilizzo di strumenti IA nelle attività didattiche, fornendo adeguata informativa ex artt. 13-14 GDPR.
- Non è consentito caricare elaborati, dati o produzioni degli studenti su piattaforme di IA non contrattualizzate dall'Istituto.
- Gli utilizzatori devono segnalare eventuali anomalie, usi impropri o incidenti di sicurezza legati agli strumenti di IA al Titolare del trattamento e al DPO.

Art. 4– Uso dell'IA per la gestione amministrativa e istituzionale

- Gli strumenti dell'IA possono essere utilizzati per migliorare i processi organizzativi, purché rispettino la normativa sulla protezione dei dati personali (GDPR). L' IA non può essere impiegata per decisioni automatizzate che abbiano conseguenze dirette sugli studenti o sul personale senza supervisione umana.
- L'uso degli strumenti di IA per attività istituzionali e per la produzione di atti e documenti deve rispettare le norme vigenti le disposizioni scolastiche in maniera di privacy sicurezza dei dati e infrastrutture informatica.
- Nei processi di selezione del personale, l'uso dell'IA deve rispettare i principi di equità e non discriminazione, come previsto dal Reg. UE 2024/1689.

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

- La responsabilità del contenuto dei documenti prodotti con l'IA rimane in capo alla persona fisica che ha utilizzato lo strumento.
- La responsabilità delle decisioni resta in capo alle persone fisiche, anche quando si siano avvalse del supporto dell'IA.
- Il personale ATA deve utilizzare esclusivamente gli strumenti indicati nell'apposito registro degli applicativi autorizzati dall'Istituto.
- Verificare sempre la correttezza degli output prodotti prima di utilizzarli in atti amministrativi, comunicazioni ufficiali o procedimenti.
- Conservare traccia dell'utilizzo di sistemi di IA nella produzione di atti o documenti ufficiali, indicando ove necessario che il contenuto è stato generato o assistito dall'IA.
- Gli utilizzatori devono segnalare eventuali anomalie, usi impropri o incidenti di sicurezza legati agli strumenti di IA al Titolare del trattamento e al DPO.

Art. 5 - Educazione digitale del personale scolastico

- La scuola deve promuovere percorsi di formazione sull'IA per docenti e personale ATA.
- La formazione deve includere: uso sicuro in ambito didattico e amministrativo; etica e responsabilità nell'uso dell'IA; prevenzione del plagio e dell'abuso degli strumenti di IA.

Art. 6 – Responsabilità e limiti nell'uso dell'IA

L'uso improprio dell'IA da parte del personale può comportare sanzioni disciplinari.

- Gli strumenti di IA non devono essere impiegati per sostituire il giudizio umano in decisioni strategiche o che producano effetti giuridici sulle persone, senza adeguata revisione e supervisione.
- L' IA non deve essere utilizzata per la sorveglianza degli studenti o per raccogliere dati sensibili senza autorizzazione, quali: nomi degli studenti, voti, giudizi, PDP, PEI, relazioni, dati sanitari e informazioni personali.
- È vietato inserire nei sistemi di IA informazioni riservate, sensibili, protette da segreto o dati personali di dipendenti, studenti o famiglie, a meno che lo strumento non sia stato espressamente autorizzato e contrattualizzato come Responsabile del trattamento ex art. 28 GDPR.

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

- È vietato l'uso di IA per creare, diffondere o manipolare contenuti ingannevoli o falsificati, incluse immagini, testi o video con finalità fraudolente (c.d. deepfake).
- L'IA non deve essere utilizzata per discriminare docenti, studenti o personale ATA sulla base di dati personali o profili analizzati automaticamente.
- I sistemi di IA non devono essere impiegati per operazioni che richiedano l'accesso a dati sensibili o giudiziari, salvo espressa autorizzazione del Titolare e valutazione del rischio.

SEZIONE II – Uso dell'intelligenza artificiale da parte degli alunni della scuola primaria

Art. 7 – Utilizzo dell'IA nella scuola primaria

Nella scuola primaria l'utilizzo diretto di strumenti di IA da parte degli studenti **non è consentito**.

SEZIONE III – Uso dell'intelligenza artificiale da parte degli alunni della scuola secondaria di primo grado

Art. 8 – Utilizzo dell'IA nella scuola secondaria di I grado

Nella scuola secondaria di I grado l'utilizzo dell'AI da parte degli studenti è consentito esclusivamente per scopi educativi, sotto la supervisione o le indicazioni del docente.

- È fatto divieto di inserire immagini, filmati o registrazioni audio che riproducano persone, voci o dati personali di terzi.
- È vietato l'uso dell'IA per automatizzare compiti tesine o verifiche senza esplicita autorizzazione.
- L'accesso agli strumenti di IA deve rispettare le limitazioni d'età e imposte dai fornitori e dalle linee guida ministeriali.
- Per gli studenti minorenni, l'utilizzo di IA deve essere approvato dai genitori o tutori legali.
- Gli studenti sono responsabili di qualsiasi contenuto prodotto con strumenti di IA.
- I genitori sono responsabili per l'uso dell'IA al di fuori dell'ambiente scolastico e devono essere coinvolti nella formazione sul suo uso consapevole.

Art. 9 – Trasparenza nell'uso

- Gli studenti devono dichiarare esplicitamente l'utilizzo dell'AI nei propri lavori scolastici.
- Esempio: "Ho utilizzato uno strumento di Intelligenza Artificiale per ottenere suggerimenti e spiegazioni."

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

- L'uso di IA senza dichiarazione esplicita è considerato plagio con conseguenti provvedimenti disciplinari.

SEZIONE V – Tutela dei minori

Art. 10 – Misure di protezione rafforzate

Considerata la natura dell'Istituto, che opera quotidianamente con soggetti minorenni, l'utilizzo di sistemi di IA nel contesto scolastico richiede misure di protezione rafforzate.

- È vietato l'utilizzo di sistemi di IA che raccolgano o elaborino immagini, voci, biometria o dati comportamentali di minori, salvo espressa valutazione d'impatto (DPIA) e autorizzazione del Titolare.
- I sistemi di IA utilizzati per attività che coinvolgono minori devono essere previamente sottoposti a valutazione del rischio e, ove necessario, a DPIA ai sensi dell'art. 35 GDPR.
- È vietato l'utilizzo di sistemi di IA classificati come sistemi a «risco inaccettabile» ai sensi dell'art. 5 del Reg. UE 2024/1689, inclusi i sistemi di categorizzazione biometrica, di emozioni o di scoring sociale.
- I dati degli studenti minori non possono essere condivisi con fornitori di IA che non abbiano sottoscritto un accordo di trattamento dei dati ex art. 28 GDPR con l'Istituto.
- Il DPO dell'Istituto deve essere coinvolto preventivamente nell'adozione di qualsiasi nuovo strumento di IA che tratti dati di minori.
- Le famiglie devono essere informate, tramite apposita informativa, dell'utilizzo di strumenti di IA che interagiscono con i loro figli o ne elaborano i dati, anche in forma anonima o aggregata.

SEZIONE V – Privacy, protezioni dei dai e gestione delle violazioni

Art. 11 – Principi generali

L'utilizzo degli strumenti di IA deve avvenire nel pieno rispetto della privacy e dei diritti fondamentali degli individui, come stabilito dal Reg. UE 2016/679 (GDPR) e dal Reg. UE 2024/1689. In particolare, deve essere garantito che:

- I dati personali non siano trattati tramite sistemi di IA in assenza di un'adeguata base giuridica (art. 6 GDPR).
- I sistemi di IA adottati rispettino i principi di minimizzazione dei dati, limitazione della finalità e integrità e riservatezza (art. 5 GDPR).

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

- Non vengano generati profili automatizzati con effetti legali significativi per gli individui senza garanzie appropriate (art. 22 GDPR).
- I fornitori di strumenti di IA che trattino dati per conto dell'Istituto siano contrattualizzati come Responsabili del trattamento ai sensi dell'art. 28 GDPR, con adeguate garanzie di sicurezza.

Art. 12 – Gestione delle violazioni dei dati (Data Breach)

- Chiunque rilevi o sospetti una violazione dei dati personali connessa all'utilizzo di sistemi di IA è tenuto a segnalarla immediatamente al Titolare del trattamento e al DPO.
- La segnalazione deve avvenire in modo da consentire al Titolare di valutare la necessità di notifica al Garante entro 72 ore dall'acquisizione della conoscenza dell'evento, ai sensi dell'art. 33 GDPR.
- Non tentare di risolvere autonomamente incidenti di sicurezza che coinvolgano sistemi di IA o dati personali: informare immediatamente il responsabile tecnico e il DPO, documentando l'accaduto.
- L'Istituto mantiene un registro interno delle violazioni dei dati personali (art. 33, par. 5 GDPR), nel quale vengono annotati tutti gli incidenti, anche quelli che non richiedono notifica al Garante.

SEZIONE VI – Responsabilità e sanzioni

Art. 13 – Responsabilità degli utilizzatori

L'utilizzo improprio degli strumenti di IA può comportare conseguenze disciplinari, in conformità con le normative istituzionali e le disposizioni di legge vigenti. Ogni utilizzatore è personalmente responsabile per l'uso consapevole e conforme di tali tecnologie.

- Responsabilità dell'operatore: gli istituti che utilizzano IA, in particolare sistemi ad alto rischio, devono essere in grado di dimostrare la conformità con la legislazione applicabile (Reg. UE 2024/1689).
- Accountability e audit: l'utilizzo degli strumenti di IA deve essere tracciabile, auditabile e documentato, inclusa la registrazione dei processi decisionali automatizzati.

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

- Responsabilità civile: l'uso improprio di IA può comportare danni economici o morali a terzi. L'Istituto è tenuto a risarcire eventuali danni causati da sistemi di IA, conformemente alle leggi vigenti.
- Sanzioni disciplinari: eventuali violazioni gravi del presente Regolamento possono portare a procedimenti disciplinari fino alla sospensione o cessazione del rapporto di lavoro, ai sensi del CCNL applicabile.

Art. 14 - Valutazione dei Rischi (DVR)

L'introduzione dell'IA comporta l'aggiornamento del DVR per monitorare cybersecurity e stress lavoro-correlato.

SEZIONE VII – Regole di comportamento (netiquette)

Art. 15 – Principi di comportamento nell'uso degli strumenti IA

L'utilizzo degli strumenti e dei sistemi basati su Intelligenza Artificiale deve essere sempre improntato al rispetto reciproco, alla professionalità e alla collaborazione.

- Comunicazione chiara e trasparente: garantire che la comunicazione prodotta anche con il supporto dell'IA sia chiara, precisa e comprensibile, evitando linguaggi ambigui o fuorvianti.
- **Rispetto per gli altri:** rispettare sempre la dignità degli altri, evitando comportamenti o contenuti offensivi, discriminatori o pregiudizievoli.
- **Uso equilibrato e professionale:** evitare abusi degli strumenti IA per scopi personali o per creare situazioni di conflitto all'interno dell'Istituto.
- **Gestione delle informazioni sensibili:** utilizzare la massima cautela nell'inserire dati sensibili, riservati o confidenziali negli strumenti di IA.
- **Verifica dei contenuti:** verificare sempre la correttezza e l'affidabilità dei risultati prodotti dall'IA prima di utilizzarli. Non fare mai affidamento esclusivo sulle risposte generate senza supervisione umana.
- **Approccio critico e riflessivo:** mantenere sempre un approccio critico riguardo agli strumenti e ai risultati prodotti dall'IA, affinché le decisioni finali siano sempre improntate alla valutazione umana.

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

SEZIONE VII – Disposizioni finali

Art. 16 – Aggiornamento

Il regolamento sarà aggiornato periodicamente per adeguarsi all'evoluzione normativa e tecnologica e alle esigenze didattiche.

Il dirigente scolastico, in collaborazione con il Collegio dei Docenti, il Consiglio d'Istituto, il DPO e il team digitale, valuterà l'efficacia del regolamento e proporrà eventuali modifiche.

Art. 17 - Entrata in vigore

Il presente regolamento entra in vigore 15 giorni dopo la sua pubblicazione sul sito istituzionale.

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

ALLEGATO A

ELENCO DEGLI STRUMENTI DI INTELLIGENZA ARTIFICIALE AUTORIZZATI E APPROVATI

Istituto	Revisione	Data	Approvazione
IC3 Forlì	01	27 / 03 / 2026	Consiglio di Istituto / Dirigente scolastico

Il presente Allegato individua, per l'ambito scolastico, gli strumenti di intelligenza artificiale autorizzati e approvati per finalità didattiche, organizzative e amministrative, distinguendo gli utilizzi consentiti, i limiti operativi e le condizioni minime di sicurezza, protezione dei dati e supervisione umana.

1. Criteri generali di utilizzo

- L'utilizzo è ammesso esclusivamente per finalità istituzionali, didattiche, organizzative o amministrative coerenti con il PTOF, il Regolamento interno e le istruzioni del Dirigente scolastico;
- devono essere privilegiati, ove disponibili, account istituzionali, ambienti Education, Business, Team, Enterprise o equivalenti formalmente attivati dall'Istituto;
- restano sempre obbligatorie la verifica umana degli output, la valutazione critica dei contenuti generati e il controllo della correttezza normativa, fattuale e pedagogica;
- è vietato inserire nei sistemi non espressamente autorizzati dati personali, dati appartenenti a categorie particolari, dati giudiziari, documenti riservati, PEI, PDP, certificazioni sanitarie, atti disciplinari, dati stipendiali, documenti di protocollo o altre informazioni interne non anonimizzate o pseudonimizzate;
- per gli studenti l'uso avviene, di regola, sotto la supervisione del docente e nei limiti dell'età, delle condizioni del servizio e delle impostazioni adottate dall'Istituto;
- l'elenco è dinamico e deve essere riesaminato almeno annualmente, nonché ogni volta che vengano introdotti nuovi strumenti, nuove funzionalità o diverse condizioni contrattuali;

- il personale autorizzato è tenuto a rispettare le istruzioni interne, le misure di sicurezza e gli eventuali accordi privacy o contrattuali sottoscritti dall’Istituto.

2. Strumenti approvati per attività didattiche e di progettazione educativa

N.	Strumento	Destinatari	Utilizzo ammesso	Account / ambiente richiesto	Condizioni essenziali
1	**Gemini for Education / Gemini in Workspace / Gemini in Classroom**	Docenti/personale amministrativo	Supporto alla progettazione didattica, predisposizione di materiali, sintesi, brainstorming, semplificazione di testi, supporto linguistico e organizzazione del lavoro docente.	Account Google Workspace for Education dell’Istituto.	Verifica umana obbligatoria; divieto di affidare all’IA la valutazione finale; dati personali solo se indispensabili e nel rispetto delle impostazioni istituzionali.
2	**NotebookLM con Google Workspace for Education**	Docenti/personale amministrativo	Studio di fonti, sintesi ragionate, Q&A basato su documenti, preparazione lezioni, materiali di approfondimento, audio overview e organizzazione di fonti.	Account istituzionale Google Workspace for Education.	Caricare preferibilmente materiali istituzionali, pubblici o comunque autorizzati; evitare documenti contenenti dati personali non minimizzati.

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

N.	Strumento	Destinatari	Utilizzo ammesso	Account / ambiente richiesto	Condizioni essenziali
3	**Canva for Education (incluse funzioni AI)**	Docenti/personale amministrativo/alunni secondaria I grado	Presentazioni, infografiche, immagini, video, schede, materiali visivi, mappe e contenuti creativi per la didattica.	Ambiente Canva for Education o account verificato in ambito scolastico.	Non caricare immagini, file o dati personali non necessari; controllo docente su copyright, qualità e correttezza del contenuto.
6	**Zanichelli IA e strumenti IA integrati in piattaforme editoriali adottate**	Docenti/personale amministrativo/alunni secondaria I grado	Esercizi, schede, supporti allo studio, personalizzazione dei materiali e attività coerenti con gli strumenti editoriali adottati.	Accesso tramite piattaforme editoriali autorizzate dall’Istituto.	Uso nel rispetto delle condizioni editoriali, con controllo del docente e senza inserimento di dati sensibili.
7	**Genially AI e strumenti analoghi per contenuti interattivi**	Docenti/personale amministrativo/alunni secondaria I grado	Creazione di presentazioni interattive, escape room, mappe, quiz e contenuti comunicativi.	Account istituzionale o account autorizzato dal docente secondo le policy della scuola.	Utilizzo ammesso solo per contenuti didattici o divulgativi; evitare dati personali e verificare accessibilità, correttezza e pertinenza.

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

3. Strumenti approvati per attività organizzative, amministrative e di segreteria

N.	Strumento	Destinatari	Utilizzo ammesso	Account / ambiente richiesto	Condizioni essenziali
1	**Gemini in Google Workspace**	Docenti/personale amministrativo	Bozze di comunicazioni, sintesi di testi, supporto redazionale, organizzazione di attività e analisi preliminare di documenti.	Account istituzionale Google Workspace dell’Istituto.	Ammesso solo nell’ambiente organizzativo dell’Istituto; vietato inserire dati personali o documenti riservati in forma non minimizzata se non espressamente consentito dalle impostazioni e istruzioni interne.
2	**NotebookLM con account istituzionale**	Docenti/personale amministrativo	Analisi di normativa, regolamenti, circolari, manuali, procedure, capitolati, documentazione tecnica e schemi organizzativi.	Account istituzionale Google Workspace.	Per documenti interni con dati personali è richiesta preventiva minimizzazione o pseudonimizzazione; vietato il caricamento indiscriminato di fascicoli individuali.

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

N.	Strumento	Destinatari	Utilizzo ammesso	Account / ambiente richiesto	Condizioni essenziali
3	**Microsoft 365 Copilot Chat / Copilot**	Docenti/personale amministrativo	Supporto alla segreteria per testi, riassunti, note di riunione, check-list, organizzazione documentale e supporto operativo.	Tenant Microsoft 365 dell’Istituto con protezioni organizzative attive.	Consentito solo su ambiente istituzionale; non sostituisce il controllo umano su atti amministrativi, provvedimenti, contratti, graduatorie o comunicazioni ufficiali.
4	**ChatGPT Business / Enterprise**	Docenti/personale amministrativo	Supporto redazionale, analisi comparativa, sintesi di normativa, schemi di lavoro, modelli di comunicazione e supporto organizzativo.	Workspace organizzativo o contratto istituzionale formalmente attivato.	Non autorizzata la versione consumer/personal per attività di segreteria con dati o documenti dell’Istituto; uso ammesso solo in ambiente organizzativo controllato.

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

4. Modalità d’uso non autorizzate o non approvate

Categoria / condotta	Esito	Indicazione operativa
Uso di account personali o consumer per trattare dati o documenti dell’Istituto	NON AUTORIZZATO	Le attività istituzionali devono essere svolte, di regola, tramite account e ambienti organizzativi autorizzati.
Caricamento in sistemi non autorizzati di PEI, PDP, fascicoli alunni, certificazioni sanitarie, dati disciplinari, dati stipendiali, atti di protocollo, graduatorie o documenti analoghi	VIETATO	È ammessa solo la minimizzazione o pseudonimizzazione, nei limiti delle istruzioni interne e delle basi giuridiche applicabili.
Automazione integrale di giudizi, valutazioni, decisioni disciplinari, provvedimenti amministrativi o comunicazioni ufficiali senza controllo umano qualificato	VIETATO	L’IA ha funzione di supporto e non sostituisce l’assunzione di responsabilità del docente, del dirigente o dell’ufficio competente.
Riconoscimento delle emozioni, profilazioni improprie, classificazioni automatizzate non pertinenti o altre pratiche incompatibili con il contesto scolastico	VIETATO	Restano ferme le limitazioni derivanti dalla normativa europea, dalla disciplina privacy e dalle linee guida ministeriali applicabili.

5. Governance, aggiornamento e richieste di estensione

L’introduzione di ulteriori strumenti di IA non compresi nel presente Allegato richiede una preventiva valutazione tecnica, organizzativa e privacy da parte dell’Istituto, con particolare attenzione a: finalità del trattamento, tipologia di dati coinvolti, condizioni contrattuali, misure di sicurezza, presenza di account istituzionali, supervisione umana, coerenza con il contesto educativo e impatto sui minori.

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

La proposta di inserimento di nuovi strumenti può essere formulata dal Dirigente scolastico, dal DSGA, dall’Animatore digitale, dal team digitale o dai referenti di progetto.

L’aggiornamento dell’Allegato A deve essere formalizzato con atto interno dell’Istituto e comunicato al personale interessato.

Le autorizzazioni possono essere differenziate per ruolo: docenti, personale ATA, segreteria, funzioni strumentali, referenti di progetto e studenti.

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

ALLEGATO B

LETTERA DI NOMINA DEL DESIGNATO

ALL’UTILIZZO DEI SISTEMI DI INTELLIGENZA ARTIFICIALE E AL TRATTAMENTO DI DATI PERSONALI

per presa visione

VISTO

il Regolamento UE n. 2024/1689 (AI Act) – Regolamento del Parlamento Europeo e del Consiglio sull’intelligenza artificiale;

il Regolamento UE n. 679/2016 (GDPR) – Regolamento generale sulla protezione dei dati;

il D.Lgs. 30 giugno 2003, n. 196 (Codice Privacy) e successive modificazioni;

le Linee Guida del Garante per la protezione dei dati personali in materia di intelligenza artificiale;

il Piano Nazionale Scuola Digitale (PNSD) e le circolari del Ministero dell’Istruzione in materia di utilizzo di strumenti digitali;

il Regolamento IA e il Codice di Condotta IA adottati dall’Istituto, disponibili sul sito web della scuola;

PREMESSO

il Titolare del trattamento è l’Istituto, in persona del/della Dirigente Scolastico/a pro tempore;

l’Art. 4, par. 1 dell’AI Act definisce gli obblighi generali dei soggetti disciplinati dal regolamento, stabilendo che i soggetti che partecipano a uno o più ruoli nel ciclo di vita dei sistemi di IA garantiscono che tali sistemi siano conformi al regolamento e vengano utilizzati in modo da non comportare rischi per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, compresi i minori;

ai sensi del GDPR, i soggetti che trattano dati personali per conto del Titolare devono ricevere istruzioni formali e agire nel rispetto delle stesse;

l’individuazione come “Designato” non implica l’attribuzione di funzioni ulteriori rispetto a quelle già assegnate, bensì soltanto il conferimento di un’autorizzazione e di istruzioni specifiche all’utilizzo dei sistemi di IA e al trattamento dei dati personali;

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

CONSIDERATO

occorre definire istruzioni operative per ciascuna unità organizzativa nell'utilizzo dei sistemi di IA e nel trattamento di dati personali, in conformità con i principi di liceità, correttezza e trasparenza;

l'utilizzo di sistemi di IA in ambito scolastico deve avvenire nel rispetto dei diritti degli alunni, con particolare attenzione alla tutela dei minori ai sensi dell'Art. 8 GDPR e dell'Art. 28 AI Act;

la scuola ha adottato un elenco strumenti di AI autorizzati e approvati dall'Istituto (All. A "Elenco strumenti di AI autorizzati ")consultabile presso [UFFICIO/SEDE], nel quale sono elencati gli strumenti approvati per l'utilizzo didattico e amministrativo;

NOMINA

Il Sig./Sig..... CF.....

In servizio in questo Istituto con la mansione di..... nel plesso/ufficio.....

all'utilizzo dei sistemi di intelligenza artificiale e al trattamento di dati personali, e

tutti i docenti a tempo determinato e indeterminato in servizio presso il suddetto Istituto.

DETERMINA

Le seguenti **istruzioni operative vincolanti** per il personale docente designato:

1. Principi generali di trattamento

- I designati devono operare sotto la diretta autorità del Titolare (o del Responsabile del trattamento, se nominato) e trattare i dati personali attenendosi esclusivamente alle istruzioni ricevute.
- I dati personali devono essere trattati in modo lecito, corretto e trasparente, nel rispetto dei principi di cui all'Art. 5 GDPR.
- Qualunque trattamento di dati personali tramite sistemi di IA è consentito soltanto per lo svolgimento delle funzioni istituzionali dell'Istituto e non per finalità personali o estranee all'attività didattica.

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

- Il trattamento di dati sensibili (categorie particolari ex Art. 9 GDPR), dati giudiziari o dati relativi a minori tramite sistemi di IA è vietato, salvo diversa e specifica autorizzazione scritta del Titolare.

2. Sistemi di IA autorizzati

Il designato è autorizzato a utilizzare esclusivamente i sistemi di IA presenti nell' **All. A "Elenco strumenti di AI autorizzati** "e approvati dall'Istituto, disponibile sul sito web della scuola e aggiornato periodicamente dal Titolare.

L'utilizzo di sistemi di IA non autorizzati (es. applicazioni personali, strumenti non valutati dall'Istituto) a fini didattici o nell'ambito dell'attività scolastica è vietato.

Per richiedere l'autorizzazione all'utilizzo di un nuovo sistema di IA, il designato deve presentare richiesta scritta al Titolare indicando: nome dello strumento, fornitore, finalità d'uso, tipologia di dati trattati.

Prima di ogni utilizzo, il designato deve verificare che il sistema di IA sia classificato a rischio limitato o minimo ai sensi dell'AI Act e che il relativo fornitore abbia fornito adeguate garanzie contrattuali.

I sistemi di IA ad alto rischio (es. sistemi di valutazione automatica degli alunni, profilazione comportamentale) non possono essere utilizzati senza previa valutazione d'impatto (DPIA) e specifica autorizzazione scritta del Titolare e del DPO.

3. Modalità operative e sicurezza

- Richiedere e utilizzare soltanto i sistemi di IA e i dati strettamente necessari alla normale attività lavorativa (principio di minimizzazione dei dati, Art. 5, par. 1, lett. c GDPR).
- Non inserire nei prompt o nelle interfacce dei sistemi di IA dati personali identificativi di alunni, famiglie o colleghi (es. nomi, codici fiscali, informazioni sanitarie, situazioni familiari). Utilizzare, ove possibile, dati anonimizzati o pseudonimizzati.
- Verificare sempre l'output prodotto dai sistemi di IA prima di utilizzarlo a fini didattici, valutativi o comunicativi: il designato rimane responsabile del contenuto finale.
- Non presentare agli alunni output di IA come proprie elaborazioni originali senza adeguata indicazione della fonte e senza supervisione critica.

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

- Custodire i dati oggetto di trattamento in modo sicuro, rendendoli non accessibili a soggetti non autorizzati; non lasciare incustoditi dispositivi contenenti dati personali senza averli messi in sicurezza (blocco schermo, logout).
- Le credenziali di autenticazione ai sistemi di IA sono personali: devono essere custodite con cura, non condivise con terzi e non lasciate in libera visione. In caso di smarrimento o furto, darne immediata comunicazione al Titolare o al Responsabile del trattamento.
- Se si utilizza un dispositivo condiviso, accedere sempre con il proprio account personale e disconnettersi al termine di ogni sessione.
- Eseguire il logout corretto dagli account dei sistemi di IA al termine di ogni sessione di utilizzo.
- Accertarsi dell'identità di terzi e della loro autorizzazione prima di consentire l'accesso ai sistemi di IA in uso.

4. Obblighi di formazione e aggiornamento

- Il designato è tenuto a partecipare alle attività di formazione e aggiornamento organizzate dall'Istituto in materia di utilizzo responsabile dell'IA e protezione dei dati personali.
- Il designato deve prendere visione e rispettare il Regolamento IA e il Codice di Condotta IA adottati dall'Istituto, disponibili sul sito web della scuola, nonché i successivi aggiornamenti comunicati dal Titolare.
- In caso di dubbi circa la corretta modalità di utilizzo di un sistema di IA o di perplessità sulla liceità di un trattamento, il designato deve consultarsi con il Titolare, il Responsabile del trattamento o il DPO prima di procedere.
- Il **designato è tenuto a segnalare tempestivamente** al Titolare qualsiasi anomalia, malfunzionamento o sospetta violazione di dati personali (data breach) riscontrata nell'utilizzo dei sistemi di IA, ai sensi dell'Art. 33 GDPR, entro 72 ore dalla scoperta.
- Il mancato rispetto delle presenti istruzioni può configurare violazione degli obblighi di servizio e delle normative vigenti in materia di protezione dei dati personali e intelligenza artificiale, con le conseguenti responsabilità disciplinari, civili e penali.

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

5. Obblighi generali di riservatezza e correttezza

- Il personale della scuola è tenuto a mantenere il riserbo su tutte le informazioni conosciute nello svolgimento delle proprie funzioni, nel rispetto delle norme vigenti e del Codice di comportamento dei dipendenti pubblici. L’obbligo di riservatezza continua anche dopo la cessazione dell’incarico.
- I dati personali di studenti, famiglie, personale e altri soggetti sono trattati solo per finalità istituzionali della scuola, in modo lecito, corretto e trasparente e nel rispetto della normativa sulla protezione dei dati personali e delle indicazioni dell’Autorità garante.
- È vietato utilizzare sistemi informatici o di intelligenza artificiale e le informazioni acquisite per scopi personali o non autorizzati, nonché comunicare o diffondere a soggetti non autorizzati dati o documenti d’ufficio non destinati alla pubblicità, in particolare quelli relativi agli alunni e alle loro famiglie.
- In caso di dubbi sul comportamento da adottare, il personale è tenuto a rivolgersi al Dirigente scolastico o ai soggetti da questi individuati (ad esempio Responsabile del trattamento o Responsabile della protezione dei dati), al fine di prevenire violazioni di legge o di regolamento.
- Resta salva la possibilità per il personale di effettuare segnalazioni di illeciti o irregolarità secondo la normativa sul whistleblowing, che garantisce la riservatezza dell’identità del segnalante e le tutele previste dalla legge.

Principali riferimenti legislativi

- Codice penale, art. 326 – Rivelazione ed utilizzazione di segreti di ufficio.
- D.P.R. 10 gennaio 1957, n. 3, art. 15 – Doveri del pubblico dipendente (obbligo di segretezza).
- D.P.R. 16 aprile 2013, n. 62, come modificato dal D.P.R. 13 giugno 2023, n. 81 – Codice di comportamento dei dipendenti pubblici.
- Regolamento (UE) 2016/679 (GDPR), in particolare art. 5 – Principi applicabili al trattamento dei dati personali.
- Decreto legislativo 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali, come modificato e coordinato con il GDPR.

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

- Decreto legislativo 10 marzo 2023, n. 24 – Protezione delle persone che segnalano violazioni del diritto (whistleblowing).

N.B. Il Regolamento IA, il Codice di Condotta IA e **l'All. A elenco strumenti di AI autorizzati** sono disponibili sul sito web dell'Istituto e presso [UFFICIO/SEDE COMPETENTE]. Il designato è tenuto a consultarli periodicamente.

L'attribuzione di compiti e responsabilità deve intendersi valida per l'intera durata del contratto di servizio, salvo diversa comunicazione del Titolare o interruzione del rapporto di collaborazione.

[LOCALITÀ], _____ / _____ / _____

[NOME ISTITUTO]	**Il Designato al Trattamento**
Il Titolare del trattamento	L'Incaricato/a
Il/La Dirigente Scolastico/a	*[Firma per presa visione e accettazione]*
[Firma e timbro]	

Dichiarazione di presa visione: Il/la sottoscritto/a dichiara di aver ricevuto, letto e compreso le presenti istruzioni operative, di accettarne i contenuti e di impegnarsi al loro rispetto per tutta la durata del mandato, ai sensi e per gli effetti delle normative vigenti in materia di protezione dei dati personali e intelligenza artificiale.

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

ALLEGATO C

INFORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI E INTELLIGENZA ARTIFICIALE

DESTINATARI: PERSONALE DOCENTE E ATA

Ai sensi del Reg. UE n. 679/2016 (GDPR), artt. 13-14, e del Reg. UE n. 2024/1689 (AI Act), artt. 13, 20, 26 e 50

1. Premessa e finalità della presente informativa

La presente informativa, predisposta in ottemperanza al Regolamento (UE) 2016/679 ("GDPR") e, per quanto applicabile, al Regolamento (UE) 2024/1689 sull'Intelligenza Artificiale ("AI Act"), ha la finalità di informare in modo chiaro, esaustivo e trasparente il Personale Docente e ATA dell'Istituto in merito all'introduzione e all'utilizzo, nell'ambito delle attività didattiche, educative e amministrative, di strumenti basati su tecnologie di intelligenza artificiale (di seguito, "IA" o "sistemi IA"), con specifico riferimento a:

- agli aspetti relativi al trattamento dei dati personali del personale eventualmente connessi all'uso dei sistemi IA;
- ai profili di accountability previsti per l'ente scolastico quale Titolare del trattamento;
- agli obblighi e alle responsabilità del personale in qualità di Designato ai sensi del Reg. UE 2024/1689.

La presente informativa integra e non sostituisce le informative generali sul trattamento dei dati personali del personale già fornite dall'Istituto.

2. Titolare del trattamento

Il Titolare del trattamento è **Istituto Comprensivo IC3** con sede in **via Lambertelli,12, Forlì** C.F. **92089380403**, in persona del legale rappresentante pro tempore (Dirigente Scolastico Mirko Vignoli).

Per esercitare i propri diritti o per qualsiasi comunicazione relativa al trattamento dei dati: foic82400e@istruzione.it – PEC: foic82400e@pec.istruzione.it

3. Responsabile della Protezione dei Dati (DPO)

Il Responsabile della Protezione dei Dati (DPO – Data Protection Officer) è:

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

- Mario Padroni
- Sede: via G. Bovini 41 – 48123 Ravenna (RA)
- Telefono: 333 11 82307
- E-mail: dpo@sicurezzaoggi.com

Il DPO è il punto di riferimento per il personale per tutte le questioni relative alla protezione dei dati personali nell'ambito dell'utilizzo dei sistemi IA.

4. Finalità del trattamento e base giuridica

I sistemi di IA adottati dall'Istituto sono impiegati per le seguenti finalità, a seconda del ruolo del personale:

- **Finalità didattiche**: supporto alla programmazione e alla personalizzazione delle attività didattiche, generazione di contenuti educativi, creazione di materiali e risorse formative, stimolo del pensiero critico degli studenti.
- **Finalità amministrative e organizzative**: produzione di materiale amministrativo, automatizzazione di processi ripetitivi con riduzione di tempi e costi, analisi e organizzazione di grandi quantità di dati, supporto alla redazione di atti e comunicazioni ufficiali.

La base giuridica individuata per tali trattamenti è l'**art. 6, par. 1, lett. e) GDPR** (esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri), in quanto i trattamenti rientrano nell'esercizio delle funzioni istituzionali dell'Istituto. Ove siano trattati dati particolari ai sensi dell'art. 9 GDPR, la base giuridica è l'**art. 9, par. 2, lett. b) e g) GDPR**, con le relative garanzie di sicurezza.

L'Istituto agisce quale Titolare del trattamento ai sensi dell'art. 4, par. 1, n. 7 del GDPR, ed è tenuto a garantire il rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione, limitazione della finalità, esattezza e integrità/riservatezza (art. 5 GDPR).

5. Categorie di dati personali trattati

Nell'ambito dell'utilizzo dei sistemi IA da parte del personale, possono essere trattate le seguenti categorie di dati:

- **Dati identificativi** e di contatto del personale: nome, cognome, qualifica, e-mail istituzionale, in relazione alla registrazione e all'accesso ai sistemi IA autorizzati.

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

- **Dati relativi all'attività lavorativa**: contenuti prodotti tramite sistemi IA nell'esercizio delle funzioni istituzionali (documenti, comunicazioni, materiali didattici).
- **Dati di log e di utilizzo**: informazioni tecniche sugli accessi ai sistemi IA (data, ora, dispositivo), a fini di sicurezza informatica e di audit.

Si precisa che il personale non deve inserire nei sistemi IA dati particolari (art. 9 GDPR: dati sanitari, origine etnica, convinzioni religiose, orientamento sessuale, appartenenza sindacale) né dati relativi a condanne penali (art. 10 GDPR), propri o di terzi, salvo espressa autorizzazione del Titolare e adeguata valutazione del rischio. Analogamente, è vietato inserire dati personali di studenti, famiglie o colleghi in piattaforme IA non contrattualizzate come Responsabili del trattamento ex art. 28 GDPR.

6. Modalità del trattamento

L'utilizzo dei sistemi IA da parte del personale avviene esclusivamente sotto la diretta supervisione del Titolare (Dirigente Scolastico) e in conformità alle istruzioni contenute nel Regolamento d'Istituto sull'Intelligenza Artificiale, nel Codice di Condotta IA e nell'atto di designazione individuale.

- I dati trattati tramite sistemi IA sono, in via generale, anonimizzati o pseudonimizzati.
- Non vengono inseriti nei sistemi IA nomi, cognomi, immagini o altri dati direttamente identificativi di studenti o terzi, se non nei limiti consentiti dal quadro normativo e dai documenti adottati dall'Istituto.
- Il personale è stato designato quale "Designato" ai sensi del Reg. UE 2024/1689 e ha ricevuto le istruzioni operative per il corretto utilizzo dei sistemi IA e per il trattamento dei dati personali.

L'Istituto ha adottato misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio (art. 32 GDPR), inclusa la pseudonimizzazione, la cifratura e il controllo degli accessi.

I sistemi di IA autorizzati dall'Istituto sono indicati nel Registro degli applicativi IA approvati, disponibile sul sito web istituzionale e presso la segreteria.

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

7. Periodo di conservazione

I dati personali trattati tramite sistemi IA sono conservati per il tempo strettamente necessario al raggiungimento delle finalità per cui sono stati raccolti, e comunque in conformità alle disposizioni normative vigenti in materia di conservazione dei documenti scolastici e amministrativi.

I dati di log relativi all'utilizzo dei sistemi IA sono conservati per un periodo massimo di **12 mesi**, salvo diverse esigenze di sicurezza o obblighi di legge.

Decorso il periodo di conservazione, i dati sono cancellati o resi anonimi in modo irreversibile. Le specifiche politiche di conservazione per ciascun sistema IA sono indicate nel Registro dei Trattamenti dell'Istituto.

8. Destinatari dei dati

I dati personali possono essere trattati esclusivamente dal personale autorizzato e adeguatamente formato, come previsto dall'art. 4, par. 1 del Reg. UE 2024/1689.

In relazione ai fornitori dei sistemi IA:

- I fornitori che trattano dati personali per conto dell'Istituto sono formalmente designati come Responsabili del trattamento ai sensi dell'art. 28 GDPR, con apposito contratto o atto giuridico che prevede le garanzie di sicurezza richieste.
- I dati non vengono comunicati a terzi per finalità commerciali o pubblicitarie.
- L'elenco aggiornato dei Responsabili del trattamento è disponibile su richiesta al DPO e sul sito web istituzionale.

Si precisa che la dichiarazione "Nessun dato personale viene custodito dalle applicazioni" si riferisce unicamente agli strumenti per i quali sia stata verificata tale condizione contrattuale. Il personale è tenuto a verificare, prima dell'utilizzo di qualsiasi strumento IA, che questo sia incluso nell'elenco degli applicativi autorizzati dall'Istituto.

9. Trasferimento dei dati verso Paesi terzi

L'Istituto privilegia l'utilizzo di sistemi di IA i cui server siano ubicati all'interno dello Spazio Economico Europeo (SEE).

Qualora un sistema IA autorizzato comporti il trasferimento di dati verso Paesi terzi, tale trasferimento avviene esclusivamente in presenza di una decisione di adeguatezza della Commissione europea (art. 45 GDPR) o di garanzie adeguate, quali clausole contrattuali standard

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

(art. 46 GDPR). Le informazioni specifiche sono indicate nel Registro dei Trattamenti, disponibile su richiesta al DPO.

10. Diritti degli interessati

In qualità di interessato, il personale può esercitare i seguenti diritti rivolgendo una richiesta scritta al Titolare del trattamento o al DPO:

- **Diritto di accesso** (art. 15 GDPR): ottenere conferma che sia in corso un trattamento di dati personali propri e, in tal caso, ricevere una copia dei dati trattati con le relative informazioni.
- **Diritto di rettifica** (art. 16 GDPR): ottenere la correzione di dati inesatti o l'integrazione di dati incompleti.
- **Diritto alla cancellazione** (art. 17 GDPR): ottenere la cancellazione dei dati personali nei casi previsti dalla norma, nei limiti compatibili con gli obblighi di conservazione imposti dalla legge.
- **Diritto di limitazione del trattamento** (art. 18 GDPR): ottenere la limitazione del trattamento nei casi previsti (es. dati inesatti, trattamento illecito, opposizione in corso).
- **Diritto alla portabilità dei dati** (art. 20 GDPR): ricevere i dati personali in formato strutturato e di uso comune, ove applicabile.
- **Diritto di opposizione** (art. 21 GDPR): opporsi, per motivi connessi alla propria situazione particolare, al trattamento dei dati basato sull'art. 6, par. 1, lett. e) GDPR, salvo motivi legittimi cogenti.
- **Diritto di non essere sottoposto a decisioni automatizzate** (art. 22 GDPR): non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato che producano effetti giuridici o che incidano significativamente sulla propria sfera lavorativa.
- **Diritto di reclamo** (art. 77 GDPR): proporre reclamo all'Autorità Garante per la protezione dei dati personali, Piazza Venezia n. 11, 00186 Roma – sito web: www.gpdp.it.

Si precisa che, in relazione ai dati elaborati automaticamente dai sistemi IA, il diritto di rettifica potrà essere esercitato nei limiti della natura tecnica del sistema. Il Titolare risponde alle richieste entro un mese dalla ricezione, prorogabile di ulteriori due mesi in casi di particolare complessità (art. 12 GDPR).

Le richieste di esercizio dei diritti vanno indirizzate a:

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

Titolare del trattamento: ISTITUTO COMPRENSIVO n. 3 FORLI’ – foic82400e@istruzione.it link: https://www.ictreforli.edu.it/

DPO: Mario Padroni c/o S&L srl – dpo@sicurezzaoggi.com, link: Privacy Policy - Istituto Comprensivo Statale N. 3 GIUSEPPE PRATI "DON PIPPO"

11. Obblighi del personale in caso di violazione dei dati (Data Breach)

Il personale che rilevi o sospetti una violazione dei dati personali connessa all'utilizzo di sistemi IA (es. accesso non autorizzato, perdita, diffusione indebita di dati) è tenuto a:

- Segnalare **immediatamente** l'accaduto al Titolare del trattamento (Dirigente Scolastico) e al DPO, fornendo tutte le informazioni disponibili.
- Non tentare di risolvere autonomamente l'incidente, ma documentare i fatti e attendere le istruzioni del Titolare e del DPO.
- Rispettare i termini previsti dall'**art. 33 GDPR**: il Titolare deve valutare la necessità di notifica al Garante entro **72 ore** dall'acquisizione della conoscenza dell'evento.

Per segnalazioni urgenti: DPO Mario Padroni – dpo@sicurezzaoggi.com.

12. Modifiche alla presente informativa

La presente informativa potrà essere aggiornata periodicamente per recepire modifiche normative, tecnologiche o operative. Gli aggiornamenti saranno comunicati attraverso i canali ufficiali dell'Istituto (sito web, registro elettronico, comunicazioni interne).

La versione aggiornata sostituisce integralmente le precedenti ed è disponibile sul sito web istituzionale.

Modalità di presa visione della presente informativa:

La presa visione viene gestita dall'Istituzione scolastica attraverso la seguente modalità: □ REGISTRO ELETTRONICO □ CARTACEA □ PUBBLICAZIONE SU SITO WEB (con firma di presa visione in fascicolo "presa di servizio")

[Città], __/__/____

Il Titolare del trattamento Il DPO

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

Il Dirigente Scolastico

_____ _____

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

ALLEGATO D

LINEE GUIDA PER IL TRATTAMENTO E LA PROTEZIONE DEI DATI PERSONALI DEL PERSONALE DOCENTE

INCARICATI DEL TRATTAMENTO: PERSONALE DOCENTE

PREMESSA E BASE NORMATIVA

L'Istituto, nella persona del Dirigente Scolastico in qualità di Titolare del trattamento dati, ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018 e del Reg. UE 2016/679 (GDPR), fornisce le presenti istruzioni per il trattamento dei dati personali da parte dei dipendenti appartenenti all'unità organizzativa docenti, istituita con apposita determina dirigenziale.

L'incaricato è tenuto a rispettare le disposizioni di cui alle presenti Linee Guida, a partecipare a tutte le iniziative formative in materia di protezione dei dati personali proposte dal Titolare del trattamento e ad astenersi da qualsiasi operazione di trattamento non espressamente prevista o autorizzata.

QUADRO NORMATIVO DI RIFERIMENTO

Le presenti Linee Guida sono adottate ai sensi e per gli effetti della seguente normativa vigente:

Fonte normativa	Oggetto
Reg. UE 2016/679 (GDPR)	Regolamento generale sulla protezione dei dati personali
D.Lgs. 196/2003 (Codice Privacy)	Come modificato dal D.Lgs. 101/2018 di adeguamento al GDPR
D.Lgs. 101/2018	Adeguamento dell'ordinamento nazionale al Regolamento UE 2016/679
Reg. UE 2024/1689 (EU AI Act)	Regolamento europeo sull'intelligenza artificiale – in vigore dal 01/08/2024
Linee guida AGID – Misure minime ICT	Circolare AgID n. 2 del 18 aprile 2017 e s.m.i.

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

Provvedimento Garante / MIUR – Scheda competenze	Prescrizioni per il trattamento dati nelle schede di valutazione scolastica (Provvedimento Garante 15 maggio 2014 e s.m.i.)
Provvedimenti Garante Privacy	Provvedimenti e linee guida del Garante per la protezione dei dati personali
D.Lgs. 82/2005 (CAD)	Codice dell’Amministrazione Digitale

DEFINIZIONI

Ai fini delle presenti Linee Guida si applicano le seguenti definizioni:

Dati personali:	Qualsiasi informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente, che può fornire informazioni sulle sue caratteristiche, abitudini, stile di vita, relazioni personali, stato di salute o situazione economica.	Art. 4, par. 1, n. 1, GDPR
Trattamento:	Qualunque operazione o insieme di operazioni compiute con o senza l’ausilio di processi automatizzati, applicate a dati personali: raccolta, registrazione, organizzazione, strutturazione, conservazione, consultazione, elaborazione, modifica, estrazione, raffronto, utilizzo, comunicazione, diffusione, cancellazione, distruzione. I trattamenti su supporto cartaceo sono pienamente assoggettati al GDPR.	Art. 4, par. 1, n. 2, GDPR
Categorie particolari di dati:	Dati che rivelano l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l’appartenenza sindacale; dati genetici, biometrici, relativi alla salute, alla vita sessuale o all’orientamento sessuale. In ambito scolastico sono particolarmente	Art. 9 GDPR

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

	rilevanti i dati di salute degli alunni (DSA, BES, disabilità).	
Dati giudiziari:	Dati relativi a condanne penali e reati o a connesse misure di sicurezza (es. provvedimenti soggetti a iscrizione nel casellario giudiziale, liberazione condizionale, divieto/obbligo di soggiorno, misure alternative alla detenzione).	Art. 10 GDPR
Incaricato del trattamento:	Persona fisica che, sotto l'autorità del Titolare o del Responsabile del trattamento, tratta dati personali ed è autorizzata a farlo ai sensi della normativa nazionale.	Art. 29 GDPR; art. 2-quaterdecies D.Lgs. 196/2003
Violazione dei dati (Data Breach):	Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.	Art. 4, par. 1, n. 12, GDPR
RPD / DPO:	Responsabile per la Protezione dei Dati (Data Protection Officer): figura obbligatoria nelle istituzioni scolastiche pubbliche.	Artt. 37-39 GDPR

1. Istruzioni per il trattamento dei dati

1.1. Principi generali di trattamento

Il docente, in qualità di incaricato del trattamento, nell'eseguire le operazioni di trattamento deve:

- trattare i dati secondo liceità, correttezza e trasparenza, accedendo esclusivamente alle banche dati e ai dati personali necessari e pertinenti allo svolgimento dei compiti affidati e solo per scopi determinati e legittimi (artt. 5 e 6 GDPR).
- Rispettare il principio di minimizzazione dei dati: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono raccolti e trattati (art. 5, par. 1, lett. c), GDPR).

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

- Partecipare a tutte le iniziative formative in materia di protezione dei dati personali proposte dal Titolare del trattamento.
- Segnalare prontamente al Dirigente Scolastico, al Referente Privacy o al RPD/DPO qualsiasi circostanza che possa costituire una violazione dei dati personali (data breach), anche solo potenziale, senza ingiustificato ritardo, per consentire al Titolare di rispettare il termine di 72 ore per la notifica al Garante ove applicabile (art. 33 GDPR).

1.2. Scheda delle competenze e valutazione degli alunni

Nel compilare la scheda delle competenze e i documenti di valutazione, il docente deve attenersi alle prescrizioni del Garante per la Protezione dei Dati Personali adottate in concerto con il Ministero dell'Istruzione (Provvedimento Garante 15 maggio 2014 e s.m.i.) e in particolare:

- raccogliere nella scheda delle competenze dati esclusivamente se pertinenti e non eccedenti rispetto alle finalità di valutazione; nel caso dei dati appartenenti a categorie particolari, solamente se indispensabili per la valutazione e l'orientamento dell'alunno.
- Il trattamento dei dati mediante la scheda delle competenze è consentito solo per le finalità di valutazione dell'apprendimento, del comportamento degli alunni e di certificazione delle competenze acquisite.
- Non rientrano tra le finalità perseguibili l'individuazione del profilo psicologico dell'alunno o la raccolta di informazioni sul suo ambiente sociale e culturale di provenienza, se non strettamente necessarie.
- Evitare che vengano raccolti dati appartenenti a categorie particolari (es. dati relativi allo stato di affidamento o adozione) quando non strettamente indispensabili per raggiungere le finalità di documentazione.
- Evitare di riportare descrizioni di rapporti interpersonali di natura privata o vicende familiari, in quanto del tutto estranei alla finalità della scheda delle competenze, che è e rimane uno strumento didattico.

Nota normativa: I dati degli alunni con DSA, BES o disabilità costituiscono categorie particolari di dati ai sensi dell'art. 9 GDPR. Il loro trattamento richiede basi giuridiche rafforzate e misure di sicurezza adeguate. Tali dati non devono mai essere comunicati a soggetti non autorizzati né discussi in presenza di terzi.

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

1.3. Comunicazione di dati a soggetti terzi

In caso di comunicazione di dati a soggetti terzi, il docente deve:

- verificare sempre l’identità del richiedente prima di comunicare dati personali, in particolare nel caso di richieste pervenute per telefono o tramite strumenti che non consentano il controllo dell’identità del chiamante.
- Garantire l’esattezza dei dati comunicati: nell’accogliere una richiesta di comunicazione di dati personali, prestare attenzione alla correttezza del dato trasmesso, in particolare quando la richiesta viene soddisfatta telefonicamente o attraverso trascrizione.
- Non discutere, comunicare o trattare dati personali per telefono se non si ha la certezza che il corrispondente sia un incaricato con profilo di autorizzazione tale da consentire l’acquisizione di quei dati. Tale precauzione è indispensabile se l’apparecchio viene utilizzato in luogo pubblico o aperto al pubblico.
- Non parlare ad alta voce di dati personali in presenza di terzi non autorizzati che potrebbero venirne a conoscenza in modo fortuito o accidentale.

2.Istruzioni per l’uso degli strumenti informatici

2.1. Gestione delle credenziali di accesso

- Custodire con cura le credenziali di autenticazione assegnate (accesso alla rete wireless, al registro elettronico, alle piattaforme cloud e agli altri sistemi istituzionali). Le credenziali sono strettamente personali e non possono essere rivelate a terzi.
- In caso di smarrimento, furto o compromissione delle credenziali, darne comunicazione immediata al Titolare del trattamento e al responsabile tecnico.
- Cambiare la password di accesso ai sistemi informatici e digitali con cadenza almeno trimestrale per i sistemi che trattano categorie particolari di dati; almeno semestrale per gli altri sistemi.
- La password deve essere composta da almeno dodici caratteri, contenere almeno una lettera maiuscola, una minuscola, un numero e un carattere speciale; non deve contenere riferimenti a dati personali propri o dei familiari.
- Ove disponibile, attivare l’autenticazione a due fattori (MFA/2FA) per l’accesso ai sistemi istituzionali (registro elettronico, piattaforme cloud, e-mail istituzionale).

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

2.2. Utilizzo della postazione di lavoro e del registro elettronico

- Prima di abbandonare la postazione di lavoro, anche temporaneamente, effettuare il log-off dai sistemi in uso o attivare il blocco schermo con password (blocco automatico entro 5 minuti di inattività).
- Non lasciare il registro elettronico aperto e incustodito su dispositivi accessibili ad alunni, genitori o personale non autorizzato.
- I supporti rimovibili (chiavette USB, dischi esterni) nei quali siano memorizzati dati personali devono essere custoditi con attenzione per prevenire accessi non autorizzati o smarrimento, e verificati con antivirus prima dell'uso.
- L'utilizzo di dispositivi personali (BYOD) per il trattamento di dati personali istituzionali è consentito solo previa autorizzazione scritta del Titolare e nel rispetto delle policy istituzionali.

2.3. Comunicazioni elettroniche

- Per le comunicazioni istituzionali contenenti dati personali utilizzare esclusivamente l'indirizzo e-mail istituzionale fornito dalla scuola, seguendo procedure che garantiscano la riservatezza dei dati trasmessi.
- Nelle comunicazioni via e-mail con più destinatari, quando sia necessario tutelare la riservatezza degli indirizzi dei destinatari, utilizzare il campo CCN (Copia Conoscenza Nascosta) anziché il campo CC.
- Non aprire allegati di provenienza incerta; segnalare al responsabile tecnico eventuali tentativi di phishing o accessi non autorizzati.
- È fatto divieto di utilizzare social network o applicazioni di messaggistica personali (es. WhatsApp) per comunicazioni contenenti dati personali di alunni, famiglie o colleghi.

Nota normativa: L'uso di WhatsApp o altri servizi di messaggistica non istituzionali per comunicazioni contenenti dati personali di alunni o famiglie costituisce una violazione del GDPR. Il Garante ha adottato numerosi provvedimenti sanzionatori in materia nei confronti di istituzioni scolastiche.

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

3. Istruzioni per il trattamento di documenti cartacei

3.1. Custodia e conservazione

- I documenti cartacei contenenti dati personali devono essere riposti e custoditi in contenitori muniti di serratura; le chiavi devono essere adeguatamente custodite e non devono esistere duplicati non autorizzati.
- Documenti e registri cartacei della scuola contenenti dati personali non possono essere portati all’esterno della sede scolastica né copiati, se non dietro espressa autorizzazione scritta del Titolare del trattamento.
- Verificare che i documenti siano sempre sotto il proprio controllo e custodia per l’intero ciclo necessario allo svolgimento delle operazioni di trattamento, al fine di garantire che non siano visti o trattati da persone non autorizzate.
- Conservare i documenti, in caso di trasferimento, in contenitori chiusi e anonimi (senza indicazioni del contenuto visibili dall’esterno).
- Controllare che i documenti composti da numerose pagine o raccoglitori siano sempre completi, verificando che il numero dei fogli e l’integrità del contenuto siano conformi a quanto presente all’atto del prelievo dal luogo sicuro.

3.2. Distruzione e copie

- I documenti cartacei non più utilizzati, in particolare quelli contenenti categorie particolari di dati o dati giudiziari, devono essere distrutti o resi illeggibili prima di essere eliminati (mediante distruggi-documenti o sistemi equivalenti). Evitare assolutamente di gettarli nel cestino della carta senza preventiva distruzione.
- Coloro che sono preposti alla duplicazione di documentazione (con stampanti, fotocopiatrici o altre periferiche) devono procedere alla distruzione controllata dei supporti cartacei non più necessari o che presentino errori di stampa.
- Effettuare copie di documenti contenenti dati personali solo se strettamente necessario; trattare le copie con la stessa cura degli originali e distruggere le copie non utilizzate al termine del trattamento.
- Per la consegna di copie di documenti, utilizzare buste di sicurezza con chiusura auto-sigillante; ove possibile, effettuare la consegna personalmente per ridurre al minimo la possibilità che soggetti terzi non autorizzati possano prendere visione del contenuto.

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

4. Utilizzo di strumenti basati su Intelligenza Artificiale

La presente sezione è redatta in conformità al Reg. UE 2016/679 (GDPR), al Reg. UE 2024/1689 (EU AI Act, in vigore dal 1° agosto 2024) e alle indicazioni del Garante per la Protezione dei Dati Personali in materia di intelligenza artificiale.

Nota normativa: Il Reg. UE 2024/1689 (EU AI Act) è in vigore dal 1° agosto 2024. I divieti assoluti si applicano dal 2 febbraio 2025; le norme sui sistemi AI ad alto rischio si applicheranno dal 2 agosto 2026. I sistemi AI per la valutazione automatizzata degli studenti rientrano tra i sistemi ad alto rischio (Allegato III, punto 3). L'uso di sistemi di riconoscimento delle emozioni in ambienti scolastici è vietato (art. 5).

4.1. Autorizzazione e conformità

- È consentito l'uso di strumenti basati su intelligenza artificiale (es. piattaforme di supporto alla didattica, sistemi di traduzione, strumenti di correzione automatica, chatbot educativi, generatori di contenuti, ambienti immersivi) solo se preventivamente autorizzati dall'Istituto, conformi al GDPR e contrattualizzati come responsabili del trattamento ai sensi dell'art. 28 GDPR.
- È vietato inserire dati personali, dati appartenenti a categorie particolari (art. 9 GDPR) o dati giudiziari (art. 10 GDPR) in strumenti di intelligenza artificiale pubblici o non approvati dall'Istituto (es. ChatGPT pubblico, altri chatbot online non contrattualizzati).

4.2. Uso con dati personali

L'uso di piattaforme AI con dati personali è consentito solo se preventivamente autorizzato dall'Istituto. In tali casi:

- devono essere trattati esclusivamente i dati strettamente necessari (principio di minimizzazione, art. 5, par. 1, lett. c), GDPR);
- il trattamento deve essere documentato nel Registro delle Attività di Trattamento dell'Istituto (art. 30 GDPR);
- devono essere adottate misure di sicurezza adeguate e proporzionate al rischio;
- il fornitore del servizio AI deve essere contrattualizzato come Responsabile del trattamento ex art. 28 GDPR.

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

4.3. Supervisione umana, verifica degli output e valutazione

- Qualsiasi output prodotto da un sistema AI (es. testi, traduzioni, valutazioni, analisi statistiche, piani didattici) deve essere trattato come bozza di lavoro e sottoposto a verifica critica e validazione da parte del docente prima di essere condiviso con studenti, famiglie o colleghi. L'AI non sostituisce il giudizio professionale del docente.

- L'uso dell'AI non può in alcun caso sostituire la valutazione autonoma e professionale del docente, né essere impiegato per profilazioni, giudizi automatizzati o predizioni sul rendimento scolastico degli studenti, salvo esplicita autorizzazione del Titolare e nel rispetto delle garanzie previste dall'art. 22 GDPR.

- Ai sensi dell'art. 14 del Reg. UE 2024/1689 (EU AI Act), i sistemi AI ad alto rischio devono essere dotati di funzionalità di supervisione umana; il docente è tenuto a non eludere tali meccanismi.

- I sistemi AI classificati come «ad alto rischio» dall'EU AI Act (es. sistemi per la valutazione delle prestazioni scolastiche) richiedono una specifica valutazione d'impatto sulla protezione dei dati (DPIA, art. 35 GDPR) prima della messa in uso.

4.4. Trasparenza verso studenti e famiglie

- In attività didattiche sperimentali che prevedono l'impiego di AI (es. coding, simulazioni, robotica educativa, ambienti immersivi), i docenti devono informare preventivamente gli studenti e le famiglie, garantendo trasparenza sugli obiettivi e le modalità d'uso (art. 13 GDPR).

- I docenti devono favorire un uso consapevole e critico dell'AI da parte degli studenti, illustrandone potenzialità, limiti e rischi per la protezione dei dati, e vigilando che non venga impiegata per attività non autorizzate o in violazione delle norme sulla protezione dei dati personali.

4.5. Segnalazione di anomalie e tracciabilità

- È obbligatorio informare il Dirigente Scolastico, il Referente Privacy o il RPD/DPO in caso di anomalie, malfunzionamenti, allucinazioni o sospetti trattamenti impropri di dati da parte delle piattaforme AI utilizzate.

- I log e le attività svolte tramite piattaforme AI autorizzate devono essere conservati secondo le modalità previste dal Registro delle Attività di Trattamento dell'Istituto (art. 30 GDPR).

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

Indicazione operativa: In caso di dubbio sull'utilizzo di uno specifico strumento AI (es. se sia o meno autorizzato, se tratti dati personali), il docente deve astenersi dall'uso e contattare il RPD/DPO dell'Istituto prima di procedere.

5. Responsabilità degli incaricati del trattamento

Il Titolare del trattamento (Dirigente Scolastico) è sempre e comunque responsabile della corretta esecuzione degli adempimenti previsti dal D.Lgs. 196/2003 e dal Reg. UE 2016/679 (GDPR). Tuttavia, ai sensi dell'art. 83 GDPR, le responsabilità per l'inosservanza delle istruzioni impartite dal Titolare e/o dai Responsabili del trattamento possono riguardare anche gli incaricati che non rispettino o non adottino le misure necessarie.

Le violazioni dei principi di base del trattamento possono comportare sanzioni amministrative fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato annuo mondiale totale (art. 83, par. 5, GDPR). Fermo restando quanto sopra, la responsabilità disciplinare, civile e penale dell'incaricato rimane impregiudicata.

Nota normativa: Ai sensi dell'art. 2-quaterdecies, comma 2, del D.Lgs. 196/2003, la designazione dell'incaricato deve indicare l'ambito del trattamento consentito. L'incaricato che agisca al di fuori di tale ambito risponde a titolo personale dei danni eventualmente cagionati.

Luogo e data: _____

IL DIRIGENTE SCOLASTICO

Titolare del trattamento

Firmato digitalmente ai sensi del D.Lgs. 82/2005 (CAD)

Ricevuta di presa visione

Il/La sottoscritto/a _____, nella qualità di Docente presso l'Istituto Scolastico _____, dichiara di aver ricevuto e letto le presenti Linee Guida per il Trattamento e la Protezione dei Dati Personali e si impegna a rispettarle nell'esercizio delle proprie funzioni.

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

Presa visione in data: _____

Firma dell’Incaricato del trattamento: _____

Copia consegnata il: _____ | Copia agli atti dell’Istituto: ☐ Sì ☐ No

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

ALLEGATO E

LINEE GUIDA PER IL TRATTAMENTO E LA PROTEZIONE DEI DATI PERSONALI DEL PERSONALE AMMINISTRATIVO

INCARICATI DEL TRATTAMENTO – PERSONALE AMMINISTRATIVO

Versione 01 del 27/03/2026

per presa visione

QUADRO NORMATIVO DI RIFERIMENTO

Le presenti Linee Guida sono adottate ai sensi e per gli effetti della seguente normativa vigente:

Fonte normativa	Oggetto
Reg. UE 2016/679 (GDPR)	Regolamento generale sulla protezione dei dati personali
D.Lgs. 196/2003 (Codice Privacy)	Come modificato dal D.Lgs. 101/2018 di adeguamento al GDPR
D.Lgs. 101/2018	Adeguamento dell'ordinamento nazionale al Regolamento UE 2016/679
Reg. UE 2024/1689 (EU AI Act)	Regolamento europeo sull'intelligenza artificiale – in vigore dal 01/08/2024
Linee guida AGID – Misure minime ICT	Circolare AgID n. 2 del 18 aprile 2017 e s.m.i. per la sicurezza ICT nelle PA
Provvedimenti Garante Privacy	Provvedimenti e linee guida del Garante per la protezione dei dati personali
D.Lgs. 82/2005 (CAD)	Codice dell'Amministrazione Digitale – rilevante per le comunicazioni elettroniche e la firma digitale

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

Le presenti Linee Guida si applicano a tutto il personale amministrativo autorizzato al trattamento dei dati personali in qualità di incaricato ai sensi dell'art. 29 del Reg. UE 2016/679 e dell'art. 2-quaterdecies del D.Lgs. 196/2003. Ulteriori informazioni sulle modalità di trattamento e sulle misure di sicurezza adottate sono contenute nel Registro delle Attività di Trattamento (art. 30 GDPR).

DEFINIZIONI

Ai fini delle presenti Linee Guida si applicano le seguenti definizioni:

Dati personali:	Qualsiasi informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente, che può fornire informazioni sulle sue caratteristiche, abitudini, stile di vita, relazioni personali, stato di salute o situazione economica.	Art. 4, par. 1, n. 1, GDPR
Trattamento:	Qualunque operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali: raccolta, registrazione, organizzazione, strutturazione, conservazione, consultazione, elaborazione, modifica, estrazione, raffronto, utilizzo, comunicazione, diffusione, cancellazione, distruzione. I trattamenti su supporto cartaceo sono pienamente assoggettati al GDPR.	Art. 4, par. 1, n. 2, GDPR
Categorie particolari di dati:	Dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale; dati genetici, biometrici, relativi alla salute, alla vita sessuale o all'orientamento sessuale. In ambito scolastico sono particolarmente rilevanti i dati di salute degli alunni (DSA, BES, disabilità).	Art. 9 GDPR

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

Dati giudiziari:	Dati relativi a condanne penali e reati o a connesse misure di sicurezza (es. provvedimenti soggetti a iscrizione nel casellario giudiziale, liberazione condizionale, divieto/obbligo di soggiorno, misure alternative alla detenzione).	Art. 10 GDPR
Incaricato del trattamento:	Persona fisica che, sotto l'autorità del Titolare o del Responsabile del trattamento, tratta dati personali ed è autorizzata a farlo ai sensi della normativa nazionale.	Art. 29 GDPR; art. 2-quaterdecies D.Lgs. 196/2003
Violazione dei dati (Data Breach):	Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.	Art. 4, par. 1, n. 12, GDPR
RPD / DPO:	Responsabile per la Protezione dei Dati (Data Protection Officer): figura obbligatoria nelle istituzioni scolastiche pubbliche.	Artt. 37-39 GDPR

1. Misure operative per la gestione di documenti e archivi

Il personale amministrativo, in qualità di incaricato del trattamento, è tenuto a rispettare le seguenti misure nell'ambito della gestione documentale.

1.1. Custodia e conservazione degli atti

- Controllare e custodire gli atti e i documenti contenenti dati personali in modo da assicurarne l'integrità e la riservatezza.
- Conservare i dati trattati in apposito armadio assegnato, accertandosi della corretta funzionalità dei meccanismi di chiusura e segnalando tempestivamente eventuali anomalie al responsabile.

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

- I documenti e gli atti contenenti dati appartenenti a categorie particolari (dati sensibili) o dati giudiziari devono essere conservati in archivi chiusi a chiave (stanze, armadi, schedari, contenitori).
- Non lasciare incustoditi registri contenenti indirizzi, recapiti telefonici o altri dati del personale, degli studenti o dei genitori; non annotarne il contenuto su fogli di lavoro o agende accessibili a terzi.
- Non abbandonare la postazione di lavoro senza aver provveduto a custodire in luogo sicuro i documenti trattati.
- Segnalare tempestivamente al Responsabile la presenza di documenti incustoditi, provvedendo temporaneamente alla loro custodia.

1.2. Informativa, consenso e raccolta dati

- Prima di procedere alla raccolta e al trattamento dei dati, fornire sempre l'informativa all'interessato o alla persona presso cui si raccolgono i dati, ai sensi degli artt. 13-14 GDPR.
- Consegnare, quando necessario, il modulo per il consenso e ricevere il modello opportunamente firmato dall'interessato o da chi lo rappresenta legalmente.
- Procedere alla raccolta dei dati con la massima cura, verificando l'esattezza dei dati (principio di esattezza, art. 5, par. 1, lett. D), GDPR).
- Accedere esclusivamente ai dati personali la cui conoscenza sia strettamente necessaria per lo svolgimento delle funzioni e dei compiti affidati e per le finalità indicate nel provvedimento di incarico (principio di minimizzazione, art. 5, par. 1, lett. C), GDPR).

1.3. Comunicazione e verifica dell'identità

- Non fornire telefonicamente, via fax o via e-mail dati e informazioni relativi a terzi senza specifica autorizzazione del Titolare.
- Non fornire dati agli stessi interessati senza aver prima accertato con certezza la loro identità.
- Qualora giungano richieste telefoniche di dati da parte dell'Autorità Giudiziaria o degli organi di polizia, richiedere l'identità del chiamante e richiamare al numero ufficiale dell'Ente per avere la certezza sull'identità del richiedente.

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

- Nella comunicazione di dati appartenenti a categorie particolari, adottare procedure che garantiscano la sicurezza e la riservatezza delle informazioni, anche mediante tecniche di pseudonimizzazione o anonimizzazione ove applicabili.

Nota normativa: La pseudonimizzazione e la minimizzazione dei dati sono principi cardine del GDPR (artt. 5 e 25). L'accesso ai dati da parte di Autorità Giudiziaria e Forze di Polizia avviene secondo procedure specifiche; il personale non è tenuto a fornire dati telefonicamente senza verifica preventiva.

1.4. Gestione di copie e supporti fisici

- Effettuare copie fotostatiche o su supporto informatico esclusivamente di documenti per i quali si è autorizzati.
- Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti contenenti dati personali; assicurarsi che vengano distrutte mediante trituratore di documenti.
- I documenti cartacei non più utilizzati, specie se contenenti categorie particolari di dati o dati giudiziari, devono essere distrutti o comunque resi illeggibili prima di essere eliminati (tramite distruggi-documenti).
- Consegnare al personale o ai genitori/studenti documentazione inserita in buste non trasparenti; conservare i documenti ricevuti in apposite cartelline non trasparenti.
- Non consentire l'accesso a estranei o soggetti non autorizzati ad aree in cui sono conservati dati personali su supporto cartaceo o informatico.

1.5. Notifica delle violazioni dei dati personali

- Informare prontamente il Titolare del trattamento, il Referente Privacy o il RPD/DPO dell'Istituto di ogni circostanza idonea a determinare o che possa costituire una violazione dei dati personali (data breach), anche solo potenziale.
- La segnalazione deve avvenire senza ingiustificato ritardo, anche per consentire al Titolare di rispettare il termine di 72 ore per la notifica al Garante ove applicabile (art. 33 GDPR).
- Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si è stati espressamente autorizzati dal Titolare.

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

2. Misure operative per i trattamenti con supporto informatico

Le seguenti misure sono adottate in conformità alle Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni (Circolare AgID n. 2 del 18 aprile 2017 e s.m.i.) e ai provvedimenti del Garante per la protezione dei dati personali.

2.1. Gestione delle credenziali di accesso

- Per l’accesso al sistema informatico utilizzare esclusivamente le credenziali di accesso assegnate personalmente; è fatto divieto di comunicarle a qualsiasi altro incaricato.
- Adottare le necessarie cautele per assicurare la segretezza della password e la diligente custodia di ogni altro dispositivo di autenticazione informatica (badge, schede magnetiche, chiavi USB, token OTP, ecc.).
- Ove disponibile, attivare l’autenticazione a due fattori (MFA/2FA) per l’accesso ai sistemi informatici istituzionali.

2.2. Regole per la scelta della password

- Utilizzare una password di almeno dodici caratteri, contenente: almeno una lettera maiuscola, una lettera minuscola, un numero e un carattere speciale o segno di interpunzione.
- La password non deve contenere riferimenti facilmente riconducibili all’incaricato (nome, cognome, data di nascita, numero di telefono, ecc., propri o dei propri familiari).
- Conservare con cura la password, evitando di trascriverla su fogli posti in vista in prossimità del PC o sulla rubrica dell’ufficio.
- Cambiare la password almeno ogni novanta giorni per i sistemi che trattano categorie particolari di dati o dati giudiziari; almeno ogni sei mesi per gli altri sistemi.

2.3. Utilizzo delle postazioni di lavoro

- Ogni volta che si abbandoni la postazione di lavoro, anche temporaneamente, chiudere tutte le applicazioni in uso e attivare il blocco del sistema mediante password o screensaver con blocco automatico entro 5 minuti di inattività.
- Spegnere sempre il PC al termine della giornata lavorativa o in caso di assenze prolungate dalla postazione.

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

- Qualora si riscontrino anomalie nel funzionamento degli elaboratori o difformità nei dati trattati, darne immediata comunicazione al Titolare del trattamento e al responsabile tecnico.

2.4. Sicurezza informatica e antivirus

- Utilizzare il software antivirus istituzionale per la verifica di ogni documento trattato, di qualunque file scaricato da Internet o ricevuto tramite e-mail.
- Verificare sempre con l'antivirus il contenuto di qualunque supporto di memorizzazione esterno (chiavetta USB, disco esterno) prima di collegarlo alla postazione di lavoro.
- Assicurarsi che il software antivirus sia aggiornato; segnalare tempestivamente al responsabile tecnico eventuali impossibilità di aggiornamento.
- Non installare software non autorizzato sulle apparecchiature informatiche dell'Istituto.

2.5. Piattaforme digitali e lavoro a distanza

- Utilizzare esclusivamente le piattaforme identificate e approvate dall'Istituto come sicure e nominate responsabili del trattamento, in particolare per attività lavorative in modalità agile (smart working) o a distanza.
- L'utilizzo di dispositivi personali (BYOD – Bring Your Own Device) per il trattamento di dati personali istituzionali è consentito solo previa autorizzazione scritta del Titolare del trattamento e nel rispetto delle relative policy istituzionali.
- Verificare sempre la corretta modifica e/o cancellazione di dati su documenti, cartelle o informazioni condivise (double check), al fine di evitare modifiche o cancellazioni non intenzionali.

2.6. Comunicazioni via e-mail

- Nelle comunicazioni via e-mail assicurarsi di non usare impropriamente il campo CC (copia conoscenza): qualora sia necessario tutelare la riservatezza degli indirizzi e-mail dei destinatari, utilizzare il campo CCN (copia conoscenza nascosta).
- Verificare accuratamente l'indirizzo dei destinatari prima di inviare messaggi contenenti dati personali in allegato o nel corpo del messaggio.
- Non aprire allegati di cui non sia certa la provenienza; segnalare al responsabile tecnico eventuali tentativi di phishing o accessi non autorizzati.

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

Nota normativa: L'invio di e-mail con dati personali a destinatari sbagliati o l'uso improprio del campo CC costituisce una potenziale violazione dei dati personali (data breach) soggetta agli obblighi di notifica ex art. 33 GDPR. Il Garante ha sanzionato istituzioni per invio indiscriminato di e-mail con dati personali in CC anziché CCN.

3.Utilizzo di strumenti basati su Intelligenza Artificiale

La presente sezione è redatta in conformità al Regolamento UE 2016/679 (GDPR), al Reg. UE 2024/1689 (EU AI Act, in vigore dal 1° agosto 2024) e alle indicazioni del Garante per la Protezione dei Dati Personali in materia di intelligenza artificiale.

Nota normativa: Il Regolamento UE 2024/1689 (EU AI Act) è entrato in vigore il 1° agosto 2024. I divieti assoluti si applicano dal 2 febbraio 2025; le norme sui sistemi AI ad alto rischio si applicheranno dal 2 agosto 2026. I sistemi AI per la valutazione automatizzata di studenti e personale rientrano tra i sistemi ad alto rischio (Allegato III).

3.1. Autorizzazione e conformità

- È consentito utilizzare esclusivamente strumenti e servizi di intelligenza artificiale (es. chatbot, assistenti virtuali, sistemi di analisi automatica, generatori di testo) preventivamente autorizzati dall'Istituto e contrattualizzati come responsabili del trattamento o sub-responsabili, ai sensi dell'art. 28 GDPR.
- Prima di autorizzare l'uso di uno strumento AI, il Titolare del trattamento (Dirigente Scolastico) deve verificarne la conformità al GDPR e, ove applicabile, all'EU AI Act.

3.2. Protezione dei dati nei sistemi AI

- È vietato inserire dati personali, dati appartenenti a categorie particolari (art. 9 GDPR) o dati giudiziari (art. 10 GDPR) in strumenti di intelligenza artificiale pubblici o non approvati dall'Istituto (es. chatbot pubblici, assistenti AI online non contrattualizzati).
- L'uso di piattaforme AI con dati personali è consentito solo se preventivamente autorizzato dall'Istituto. In tali casi:
- devono essere trattati esclusivamente i dati strettamente necessari (principio di minimizzazione, art. 5, par. 1, lett. c), GDPR);
- il trattamento deve essere documentato nel Registro delle Attività di Trattamento (art. 30 GDPR);
- devono essere adottate misure di sicurezza adeguate e proporzionate al rischio;

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

- il fornitore del servizio AI deve essere contrattualizzato come Responsabile del trattamento ex art. 28 GDPR.
- In caso di utilizzo di sistemi AI autorizzati, l'incaricato deve limitarsi a trattare solo i dati strettamente necessari alla finalità lavorativa.

3.3. Supervisione umana e verifica degli output

- Ogni output generato dall'AI (es. bozze di comunicazioni, risposte automatiche, elaborazione dati, traduzioni) deve essere considerato una bozza e sottoposto a verifica umana prima di essere utilizzato in documenti ufficiali o comunicazioni esterne. L'AI non sostituisce il giudizio professionale dell'operatore.
- Ai sensi dell'art. 14 del Reg. UE 2024/1689 (EU AI Act), i sistemi AI ad alto rischio devono essere dotati di funzionalità di supervisione umana; il personale amministrativo è tenuto a non eludere tali meccanismi.

3.4. Divieto di profilazione e decisioni automatizzate

- Non è consentito utilizzare sistemi di AI per profilazioni, valutazioni o decisioni automatizzate sugli interessati (studenti, genitori, personale) senza espressa autorizzazione del Titolare e senza le garanzie previste dall'art. 22 GDPR (diritto di non essere sottoposto a decisioni basate unicamente su trattamento automatizzato).
- I sistemi AI classificati come «ad alto rischio» dall'EU AI Act richiedono specifica valutazione d'impatto sulla protezione dei dati (DPIA, art. 35 GDPR) prima della messa in uso.

3.5. Informativa e consenso per uso AI

- Per attività amministrative o sperimentali che prevedono l'uso di AI, deve essere sempre fornita informativa preventiva agli interessati (art. 13 GDPR) e raccolto il consenso ove richiesto dalla normativa vigente.

3.6. Tracciabilità e segnalazione anomalie

- I log e le attività svolte tramite piattaforme AI autorizzate devono essere conservati secondo le modalità previste dal Registro delle Attività di Trattamento dell'Istituto (art. 30 GDPR).
- È obbligatorio segnalare al Dirigente Scolastico, al Referente Privacy o al RPD/DPO ogni anomalia tecnica, comportamento inatteso, errore, allucinazione o sospetto trattamento improprio di dati da parte di software basati su AI.

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

Nota normativa: La violazione dei divieti assoluti previsti dall'art. 5 dell'EU AI Act (es. sistemi di categorizzazione biometrica, riconoscimento delle emozioni in ambienti scolastici).

4. Responsabilità degli incaricati del trattamento

Il Titolare del trattamento (Dirigente Scolastico) è sempre e comunque responsabile della corretta esecuzione degli adempimenti previsti dal D.Lgs. 196/2003 e dal Reg. UE 2016/679 (GDPR).

Tuttavia, le responsabilità per l'inosservanza delle istruzioni impartite dal Titolare e/o dai Responsabili del trattamento possono riguardare anche gli incaricati che non rispettino o non adottino le misure necessarie. In particolare, ai sensi dell'art. 83 GDPR, le violazioni dei principi di base del trattamento possono comportare sanzioni amministrative fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato annuo mondiale totale.

Indicazione operativa: Le presenti istruzioni integrano e non sostituiscono le disposizioni di legge applicabili. In caso di dubbio su una specifica situazione, contattare il RPD/DPO dell'Istituto prima di procedere.

Luogo e data: _____

IL DIRIGENTE SCOLASTICO

Titolare del trattamento

Firmato digitalmente ai sensi del D.Lgs. 82/2005 (CAD)

Ricevuta di presa visione

Il/La sottoscritto/a _____, nella qualità di Personale Amministrativo presso l'Istituto Scolastico _____, dichiara di aver ricevuto e letto le presenti Linee Guida per il Trattamento e la Protezione dei Dati Personali e si impegna a rispettarle nell'esercizio delle proprie funzioni.

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

Presa visione in data: _____

Firma dell’Incaricato del trattamento: _____

Copia consegnata il: _____ | Copia agli atti dell’Istituto: ☐ Sì ☐ No

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

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