Ministero dell'istruzione e del merito
CENTRO PROVINCIALE ISTRUZIONE ADULTI
CPIA "Silver Sirotti" di FORLÌ – CESENA
Codice M.P.I. – FOMM09500N
C.F. - 92085980404
Sede amministrativa: Via E. Dandolo, n. 18– 47121 – FORLÌ (FC) Tel. 0543 34180
e-mail fomm09500n@istruzione.it *pec:*fomm09500n@pec.istruzione.it

Ai Docenti
Agli Alunni e ai Genitori/Tutori/Comunità
Al D.S.G.A
Al personale ATA
Agli Atti
Al Sito web

Circ n. 77 del 28/04/2025

Oggetto: DPIA (Data Protection Impact Assessment) per l'adozione di piattaforme cloud orientate alla fornitura del servizio di REGISTRO ELETTRONICO

In seguito a quanto indicato dalla nota MIM n.2773 del 04/04/2025 si dispone la pubblicazione del seguente DPIA rispettivamente *Valutazione di impatto sulla protezione dei dati* così come previsto dagli artt. 35 e 36 del GDPR.
Il presente testo è strutturato in quesiti e risposte.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

L'adozione degli strumenti della presente DPIA è finalizzata al perseguimento di un rilevante interesse pubblico e non si è ritenuto necessario richiedere un parere agli interessati. Qualora vi fossero suggerimenti da parte dell'utenza, l'amministrazione si impegna ad effettuare successivi aggiornamenti della presente DPIA che tengano conto delle stesse.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

La presente DPIA valuta l'impatto legato all'utilizzo del registro elettronico, inteso come sistema digitale integrato per la gestione di attività didattiche, comunicative e amministrative della scuola. Tale sistema consente agli utenti (studenti, docenti, personale scolastico e famiglie) l'accesso e l'interazione tramite dispositivi informatici come PC, tablet e smartphone, che possono essere sia di proprietà della scuola sia degli utenti stessi (secondo il modello BYOD - Bring Your Own Device).

Il registro elettronico supporta le attività didattiche quotidiane, la gestione di assenze, voti, comunicazioni scuola-famiglia e l'organizzazione interna delle diverse componenti scolastiche. Oltre alle attività educative, il sistema facilita le comunicazioni amministrative, organizzative e la gestione operativa degli organi collegiali, delle commissioni e del personale scolastico, ciascuno dotato di una casella di posta elettronica istituzionale assegnata dall'amministrazione.

Quali strumenti si vogliono adottare?

Il sistema adottato è un registro elettronico che consente a docenti, personale amministrativo, studenti e famiglie di accedere in modo differenziato, mediante credenziali individuali, alle seguenti funzionalità:

- Registrazione e consultazione di assenze, ritardi e giustificazioni degli studenti.
- Inserimento, gestione e consultazione delle valutazioni scolastiche (voti, giudizi intermedi e finali).
- Gestione di annotazioni, note disciplinari e osservazioni didattico-comportamentali.
- Comunicazioni ufficiali scuola-famiglia attraverso appositi strumenti integrati nel registro (avvisi, circolari, messaggistica interna).
- Archiviazione digitale dei documenti amministrativi e didattici obbligatori.

La scelta del registro elettronico deve essere fatta dalla scuola sulla base dei seguenti criteri:

- Rispetto rigoroso della normativa vigente sulla protezione dei dati personali (GDPR).
- Conformità alle direttive ministeriali e alle indicazioni contenute nella circolare del Ministero dell'Istruzione e del Merito nr. 2772 del 04/04/2025.
- Facilità di utilizzo per il personale scolastico, gli studenti e le famiglie.
- Sicurezza informatica elevata e tracciabilità degli accessi.
- Efficienza nella gestione e conservazione dei dati.
- Costo sostenibile per l'amministrazione scolastica.

Perché questa DPIA?

Questa DPIA viene redatta per adempiere alle prescrizioni previste dal Regolamento UE 2016/679 (GDPR) e in ottemperanza alla *circolare del Ministero dell'Istruzione Prot. 2773 del 4/4/2025* che raccomanda la valutazione d'impatto per specifici trattamenti di dati personali, tra cui quello connesso all'utilizzo del Registro Elettronico.

L'utilizzo del Registro è previsto dal citato art. 7, comma 31, del D.L. n. 95/2012, il quale dispone che «A decorrere dall'anno scolastico 2012-2013 le istituzioni scolastiche e i docenti adottano registri on line e inviano le comunicazioni agli alunni e alle famiglie in **formato elettronico**».

Inoltre, si è provveduto a verificare preventivamente che la piattaforma scelta per il Registro Elettronico fosse conforme agli standard tecnici richiesti dall'Agenzia per l'Italia Digitale (AgID) e attualmente gestiti dall'Agenzia per la Cybersicurezza Nazionale, requisito obbligatorio per l'uso di piattaforme cloud nella pubblica amministrazione.

Quali sono le finalità del trattamento?

Il trattamento dei dati personali tramite il Registro Elettronico ha le seguenti finalità specifiche, esplicite e legittime:

- **Gestione didattica:** registrazione e monitoraggio delle attività didattiche quotidiane, comprese assenze, presenze, ritardi e giustificazioni degli studenti.
- **Valutazione degli studenti:** inserimento, conservazione e comunicazione dei voti, giudizi, risultati delle prove scritte e orali e delle altre attività didattiche finalizzate alla valutazione formativa e sommativa degli alunni.
- **Comunicazione scuola-famiglia:** facilitazione e miglioramento dei processi comunicativi tra docenti, famiglie e studenti per garantire una tempestiva informazione riguardo alla situazione scolastica, eventi, attività, comunicazioni ufficiali e documenti necessari per il percorso scolastico.
- **Gestione amministrativa e documentale:** archiviazione, conservazione e gestione digitale di documenti amministrativi obbligatori (scrutini, pagelle, verbali degli organi collegiali, ecc.), conformemente agli obblighi previsti dalla normativa vigente in materia di archivistica.
- **Supporto alle attività degli organi collegiali:** utilizzo del registro elettronico per agevolare e documentare le attività istituzionali degli organi collegiali scolastici (Consigli di Classe, Collegio Docenti, Consiglio di Istituto, ecc.).
- **Adempimento di obblighi normativi:** assicurare la conformità alle disposizioni ministeriali e normative nazionali relative alla digitalizzazione e alla dematerializzazione dei registri scolastici obbligatori.

Le finalità sopra indicate sono svolte nell'ambito del perseguimento dell'interesse pubblico rilevante connesso alle attività di istruzione e formazione erogate dall'istituto scolastico, ai sensi dell'articolo 6, comma 1, lettera e) e dell'articolo 9, comma 2, lettera g) del GDPR.

È necessario richiedere il consenso per l'utilizzo della piattaforma?

In considerazione dell'interesse pubblico perseguito e delle disposizioni di legge che ne impongono l'uso (art. 7, comma 31, del D.L. n. 95/2012) non è necessario richiedere il consenso al trattamento da parte degli interessati. D'altronde la negazione del consenso, ove richiesto, impedirebbe alla scuola di conseguire le proprie finalità istituzionali ed assolvere le disposizioni di legge.

Ci sono standard applicabili al trattamento?

Primo riferimento relativo ai trattamenti in questione è costituito dal documento edito dall'European Data Protection Board (EDPD) intitolato ***"2022 Coordinated Enforcement Action Use of cloud-based services by the public sector"*** (link) nel quale sono indicate le misure di sicurezza e le azioni da intraprendere per garantire al meglio la protezione dati degli utenti durante l'utilizzo di piattaforme cloud. L'EDPD ha pubblicato in precedenza le ***"Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE"*** (link) che vengono in rilievo per il trasferimento di dati all'estero.

In relazione alla individuazione dei fornitori viene in rilievo la **circolare AGID n. 2 del 09/04/2018** (link) che dispone che le Pubbliche Amministrazioni possono avvalersi esclusivamente di servizi cloud abilitati da AGID (oggi attività demandata a Agenzia per la Cybersicurezza Nazionale – ACN).

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati personali oggetto di trattamento tramite il Registro Elettronico includono:

- **Dati anagrafici e identificativi** degli studenti (nome, cognome, codice fiscale, data e luogo di nascita, indirizzo, recapiti telefonici ed e-mail).
- **Dati anagrafici e di contatto** dei genitori o tutori degli studenti.
- **Dati relativi alla frequenza scolastica** (presenze, assenze, ritardi, giustificazioni).
- **Dati relativi alla valutazione scolastica** (voti, giudizi, esiti intermedi e finali, pagelle e documenti correlati).
- **Note e osservazioni didattico-comportamentali**, incluse eventuali note disciplinari o annotazioni relative al comportamento degli studenti.
- **Dati relativi a situazioni particolari**, ove necessari per legge o per ragioni di tutela dell'alunno (ad esempio, informazioni su disabilità, disturbi specifici dell'apprendimento (DSA), bisogni educativi speciali (BES), o dati sensibili relativi alla salute limitatamente a quanto necessario per gestire emergenze o specifiche attività scolastiche).
- **Documenti amministrativi digitalizzati** collegati alla gestione scolastica, quali verbali di scrutini, consigli di classe e organi collegiali, e altre comunicazioni ufficiali.

Il trattamento di tali dati è limitato esclusivamente alle informazioni strettamente necessarie per il raggiungimento delle finalità educative, amministrative e organizzative dell'istituto scolastico, nel rispetto del principio di minimizzazione previsto dal GDPR.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Il ciclo di vita dei dati personali trattati mediante il Registro Elettronico si compone delle seguenti fasi, che coinvolgono il personale scolastico, gli studenti e le famiglie, nonché i fornitori tecnici esterni attraverso piattaforme cloud certificate:

1. Raccolta iniziale dei dati

I dati degli studenti e delle loro famiglie vengono raccolti inizialmente tramite moduli digitali o cartacei predisposti dalla scuola (ad esempio: iscrizioni, anagrafica degli studenti, contatti familiari), o direttamente immessi nel sistema dal personale autorizzato della segreteria scolastica. Questi dati anagrafici e di contatto sono integrati e aggiornati nel Registro Elettronico dal personale scolastico abilitato.

2. Elaborazione e aggiornamento costante

Nel corso dell'anno scolastico, i dati vengono continuamente aggiornati mediante l'utilizzo quotidiano del Registro Elettronico da parte dei docenti (che registrano voti, presenze, assenze, annotazioni disciplinari e comunicazioni didattiche), del personale ATA e amministrativo (che gestisce informazioni amministrative e organizzative) e, ove previsto, direttamente da studenti e famiglie (giustificazioni e comunicazioni). L'accesso per l'elaborazione e l'aggiornamento avviene tramite credenziali individuali, differenziate per ruolo e livello autorizzativo, per garantire l'integrità e la riservatezza dei dati.

3. Conservazione e archiviazione digitale su piattaforme cloud certificate

Tutti i dati raccolti vengono memorizzati digitalmente in ambienti cloud, secondo uno schema misto che prevede:

- **Server gestiti direttamente dal fornitore del Registro Elettronico**: Il fornitore della piattaforma del Registro Elettronico, formalmente nominato "responsabile del trattamento", gestisce direttamente alcuni server proprietari sui quali vengono inizialmente registrati e temporaneamente conservati i dati. Questi server devono essere collocati in data center sicuri, conformi agli standard richiesti dall'Agenzia per la Cybersicurezza Nazionale (ex certificazione AgID), che definisce i requisiti tecnici minimi di sicurezza informatica per i servizi cloud utilizzabili dalla Pubblica Amministrazione.
- **Piattaforme cloud certificate**: Una parte consistente dei dati viene successivamente archiviata, conservata e protetta dal Responsabile del Trattamento presso suoi subResponsabili, mediante infrastrutture cloud certificate, i cui requisiti tecnici di sicurezza e affidabilità sono periodicamente verificati e validati dall'Agenzia per la Cybersicurezza Nazionale. Questa architettura cloud consente di garantire:
    - Alta disponibilità dei dati
    - Backup regolari con ridondanza geografica
    - Misure di sicurezza elevate, inclusi sistemi di crittografia, firewall, anti-malware e monitoraggio costante degli accessi e delle attività anomale.

La scuola ha stipulato un contratto dettagliato con il fornitore che chiarisce le responsabilità reciproche in materia di sicurezza e protezione dei dati, ai sensi dell'art. 28 GDPR.

4. Consultazione differenziata e sicura

L'accesso ai dati archiviati nel Registro Elettronico è rigorosamente regolato da un sistema di autenticazione basato su identità digitali e credenziali individuali, definite e gestite dall'amministratore di sistema della scuola e dal fornitore del servizio. Nello specifico, sono previste politiche precise di controllo degli accessi per:

- **Docenti e personale scolastico** (accesso completo o limitato in base ai dati necessari per svolgere le proprie mansioni).
- **Studenti e famiglie** (accesso solo ai dati di propria pertinenza).
- **Personale amministrativo e dirigenziale** (accesso completo per finalità istituzionali).
- **Personale tecnico e amministratori di sistema** (accesso limitato per finalità manutentive e tecniche, rigorosamente tracciato e monitorato).

Ogni accesso e operazione sui dati è registrato in log digitali, che consentono l'audit e il controllo delle attività svolte.

5. Conservazione a lungo termine e cancellazione sicura:

I dati conservati nel Registro Elettronico rimangono archiviati per il periodo obbligatorio previsto dalla normativa vigente relativa agli archivi scolastici (normalmente da 5 a 10 anni, o periodi superiori in casi particolari previsti dalla legge).

Al termine del periodo di conservazione previsto, i dati possono essere:

- **Trasferiti in archivi digitali a lungo termine** gestiti dalla scuola secondo le indicazioni ministeriali in materia di archivistica digitale.
- **Eliminati in maniera definitiva e irreversibile** dalle piattaforme cloud e dai server gestiti dal fornitore del servizio, attraverso procedure tecniche certificate che ne garantiscano la non recuperabilità.

Questi processi vengono gestiti in stretto coordinamento tra la scuola (titolare del trattamento) e il fornitore del Registro Elettronico (responsabile del trattamento), in modo tale da garantire la sicurezza, l'integrità e la conformità normativa in ogni fase del ciclo di vita dei dati.

Per quanto riguarda la cancellazione dei dati, la Circolare n° 44 del 19/12/2005 della Direzione Generale per gli archivi - "Archivi delle Istituzioni Scolastiche" prescrive la conservazione di elaborati delle prove scritte, grafiche e pratiche per almeno un anno, e la conservazione di documentazione campione un anno ogni dieci (si suggerisce per omogeneità di non scartare i documenti relativi agli anni scolastici terminanti in 7/8, es. '67/'68, '77/'78 etc.).

Quali sono le risorse di supporto ai dati?

Il Registro Elettronico è una piattaforma digitale basata su tecnologie cloud certificate dall'Agenzia per la Cybersicurezza Nazionale (ACN), che consentono la gestione centralizzata e sicura dei dati relativi alla vita scolastica degli studenti. In particolare, la piattaforma utilizzata si avvale di risorse tecnologiche caratterizzate dai seguenti aspetti:

- **Server cloud certificati**

  I dati sono archiviati e gestiti principalmente su infrastrutture cloud qualificate e certificate dall'ACN, conformi ai requisiti minimi di sicurezza informatica definiti dall'Agenzia stessa per le piattaforme utilizzate dalla Pubblica Amministrazione. In alcuni casi, la gestione dei dati può prevedere l'uso di server collocati al di fuori dell'Unione Europea; in tali situazioni, la scuola verifica preventivamente che siano garantite misure di protezione dei dati equivalenti a quelle previste dal GDPR.

- **Strumenti di accesso multipiattaforma**

  Il Registro Elettronico è progettato per essere utilizzato attraverso una vasta gamma di dispositivi (computer, tablet, smartphone), indipendentemente dal sistema operativo (Windows, macOS, Android, iOS, Linux). L'accesso al servizio avviene tramite applicazioni dedicate e browser web, che offrono un ambiente sicuro e compatibile con gli standard previsti dalla normativa vigente.

- **Gestione e archiviazione sicura dei dati:**

  Le piattaforme cloud utilizzate consentono la conservazione sicura e protetta dei dati personali degli studenti e delle famiglie, delle valutazioni, delle annotazioni didattiche e disciplinari, nonché delle comunicazioni scuola-famiglia. Tutte le operazioni di archiviazione e consultazione dei dati avvengono tramite connessioni cifrate e sistemi di autenticazione basati su credenziali individuali e rigorosamente monitorate tramite appositi sistemi di logging.

- **Backup automatici e continuità operativa:**

  Sono previsti backup automatici periodici dei dati archiviati sul Registro Elettronico, in modo da garantire la possibilità di ripristino rapido delle informazioni in caso di malfunzionamenti o incidenti. Queste misure assicurano la disponibilità continua dei dati, requisito fondamentale per la regolare operatività della scuola.

- **Protezione avanzata e monitoraggio degli accessi:**

  Le piattaforme cloud sono dotate di strumenti avanzati per il monitoraggio continuo delle attività degli utenti (log degli accessi, controllo degli eventi anomali), antivirus, firewall e sistemi di rilevamento e prevenzione delle intrusioni informatiche.

In sintesi, le risorse tecnologiche che supportano il trattamento dei dati nel Registro Elettronico sono selezionate specificamente per garantire massimi standard di sicurezza, affidabilità e conformità con la normativa GDPR e con i requisiti dell'Agenzia per la Cybersicurezza Nazionale.

Trasferimento dati extra UE

È previsto il trasferimento di dati al di fuori dell'Unione europea?

No. Non è previsto un trasferimento di dati al di fuori dell'Unione Europea. Tale trasferimento potrà in ogni caso avvenire esclusivamente verso Paesi per i quali la Commissione Europea ha adottato una **decisione di adeguatezza** ai sensi dell'articolo 45 del Regolamento UE 2016/679 (GDPR).

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

Nei casi in cui il Registro Elettronico preveda il trasferimento dei dati personali al di fuori dell'Unione Europea, tale trasferimento avviene unicamente verso Paesi terzi per cui la Commissione Europea ha riconosciuto formalmente un livello di protezione adeguato tramite apposita decisione di adeguatezza.
Pertanto, la protezione dei dati personali trasferiti è garantita da standard equivalenti a quelli previsti dal GDPR, senza necessità di ulteriori misure supplementari. L'Istituto verifica preventivamente che i fornitori del servizio rispettino rigorosamente questa condizione tramite specifici accordi contrattuali.

Principi Fondamentali Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Sì. Il trattamento dei dati personali effettuato attraverso il Registro Elettronico risponde a scopi chiaramente **determinati, espliciti e legittimi**, in linea con le funzioni istituzionali dell'Istituzione scolastica. In particolare, i dati vengono trattati per:

- adempiere agli **obblighi normativi** previsti in materia di istruzione e formazione, compresa la tenuta dei registri scolastici obbligatori in formato digitale (presenze, voti, note, comunicazioni scuola-famiglia, ecc.);
- garantire una gestione **efficiente, trasparente e sicura** del percorso scolastico degli studenti;
- consentire un flusso informativo **puntuale e tracciabile** tra scuola, studenti, famiglie e organi collegiali;
- supportare l'attività **didattica, organizzativa e amministrativa** della scuola in conformità alle direttive del Ministero dell'Istruzione.

Le finalità del trattamento sono conformi all'articolo 6, paragrafo 1, lettera e) del GDPR ("esecuzione di un compito di interesse pubblico") e, ove vengano trattati dati particolari, all'articolo 9, paragrafo 2, lettera g) ("motivi di interesse pubblico rilevante").
Il trattamento è dunque proporzionato rispetto agli scopi perseguiti e strettamente necessario per il funzionamento ordinario dell'Istituto, senza eccedere rispetto a quanto richiesto per lo svolgimento dei compiti scolastici.

Quali sono le basi legali che rendono lecito il trattamento?

Il trattamento dei dati tramite registro elettronico scolastico si fonda su specifiche basi giuridiche previste dal GDPR e dalla normativa italiana. In primo luogo, esso è necessario per lo svolgimento di compiti di interesse pubblico e l'esercizio di pubblici poteri di cui è investita la scuola, ai sensi dell'art. 6 par. 1 lett. e del GDPR. La gestione di registri di classe, voti, assenze e comunicazioni rientra infatti nelle funzioni pubbliche essenziali proprie delle istituzioni scolastiche (educazione, istruzione), come riconosciuto anche dal Garante per la Protezione dei Dati Personali. Inoltre, sussiste un obbligo legale: la normativa italiana richiede espressamente l'adozione del registro elettronico. In particolare, l'art. 7, co. 31 del D.L. 95/2012 (conv. in L. 135/2012) dispone che *"A decorrere dall'anno scolastico 2012-2013 le istituzioni scolastiche e i docenti adottano registri on line…"*.
Tale obbligo normativo fornisce una base giuridica ulteriore ai sensi dell'art. 6 par. 1 lett. **c** GDPR (adempimento di un obbligo di legge).
Per effetto di queste basi legali, **non è richiesto il consenso** di studenti o genitori per i trattamenti effettuati attraverso il registro elettronico. Il consenso risulterebbe inappropriato, in quanto il mancato assenso impedirebbe alla scuola di perseguire le proprie finalità istituzionali. Questo approccio è confermato anche dal Garante Privacy, che in un proprio provvedimento ha escluso la necessità di raccogliere il consenso per trattamenti connessi a funzioni pubbliche scolastiche. I dati personali degli studenti (e delle famiglie o del personale) vengono dunque trattati lecitamente sulla base di compiti di interesse pubblico e obblighi normativi, nel rispetto del Regolamento (UE) 2016/679 e del D.Lgs. 196/2003 (Codice Privacy) così come modificato dal D.Lgs. 101/2018.
Nel caso in cui attraverso il registro elettronico vengano trattati **dati appartenenti a categorie particolari** (art. 9 GDPR), ad esempio informazioni sullo **stato di salute** o su **necessità educative speciali** degli alunni (come diagnosi DSA/BES o disabilità certificate), si applicano ulteriori basi giuridiche e cautele. Tali dati possono essere trattati perché necessari per assolvere agli obblighi ed esercitare i diritti specifici in ambito scolastico e socio-educativo (art. 9 par. 2 lett. **b** e **g** GDPR), in conformità al diritto nazionale che tutela l'inclusione scolastica. Norme come la L. 104/1992 (assistenza a studenti con disabilità) e la L. 170/2010 (disturbi specifici dell'apprendimento) impongono alla scuola misure di supporto personalizzato: il trattamento dei relativi dati sanitari risulta quindi lecito per motivi di rilevante interesse pubblico, sulla base di disposizioni di legge. In ogni caso, la scuola adotterà misure adeguate per proteggere questi dati sensibili, attenendosi all'art. 2-sexies del D.Lgs. 196/2003 e alle autorizzazioni generali del Garante Privacy, che permettono tali trattamenti nell'ambito educativo. Riassumendo, il registro elettronico opera in un contesto normativo chiaro: le finalità sono determinate da leggi e regolamenti di settore, il GDPR fornisce le basi di liceità (artt. 6 e 9) e la legittimità del trattamento è garantita dal perseguimento di fini istituzionali scolastici in conformità alla legge.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

Il principio di minimizzazione dei dati (art. 5 par.1 lett. c GDPR) è pienamente rispettato nell'uso del registro elettronico scolastico. Ciò significa che vengono raccolti e trattati solo i dati personali adeguati, pertinenti e limitati a quanto necessario per il perseguimento delle finalità didattiche e amministrative della scuola. In concreto, il registro elettronico contiene principalmente informazioni essenziali: dati anagrafici degli studenti e dei genitori, dati di contatto, indicazioni sulle presenze/assenze, voti, valutazioni, note disciplinari e comunicazioni scolastiche. Non vengono invece trattati dati o contenuti che esulano dallo scopo educativo. Il Ministero dell'Istruzione stesso ha ribadito che il registro deve escludere funzionalità non attinenti alle attività scolastiche, come ad esempio iniziative commerciali, marketing, giochi o contenuti non didattici, pubblicità etc., in quanto non necessari all'organizzazione e gestione dell'attività educativa. Questo assicura che la piattaforma del registro elettronico sia orientata esclusivamente agli scopi istituzionali (didattica, informazione alle famiglie, comunicazioni di servizio) e non raccolga dati superflui rispetto a tali scopi.

Particolare attenzione è posta al trattamento di eventuali dati sensibili (categorie particolari) degli studenti, quali informazioni su salute, origini etniche, convinzioni o condizioni familiari delicate, benché la maggior parte di tali dati non debba comparire nel registro quotidiano. Se per ragioni istituzionali fosse necessario registrare informazioni di natura speciale (es. l'indicazione di un piano didattico personalizzato per un alunno con DSA/BES o note relative alla salute per tutelare lo studente), questi dati verrebbero trattati solo se strettamente indispensabili e con garanzie aggiuntive. I docenti e il personale sono istruiti ad applicare in modo rigoroso i principi di adeguatezza, pertinenza e minimizzazione proprio in presenza di dati particolari. Tali informazioni dovranno essere inserite solo nei casi obbligatori (ad esempio per attuare misure di supporto previste dalla legge) e comunque utilizzando accorgimenti di tutela: ad esempio evitando diciture palesi visibili a tutti, limitando l'accesso solo ai soggetti autorizzati, o ricorrendo alla pseudonimizzazione/codificazione quando possibile. È infatti fondamentale che dati come lo stato di salute o i bisogni educativi speciali non siano diffusi o accessibili indiscriminatamente attraverso il registro. A tal proposito, il Garante Privacy ha sanzionato la pubblicazione in chiaro, su un registro elettronico, dell'elenco di alunni contrassegnati con le sigle *BES/DSA/H* (indicative di bisogni speciali e disabilità), evidenziando che ciò costituisce un'illecita comunicazione di dati sanitari. Questo caso esemplare conferma l'obbligo di massima cautela: eventuali annotazioni su condizioni particolari degli studenti devono essere gestite in modo riservato, evitando riferimenti identificativi visibili ad utenti non autorizzati (ad es. altri genitori o studenti).

In sintesi, la scuola dovrà garantire che saranno oggetto di trattamento solo i dati strettamente necessari alle finalità del registro elettronico. Verranno adottate policy interne affinché i docenti carichino o inseriscano nel sistema solo informazioni pertinenti all'andamento scolastico. Ogni dato superfluo o eccedente (cioè non richiesto per finalità didattiche, valutative o amministrative) non verrà raccolto, e in ogni caso il registro non verrà utilizzato come repository generico di documenti personali al di fuori del contesto scolastico. Attraverso configurazioni tecniche e formazione del personale, si garantisce inoltre che i dati eventualmente sensibili (es. indicazioni sullo stato di salute per diete speciali, o dati giudiziari se mai trattati) siano tutelati da misure adeguate e non risultino visibili oltre quanto strettamente necessario. In questo modo il principio di minimizzazione è rispettato: dati adeguati e rilevanti, nulla di eccedente rispetto alle finalità educative e di trasparenza verso le famiglie.

I dati sono esatti e aggiornati?

La procedura di raccolta e conservazione dei dati prevede la creazione spesso cooperativa di contenuti, perciò potrebbe presentarsi il caso in cui un elaborato venga deliberatamente modificato da eventuali collaboratori durante il suo processo di creazione. In tal caso, è preferibile utilizzare uno strumento che tenga traccia delle modifiche apportate alla documentazione, tramite soluzioni di backup e di cronologia delle modifiche (versioning).

Una volta terminati, gli elaborati delle prove scritte, grafiche e pratiche possono essere considerati documentazione amministrativa oggetto di valutazione scolastica. Per questo motivo, essa non può essere modificata o cancellata neppure su richiesta degli interessati per il periodo prescritto dalla legge e comunque funzionale alla corretta valutazione da parte dei docenti e del consiglio di classe.

Qual è il periodo di conservazione dei dati?

I dati personali registrati nel sistema del registro elettronico vengono conservati in conformità al principio di limitazione della conservazione (art. 5 par.1 lett. e GDPR) e alle normative archivistiche italiane applicabili alle istituzioni scolastiche. In generale, i dati sono conservati per il tempo strettamente necessario allo svolgimento delle finalità didattiche e amministrative correnti, dopodiché vengono archiviati o cancellati a seconda della loro natura e degli obblighi di legge. La scuola, essendo pubblica amministrazione, è soggetta alle regole del Sistema Archivistico Nazionale: molti documenti scolastici devono essere conservati a lungo o permanentemente per motivi storici e amministrativi (come previsto dal D.Lgs. 42/2004 *Codice dei beni culturali* e dalla Circolare MIBACT n.44/2005 sugli archivi scolastici). Di seguito si dettagliano i tempi di conservazione in base alle diverse categorie di dati (didattici, disciplinari, amministrativi), tenendo conto delle indicazioni della Direzione Generale degli Archivi e delle esigenze pratiche di gestione:

- **Dati didattici (andamento scolastico):** comprendono voti, assenze, programmi svolti, giudizi, esiti degli scrutini ed esami, registri di classe e del docente. Si tratta di informazioni costituenti la documentazione ufficiale dell'attività didattica, che la normativa archivistica classifica tra gli atti da conservare a lungo termine. In particolare, i risultati scolastici e gli atti degli scrutini/esami finali fanno parte del fascicolo personale dell'alunno, il quale deve essere conservato *illimitatamente* (permanentemente) dall'istituto. Ciò garantisce che anche a distanza di molti anni la scuola possa certificare carriere scolastiche, voti finali, diplomi e frequenza degli studenti. Analogamente, i registri di classe e i registri dei voti sono considerati documenti ufficiali: al termine dell'anno scolastico essi vengono chiusi e archiviati come atti amministrativi, con conservazione potenzialmente senza scadenza, salvo diverse indicazioni di scarto. In pratica, dunque, i dati didattici essenziali vengono mantenuti negli archivi della scuola a tempo indeterminato, diventando parte dell'archivio storico scolastico. Questo non significa però che restino *attivamente* disponibili sulla piattaforma per sempre: dopo la conclusione dell'anno o del ciclo scolastico, tali dati vengono generalmente esportati e conservati in sistemi di conservazione digitale a norma o in copie archivistiche, venendo rimossi dall'area operativa del registro. Restano accessibili solo tramite richiesta formale (es. richiesta di certificati, copia di documenti) e non più visibili nell'area utente quotidiana. Eventuali elaborati prodotti dagli studenti (compiti, tesine, verifiche) che non abbiano rilevanza ai fini della valutazione finale vengono conservati solo finché necessari per la didattica e poi eliminati; ad esempio, i compiti non più utili vengono cancellati alla fine dell'anno scolastico, a meno che servano per attività didattiche pluriennali. Al contrario, i compiti in classe e gli elaborati utilizzati per valutazioni ufficiali possono essere conservati per un periodo minimo (es. almeno un anno scolastico) e poi anch'essi destinati allo scarto, salvo campionature storiche richieste da norme archivistiche.
- **Dati disciplinari:** riguardano note di demerito, provvedimenti disciplinari, sospensioni o altri eventi sanzionatori annotati sul registro. Anche in questo caso occorre distinguere tra le semplici annotazioni quotidiane e gli atti disciplinari formali. Le annotazioni disciplinari minori (es. note sul registro di classe per comportamento) vengono tenute per la durata dell'anno scolastico di riferimento e considerate parte integrante del registro di classe annuale. Al termine dell'anno, il registro (comprensivo di tali note) viene archiviato come documento storico. Tali dati non hanno ulteriore utilizzo attivo oltre l'anno in cui sono stati raccolti e, una volta archiviati, non sono più consultabili salvo necessità legali. I provvedimenti disciplinari ufficiali (es. sospensioni deliberate dal Consiglio di istituto, richiami formali) vengono inseriti nel fascicolo personale dell'alunno e, in quanto parte della carriera dello studente, seguono la regola di conservazione illimitata prevista per tali fascicoli. Di norma, dunque, le sanzioni importanti restano agli

atti in via permanente. Tuttavia, trascorso un certo tempo dalla fine della carriera scolastica dello studente, la loro consultazione è limitata solo a fini amministrativi interni o storici. In applicazione del GDPR, la scuola evita di conservare *attivamente* nel registro online informazioni disciplinari oltre il periodo necessario: dopo la conclusione del ciclo scolastico, queste informazioni vengono archiviate offline. Qualora taluni atti disciplinari non abbiano rilevanza storica o amministrativa, l'istituto potrà proporne lo scarto archivistico seguendo le procedure di legge (ad esempio dopo alcuni anni dalla fine della carriera dello studente), previa autorizzazione dell'Autorità archivistica competente. Ogni eliminazione definitiva di documenti contenenti dati disciplinari, infatti, deve avvenire con il nulla osta della Soprintendenza Archivistica, a garanzia che non si distrugga materiale ancora necessario o di valore storico.

- **Dati amministrativi:** includono i dati personali e burocratici relativi all'iscrizione e alla gestione amministrativa degli studenti e del personale. Ad esempio, dati anagrafici, certificati di iscrizione, modulistica, autorizzazioni, nonché comunicazioni scuola-famiglia o documenti contabili. Per questa eterogenea categoria si applicano tempi di conservazione diversificati in base alla tipologia di documento. I dati anagrafici di base degli studenti e i documenti di carriera (es. domanda di iscrizione, certificati, pagelle) confluiscono anch'essi nel *fascicolo personale* dello studente, che – come detto – va conservato permanentemente. Ciò risponde a obblighi legali di archiviazione e permette alla scuola di documentare in qualsiasi momento il percorso scolastico di ciascun alunno. Altri dati amministrativi, invece, hanno un uso temporaneo e vengono eliminati al termine della loro utilità. Ad esempio, comunicazioni quotidiane alle famiglie (circolari, avvisi inviati tramite il registro) e informazioni logistiche (orari, prenotazioni di colloqui) sono conservati solo finché necessari per l'anno scolastico in corso e non oltre. Allo scadere dell'anno, tali dati di breve termine vengono rimossi dal sistema del registro (o comunque resi inaccessibili agli utenti) in mancanza di ulteriori necessità. Analogamente, eventuali consensi o autorizzazioni facoltative raccolte tramite il registro (es. adesione a progetti, autorizzazione uscite) vengono conservati per la durata del progetto o attività e poi cancellati quando non più necessari, salvo che la scuola debba conservarne copia cartacea/digitale secondo norme interne di protocollo. I dati contabili (es. pagamento di contributi scolastici volontari, gestione mensa) seguono le normative di contabilità pubblica: tipicamente, documenti di pagamento e ricevute vanno conservati per 10 anni o per il periodo stabilito dal massimario di conservazione, dopodiché possono essere eliminati su autorizzazione. I dati del personale (che compaiono eventualmente nel registro, ad es. firma del docente sulle lezioni) sono anch'essi soggetti a conservazione nei fascicoli personali del personale docente/ATA, spesso a tempo indeterminato per il loro valore giuridico. In definitiva, il registro elettronico adotta una politica di conservazione dati conforme al GDPR e alle disposizioni archivistiche italiane: i dati restano nel sistema attivo solo per il tempo necessario alla gestione didattica e amministrativa corrente, mentre per il lungo periodo vengono trasferiti in archiviazione certificata oppure cancellati se non più utili. La conservazione a lungo termine riguarda solo quei dati/documenti previsti dalle norme (es. fascicoli degli alunni, registri, verbali ufficiali), i quali vengono custoditi a norma di legge anche oltre la permanenza dello studente a scuola. Tutti gli altri dati vengono eliminati o anonimizzati una volta esaurite le finalità originarie, rispettando i tempi minimi obbligatori. L'istituto documenta queste tempistiche nel proprio *Manuale di gestione documentale* e nel Registro dei Trattamenti, così da dimostrare la conformità al principio di limitazione della conservazione. In caso di necessità di scarto (distruzione) di documenti contenenti dati personali, si procederà secondo la procedura autorizzativa prevista dal Codice dei Beni Culturali, assicurando così che nessun dato venga conservato più a lungo del dovuto, ma nemmeno cancellato prima che sia lecito farlo. Questo bilanciamento garantisce che il registro elettronico conservi i dati per il periodo corretto, in modo lecito e trasparente, tutelando sia le esigenze istituzionali sia i diritti degli interessati.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati vengono informati del trattamento precedentemente all'inizio dello stesso, tramite somministrazione di informativa ex Art. 13 del Reg. UE 206/679. L'informativa viene somministrata a personale, alunni e genitori degli stessi tramite una combinazione più completa possibile dei canali disponibili alla scuola, che includono, a titolo esemplificativo e non esaustivo:

- L'utilizzo delle modalità di comunicazione scuola famiglia messe a disposizione dal registro elettronico.
- La pubblicazione nella sezione privacy del sito web istituzionale;
- L'invio della stessa agli indirizzi mail indicati da genitori, alunni e dipendenti (si sottolinea anche qui l'importanza di utilizzare il campo CCN per l'invio, che a differenza del campo "a" e "cc" consente l'invio a più destinatari senza condividerne gli indirizzi);

Gli interessati sono informati sulle modalità di trattamento e sui possibili rischi associati anche in relazione al possibile trasferimento dei dati personali al di fuori dell'UE. Durante il processo didattico stesso verranno forniti agli studenti le conoscenze necessarie ad un utilizzo consapevole della piattaforma anche per garantire la protezione dei dati personali propri e altrui.

Ove applicabile: come si ottiene il consenso degli interessati?

Il consenso non costituisce base legale del trattamento e non viene richiesto agli interessati.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati possono sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati posso sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati posso sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

I trattamenti operati dal fornitore devono essere effettuati solo tramite previa nomina dello stesso quale Responsabile del Trattamento ai sensi dell'Art. 28 del GDPR, dove sono specificati gli obblighi del fornitore individuato responsabile del trattamento. Per quanto riguarda la valutazione dell'affidabilità dei servizi presi in esame, si deve necessariamente provvedere a verificare che il fornitore sia inserito nel c.d. Cloud Marketplace gestito dall'agenzia all'**Agenzia per la Cybersicurezza nazionale** nell'elenco SaaS (Software as a Service), e a verificarne periodicamente la permanenza nell'elenco suddetto**.**

Rischi

Misure esistenti o pianificate

Crittografia

Il fornitore cripta i dati per impostazione predefinita. I dati sono protetti con più livelli di sicurezza che includono tecnologie di crittografia all'avanguardia, come i protocolli HTTPS e Transport Layer Security. Non si è ritenuto opportuno adottare tecniche di cifrature client side.

Controllo degli accessi logici

L'accesso alle funzionalità delle piattaforme utilizzate deve essere regolato da un sistema di attivazione di account con permessi specifici, protetti da password, attivabili e disattivabili dall'amministratore del software (il D.S. o un suo delegato). Si rileva a questo proposito che le circolari MIM 4588 dell'8/11/2023 e 4717 del 12/09/2024, richiamando l'art. 24, comma 4, del D.L. n. 76/2020 e dall'art. 64 del CAD raccomandano che l'accesso al Registro avvenga mediante l'utilizzo di identità digitali (i.e., SPID, CIE, eIDAS).

Archiviazione

Tutta la documentazione relativa all'attività Istituzionale dell'Amministrazione è regolata dalla normativa vigente in materia di archiviazione nella pubblica amministrazione, contenente indicazioni specifiche per la pubblica istruzione.

Minimizzazione dei dati

I dati vengono trattati e archiviati in forma minima, per quanto previsto dalla normativa vigente. I dati sensibili sono limitati a quelli strettamente necessari.

Lotta contro il malware

I sistemi scolastici sono protetti da malware con modalità di protezione sia hardware che software (firewall e antivirus). È inoltre opportuno fornire agli utilizzatori delle linee guida sull'utilizzo sicuro delle risorse elettroniche e digitali, che includano le istruzioni per una efficace lotta al malware.

Backup

Sebbene il fornitore debba predisporre le soluzioni tecniche atte a garantire la reperibilità e l'integrità dei dati caricati sulla piattaforma è opportuno che la scuola valuti ulteriori misure di salvaguardia dei dati e dei documenti.

Manutenzione

Viene effettuata regolarmente una attività di manutenzione nei confronti dei sistemi hardware e software scolastici. Il fornitore della piattaforma cloud garantisce il corretto funzionamento e la sicurezza dei propri sistemi.

Politica di tutela della privacy

L'amministrazione ha messo in atto una serie di misure orientate all'adeguamento della stessa alla normativa vigente. I dipendenti sono stati nominati incaricati al trattamento ai sensi dell'Art. 2-quaterdecies del D.Lgs. 196/2003, per l'esercizio delle loro funzioni. Specifiche istruzioni e regolamenti sono stati emessi dall'istituto per la tutela dei dati personali nell'uso delle piattaforme cloud.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

L'amministrazione ha emesso un regolamento interno per la gestione dei data breach, al cui interno sono specificate le modalità di gestione degli incidenti che coinvolgono dati personali. Emessa anche una circolare per il personale che deve essere in grado di riconoscere un data breach quando interviene e che deve sapere cosa fare all'occorrenza.

Valutazione del rischio

La presente sezione analizza i rischi connessi all'utilizzo del Registro Elettronico in ambito scolastico, tenendo conto delle sue specificità: il Registro è usato anche per le comunicazioni ufficiali scuola-famiglia (messaggistica interna, notifiche, avvisi), è integrato con la segreteria digitale dello stesso fornitore e contiene dati personali sia comuni che particolari (ad es. note su studenti con BES – Bisogni Educativi Speciali – o DSA, certificazioni sanitarie necessarie). Di seguito vengono descritti i principali rischi individuati – accesso illegittimo ai dati, modifiche indesiderate dei dati e perdita di dati – insieme alle relative fonti, misure di mitigazione e stima del livello di rischio residuo.

1. Accesso illegittimo ai dati

Descrizione del rischio: possibilità che soggetti non autorizzati (esterni o interni) accedano ai dati del registro elettronico. Nel contesto scolastico ciò significa esposizione indebita di informazioni su studenti, famiglie o personale (es. voti, assenze, comunicazioni riservate) e, in casi particolari, di dati sensibili come informazioni su BES/DSA o dati sanitari. Un accesso illecito comporterebbe violazione della riservatezza e potenziali impatti sui diritti degli interessati (es. divulgazione non autorizzata di dati personali).

Fonti di rischio:

- **Errori o negligenze:** credenziali deboli o condivise, dispositivi lasciati incustoditi con sessioni aperte, invio di dati al destinatario sbagliato.
- **Abusi o usi impropri:** accesso intenzionale oltre le proprie autorizzazioni (es. personale scolastico che consulta registri di classi non di competenza).
- **Vulnerabilità tecniche:** attacchi informatici (es. hacker, malware) al sistema del fornitore o della scuola, phishing teso a carpire le credenziali degli utenti, falle di sicurezza nell'integrazione con la segreteria digitale.

Misure di mitigazione:

- **Controllo accessi e autenticazione forte:** account individuali per ogni utente (dirigenti, docenti, personale, genitori) con password complesse e rinnovo periodico e/o autenticazione mediante SPID, CIE, eIDAS.
- **Profilazione degli utenti e principio di minima autorizzazione:** definizione di ruoli e permessi granulari (es. docenti vedono solo dati delle proprie classi, i genitori solo i dati dei propri figli, il personale di segreteria solo le sezioni pertinenti) in modo da limitare l'accesso ai soli dati necessari per ciascun profilo.
- **Cifratura e sicurezza delle comunicazioni:** utilizzo di connessioni sicure (HTTPS/TLS) per l'accesso al registro e la messaggistica interna; eventuale cifratura dei dati particolarmente sensibili a riposo, così che anche in caso di accesso illegittimo non risultino immediatamente leggibili.
- **Misure di sicurezza del fornitore (art. 28 GDPR):** contratto con il fornitore del Registro che preveda adeguate misure tecniche e organizzative (firewall, sistemi di rilevamento intrusioni, antivirus, aggiornamenti tempestivi) per proteggere l'infrastruttura cloud e la segreteria digitale integrata da accessi non autorizzati.
- **Formazione e consapevolezza:** istruzioni al personale scolastico e agli utenti sull'importanza di custodire le credenziali, riconoscere tentativi di phishing e rispettare le policy di sicurezza (es. divieto di account condivisi).
- **Minimizzazione dei dati:** limitare la raccolta e l'inserimento nel Registro di dati particolari solo ai casi strettamente necessari (es. inserire note sanitarie solo quando indispensabile), così da ridurre l'impatto in caso di eventuale accesso illecito.

Gravità del danno: 2/4 (bassa-moderata) se riguarda dati personali comuni; 4/4 (elevata) se sono coinvolti dati particolari, considerata la natura sensibile delle informazioni che potrebbero essere esposte.

Probabilità residua: 2/4 (bassa-moderata) dopo l'adozione delle misure sopra descritte, grazie a controlli di accesso stringenti e monitoraggi continui (pur permanendo il rischio di errore umano o attacco sofisticato).

Livello di rischio residuo: 4/16 per i dati comuni; 8/16 per dati particolari (calcolato come Gravità × Probabilità). Tali valori indicano un rischio basso-moderato e moderato rispettivamente, tenuto sotto controllo attraverso le misure implementate.

2. Modifiche indesiderate dei dati

Descrizione del rischio: possibilità che i dati registrati (voti, assenze, valutazioni, note disciplinari o informazioni su bisogni educativi speciali) vengano alterati in modo non autorizzato o errato. Nel Registro Elettronico scolastico questo rischio può manifestarsi sia come errore accidentale (es. un docente inserisce un voto o un'assenza in modo sbagliato, oppure una segreteria scolastica sovrascrive dati per un problema di sincronizzazione con il sistema integrato) sia come manomissione dolosa (es. un soggetto che, avendo ottenuto accesso al sistema, modifica deliberatamente voti o comunicazioni). Una modifica indesiderata compromette l'integrità delle informazioni, con potenziali effetti su studenti e famiglie: valutazioni inaccurate, comunicazioni ufficiali errate o gestione scorretta di situazioni particolari (ad esempio, se venissero alterati o rimossi riferimenti a BES/DSA o indicazioni sanitarie necessarie, gli studenti coinvolti potrebbero non ricevere le dovute attenzioni o supporti).

Fonti di rischio:

- **Errori umani:** imprecisioni nell'inserimento manuale dei dati da parte di docenti o personale di segreteria (es. digitazione errata di voti o assenze, scambio di record tra omonimi), scarsa formazione sull'uso corretto del Registro, oppure errori di configurazione nel sistema integrato registro- segreteria che causano aggiornamenti sbagliati.
- **Abusi interni:** modifiche intenzionali non autorizzate da parte di personale interno (es. un docente o amministrativo che altera dati al di fuori delle proprie competenze, magari per favoritismi o altre irregolarità).
- **Vulnerabilità o attacchi:** exploit sul software del Registro che consentano a terzi di alterare informazioni (ad esempio, un attacco informatico che inserisca o modifichi dati nel sistema), oppure infezioni malware che corrompano i dati; malfunzionamenti nell'integrazione col sistema di segreteria digitale (es. bug che sovrascrivono campi con valori errati). Di particolare rilievo il rischio associato alla sottrazione delle credenziali del registro elettronico da parte di alunni che hanno così la possibilità di modificare le valutazioni.

Misure di mitigazione:

- **Accesso mediante SPID/CIE:** configurazione del Registro per consentire l'accesso mediante SPID o CIE. Tale misura si ritiene necessaria prioritariamente per il personale scolastico per il quale deve essere impedito l'acceso mediante altre credenziali rilasciate dalla scuola. L'accesso con SPID e CIE dovrà essere adottato anche per gli utenti scolastici gestendo eventuali situazioni di difficoltà dovute all'assenza di identità SPID o CIE o di digital divide.
- **Regole di autorizzazione e tracciamento:** configurazione del Registro in modo che ciascun utente possa modificare solo i dati di propria competenza (principio di segregazione dei compiti);
- **Validazione e controlli applicativi:** il software del Registro effettua controlli di validità sui dati inseriti (es. range plausibili per voti e assenze, conferma esplicita prima di modifiche massicce); eventuali discrepanze tra Registro e segreteria digitale vengono segnalate per verifica (meccanismi di sync-check sull'integrità tra sistemi integrati).
- **Procedure organizzative:** doppio controllo su dati critici – ad esempio, validazione da parte del dirigente scolastico o di un secondo operatore per modifiche eccezionali (come variazioni di voti finali già pubblicati); istituzione di processi per la correzione di errori segnalati da docenti o genitori (es. richiesta di rettifica di un'assenza erroneamente segnata).
- **Backup e versioning dei dati:** salvataggi periodici e copie di sicurezza dei dati del Registro; possibilità di recuperare lo stato precedente di dati importanti (ad es. ripristino di un backup o annullamento di modifiche entro un certo periodo) così da annullare gli effetti di manomissioni o errori gravi.
- **Formazione e sensibilizzazione:** addestrare il personale all'utilizzo corretto del Registro Elettronico e della segreteria digitale integrata, sottolineando l'importanza dell'accuratezza dei dati e delle procedure di verifica (riducendo gli errori di distrazione); diffondere linee guida su come rilevare e segnalare tempestivamente eventuali anomalie nei dati.
- **Clausole contrattuali col fornitore:** assicurare che il fornitore del sistema preveda misure per mantenere l'integrità dei dati (ad es. protezioni contro operazioni non valide e test approfonditi sulle funzionalità di sincronizzazione registro-segreteria), nonché un supporto tecnico rapido per risolvere bug o incoerenze che possano causare modifiche indesiderate.

Gravità del danno: 3/4 (moderata) per dati comuni inesatti (impatti su valutazioni scolastiche, trasparenza e fiducia delle famiglie); 4/4 (elevata) se vengono coinvolti dati particolari o informazioni critiche (un'alterazione su questi potrebbe ledere diritti allo studio di studenti fragili o causare trattamenti inadeguati).

Probabilità residua: 2/4 (bassa-moderata) dopo le misure di mitigazione. Gli errori umani occasionali restano possibili, ma con formazione e controlli l'incidenza di modifiche non corrette e non intercettate si riduce sensibilmente. Le possibilità di manomissione dolosa o tecniche sono contenute da rigorosi controlli di accesso e audit**.**

Livello di rischio residuo: 6/16 per scenari con dati comuni; 8/16 se coinvolti dati particolari. Questo punteggio (Gravità × Probabilità) indica un rischio sotto controllo: l'integrità dei dati del Registro è generalmente garantita, fermo restando che ogni segnalazione di errore o anomalia va gestita tempestivamente secondo le procedure previste.

3. Perdita di dati

Descrizione del rischio: possibilità che i dati del Registro Elettronico vadano persi o risultino temporaneamente/permanentemente indisponibili. Ciò può avvenire a causa di guasti tecnici, cancellazioni involontarie o maliziose, oppure eventi avversi (es. attacchi ransomware che cifrano i database). Nel contesto del registro scolastico integrato con la segreteria, una grave perdita di dati potrebbe significare l'irreperibilità di informazioni essenziali: dai voti e assenze degli studenti, ai documenti amministrativi digitalizzati, fino alle comunicazioni ufficiali inviate. Le conseguenze includono interruzioni del servizio (impossibilità per docenti e famiglie di accedere al registro), disagi per l'attività didattica e amministrativa, e potenziali danni per gli interessati (es. mancanza di traccia di percorsi educativi speciali o potenziali errori nelle valutazioni finali).

Fonti di rischio:

- **Errori/incidenti tecnici:** guasto dei server o dei dispositivi di storage del fornitore, malfunzionamenti software che causino corruzione dei database, errori nella sincronizzazione tra Registro e segreteria che portino alla cancellazione errata di record; eventi accidentali come blackout elettrici o incendi che colpiscano i data center.
- **Errori umani:** cancellazione involontaria di dati da parte di operatori (es. errata eliminazione di registri di classe o messaggi), configurazioni sbagliate (ad es. periodi di conservazione errati che rimuovono dati anzitempo), mancato salvataggio di informazioni inserite.
- **Attacchi malevoli:** ransomware o altri malware che rendono inaccessibili i dati (cifratura o distruzione), azioni dolose interne o esterne volte a cancellare o sabotare archivi (es. un alunno che elimina intenzionalmente dati cruciali).
- **Vulnerabilità infrastrutturali:** mancanza di adeguati backup o piani di disaster recovery da parte del fornitore; dipendenza dall'infrastruttura cloud del fornitore senza misure di business continuity (un singolo punto di errore potrebbe propagarsi all'intero sistema integrato registro+segreteria).

Misure di mitigazione:

- **Accesso mediante SPID/CIE:** configurazione del Registro per consentire l'accesso mediante SPID o CIE. Tale misura riduce i rischi di perdita dati dovuti ad accessi abusivi a seguito di sottrazione di credenziali (ad esempio perdita dati dovute ad alunni che accedono al registro con le credenziali sottratte al docente)
- **Backup regolari e disaster recovery:** implementazione di backup automatizzati e frequenti di tutti i dati del Registro e della segreteria digitale integrata, conservati in luoghi/sistemi separati. Predisposizione di un piano di disaster recovery da parte del fornitore, per poter ripristinare in tempi rapidi i servizi e i database in caso di incidente grave (come previsto dall'art. 32 GDPR – integrità e disponibilità).
- **Redundancy e alta affidabilità:** uso di infrastrutture cloud robuste con server ridondati (cluster, mirroring dei dati) in modo che un singolo guasto non comporti perdita definitiva; sistemi di alimentazione di emergenza e protezioni fisiche nei data center per prevenire perdite da eventi ambientali.
- **Conservazione distribuita delle informazioni critiche:** possibilità di esportare periodicamente i dati rilevanti (es. backup locali dei registri di classe, copie dei verbali o degli archivi di valutazione) da conservare presso la scuola, così da avere un'ulteriore garanzia in caso di indisponibilità prolungata del servizio online.
- **Sicurezza informatica preventiva:** aggiornamento costante dei sistemi e antivirus/antimalware attivi per prevenire infezioni; formazione rivolta agli utenti sul rischio ransomware (non aprire allegati sospetti, etc.); controllo di integrità sui dati sincronizzati tra Registro e segreteria per rilevare subito eventuali anomalie.
- **Procedure di recovery e continuità operativa:** test periodici di ripristino dai backup per verificare l'efficacia delle copie di sicurezza; pianificazione di procedure manuali emergenziali (ad esempio utilizzo temporaneo di registri cartacei o fogli di calcolo) per garantire la continuità della didattica e delle comunicazioni in caso di downtime del sistema digitale.
- **Minimizzazione e conservazione adeguata:** mantenere nei sistemi solo i dati necessari per il tempo necessario, evitando accumuli e archivi obsoleti (che aumentano il volume di informazioni a rischio in caso di perdita); trasferire periodicamente dati storici chiusi su supporti di archivio sicuri, così che l'eventuale perdita riguardi solo il periodo corrente e non l'intero storico.

Gravità del danno: 3/4 (moderata) per dati comuni non disponibili (impedimento temporaneo alla regolare attività didattica e amministrativa, con disagi gestibili); 4/4 (elevata) se la perdita coinvolge dati particolari o documenti insostituibili (es. piani educativi personalizzati o certificati medici andati persi, con potenziali ricadute sul supporto agli studenti o violazione di obblighi di conservazione).

Probabilità residua: 1/4 (bassa) grazie alle contromisure adottate. Con backup e piani di recovery efficaci, la probabilità di una perdita permanente di dati è molto ridotta; rimane possibile qualche disponibilità temporaneamente limitata (es. breve fermo sistema) ma gestita dai piani di continuità.

Livello di rischio residuo: 3/16 per i dati comuni; 4/16 per dati particolari. Si tratta di un rischio residuo basso: l'adozione di robuste misure di backup e continuità operativa garantisce che anche in caso di incidente i dati possano essere recuperati e l'impatto sugli interessati rimanga limitato.

Valutazione gravità del rischio

A seguito dell'analisi condotta abbiamo quindi ricavato le seguenti valutazioni:

Rischio	Entità del danno	probabilità	Gravità del rischio
Accesso illegittimo ai dati	2-4	2	4-8
Modifiche indesiderate ai dati	3-4	2	6-8
Perdita di dati	3-4	1	3-4

Quelle condotte sono delle valutazioni sommarie volte a stimare l'entità dei rischi connessi all'uso della piattaforma. L'analisi condotta evidenzia come i rischi, valutati in relazione alla probabilità ed alla entità del danno, sono al di sotto di una soglia accettabile considerate le misure di contenimento del rischio già adottate. Non si ritiene quindi di dover fare analisi più approfondite sui rischi volte a stimare questi in modo più puntuale e alla ulteriore riduzione del rischio residuo.

Conclusioni

Gli organi collegiali del nostro istituto hanno deliberato l'adozione del Registro Elettronico al fine di garantire una gestione più efficiente e trasparente delle attività didattiche e amministrative, favorendo la comunicazione istituzionale con le famiglie e migliorando la qualità complessiva del servizio scolastico offerto agli studenti e alla comunità scolastica. L'impiego di questo strumento risponde agli obblighi di digitalizzazione previsti dalla normativa vigente e rappresenta un significativo passo avanti nella modernizzazione dell'amministrazione scolastica, promuovendo contemporaneamente un utilizzo consapevole e responsabile delle tecnologie digitali, anche in riferimento ai rischi legati al trattamento dei dati personali.

Il Registro Elettronico adottato è stato selezionato sulla base di criteri precisi quali affidabilità tecnica, sicurezza informatica, facilità d'uso per il personale scolastico e per le famiglie, nonché il rispetto delle norme sulla protezione dei dati personali (GDPR e normativa nazionale di riferimento). La piattaforma scelta è integrata con il sistema di segreteria digitale fornito dallo stesso produttore, assicurando una gestione coerente e protetta di tutti i dati relativi agli studenti e al personale scolastico.

Con riferimento specifico al trattamento dei dati, la presente valutazione d'impatto ha analizzato approfonditamente i rischi legati all'utilizzo del Registro Elettronico, identificando in particolare tre categorie di rischi principali:

- Accesso illegittimo ai dati
- Modifica indesiderata dei dati
- Perdita accidentale o dolosa dei dati

L'analisi condotta ha permesso di stabilire che, nonostante l'impossibilità intrinseca di eliminare completamente ogni tipo di rischio connesso all'uso di strumenti digitali, le misure tecniche e organizzative adottate dalla scuola e dal fornitore del servizio garantiscono un livello adeguato di sicurezza e consentono di mantenere tali rischi entro soglie di accettabilità chiaramente definite.

Nello specifico, il rischio di accesso illegittimo ai dati – inclusi i dati particolari eventualmente registrati, come informazioni su bisogni educativi speciali (BES/DSA) o certificazioni sanitarie – potrà essere mitigato efficacemente con identificazione degli utenti con SPID e CIE, in particolare per i dipendenti (docenti e personale amministrativo). Altre misure di mitigazione del rischio sono individuate nella formazione continua del personale, crittografia delle comunicazioni e definizione chiara dei ruoli e delle autorizzazioni. Allo stesso modo, il rischio di modifiche indesiderate o perdita di dati è ridotto a livelli minimi attraverso procedure di backup regolari, soluzioni di archiviazione affidabili, sistemi di versionamento dei dati e controlli sistematici sull'integrità delle informazioni trattate.

Particolare attenzione è stata posta all'eventuale trasferimento di dati personali verso Paesi al di fuori dell'Unione Europea. Qualora tale trasferimento fosse previsto o inevitabile (ad esempio nel caso in cui il fornitore della piattaforma utilizzi infrastrutture cloud internazionali), la scuola ha stabilito che tale trasferimento avvenga esclusivamente verso Stati per i quali la Commissione Europea abbia formalmente riconosciuto un livello di protezione dei dati equivalente a quello europeo (decisione di adeguatezza ex art. 45 GDPR). In ogni caso, il Registro Elettronico prescelto dispone di certificazioni ufficiali, ed è presente nel Cloud Marketplace dell'Agenzia per la Cybersicurezza Nazionale, che garantisce periodicamente il rispetto di alti standard tecnici e organizzativi nella gestione dei dati personali.

In conclusione, sulla base della presente valutazione di impatto, si ritiene che l'utilizzo del Registro Elettronico da parte dell'Istituto garantisca un trattamento lecito e sicuro dei dati personali degli studenti, delle famiglie e del personale scolastico, nel pieno rispetto delle disposizioni contenute nel Regolamento UE 2016/679 (GDPR), delle normative nazionali di riferimento e delle indicazioni tecniche emanate dalle autorità competenti. L'Istituto scolastico si impegna, infine, a mantenere un costante monitoraggio dei trattamenti effettuati e delle misure di sicurezza adottate, provvedendo ad aggiornare tempestivamente la presente DPIA qualora emergano variazioni significative nel contesto normativo, tecnologico o organizzativo.

Forlì, lì 28/04/2025

La Dirigente Scolastica
Tiziana Fiorino

(firma autografa sostituita a mezzo stampa ai sensi dell'art.3, comma 2 del decreto legislativo n. 39/1993)

Validatore:

DPO: S&L – Ing. Enrica Marsiglio