

Privacy Policy

ProvisionIQ Ltd – How We Collect, Use, and Protect Your Data

Document	Privacy Policy
Company	ProvisionIQ Ltd (“ProvisionIQ”, “we”, “us”, “our”)
ICO Reg. No.	ZC156305
Version	2.0
Effective Date	July 2026
Next Review	July 2027
Applies to	All users of the ProvisionIQ platform and website, including school staff, parents/carers, LA officers, and data subjects
Compliance	UK GDPR · Data Protection Act 2018 · PECR · Cyber Essentials Plus · ISO 27001:2022
Replaces	Version 1.0 (May 2026)

Your Privacy Matters

ProvisionIQ processes personal data about children and adults in the education sector, including sensitive special educational needs information, health records, safeguarding flags, and multi-agency referral data. We take this responsibility seriously. This Privacy Policy explains who we are, what data we collect, why we collect it, how we protect it, and what rights you have. If you have any questions, contact our Data Protection Officer: dpo@provisioniq.org

Version	Date	Summary of Changes
1.0	May 2026	Initial policy published on platform launch
2.0	July 2026	Added: DPIA disclosure statement; safeguarding record retention period; AI data use rules; MIS integration disclosure; corrected DPO contact to single address (dpo@provisioniq.org); parent portal data flows; equity analytics data use clarification

1. Who We Are and How to Contact Us

ProvisionIQ Ltd is a private limited company registered in England and Wales (Company No. 17240497). We develop and operate ProvisionIQ, a software-as-a-service platform that enables schools, local authorities, and multi-agency teams to create, manage, and analyse Individual Support Plans (ISPs) for pupils with special educational needs and disabilities (SEND), alongside EHCPs, multi-agency collaboration, parent co-production, and SEND compliance reporting.

Role	Detail
Data Controller	ProvisionIQ Ltd is the Data Controller for data we collect directly (e.g. account registration, website analytics, marketing enquiries, support tickets)
Data Processor	ProvisionIQ Ltd acts as Data Processor for all pupil and client data uploaded to or generated on the platform by our school/LA customers (who are the Data Controllers for that data)
Registered address	2 Houlder Drive, Howden, DN14 7ZU
Data Protection Officer	Liam Wheldon · dpo@provisioniq.org
ICO Registration	No. ZC156305 — registered under the Data Protection Act 2018
Supervisory authority	Information Commissioner's Office (ICO), Wycliffe House, Water Lane, Wilmslow, SK9 5AF — ico.org.uk

Single DPO Contact Point

All data protection queries, Subject Access Requests, rights requests, and complaints should be directed to dpo@provisioniq.org. This is the sole DPO contact address for all data protection matters. We aim to acknowledge all requests within 3 business days and respond fully within one calendar month.

2. Scope of This Policy

This Privacy Policy applies to:

- School staff (teachers, SENCOs, teaching assistants, senior leaders) who use the ProvisionIQ platform under a school or trust licence
- Parents and carers who access the Parent Portal (via authenticated Keycloak account or signed share-link)
- Local Authority officers and specialist professionals who access the platform
- Pupils and young people whose data is recorded on the platform (as data subjects)
- Visitors to our website (provisioniq.org) and marketing contacts
- Prospective customers, partners, and advisors

Controller vs Processor

When a school or local authority subscribes to ProvisionIQ, they are the Data Controller for the pupil and staff data they upload to or generate on our platform. ProvisionIQ processes that data only on their instructions, as their Data Processor. Schools and LAs must have their own Privacy Notices explaining to pupils, parents, and staff how their data is processed on the ProvisionIQ platform. ProvisionIQ provides a model Data Processor Addendum (DPA) and a model Privacy Notice supplement for this purpose. For our own directly collected data (account details, website analytics, support tickets), ProvisionIQ is the Data Controller and this Privacy Policy applies directly.

3. The Data We Collect

3.1 Data Collected About Platform Users (School Staff, LA Officers)

Category	Data Items	Source
Account data	Full name, job title, email address, school/organisation, hashed password (Keycloak-managed)	Provided on registration
Profile data	Profile picture (optional), phone number, role/permissions level	Provided by user or school administrator
Usage data	Login timestamps, features accessed, pages viewed, session duration, IP address, device type	Automatically collected
Support data	Support ticket content, screenshots, error logs, correspondence with our support team	Provided when contacting support
Communications	Emails, survey responses, webinar registrations, marketing preferences	Provided directly or via forms

3.2 Data Collected About Pupils (Processed on Behalf of Schools)

As Data Processor, ProvisionIQ handles the following categories of pupil data on behalf of our school and LA customers:

Category	Examples	Sensitivity Level
Identifying data	Full name, date of birth, UPN (Unique Pupil Number), gender, photograph	Standard personal data
Educational data	Year group, class, school, MIS reference number, attendance record (via MIS integration)	Standard personal data

SEND classification	SEND category (SEN Support or EHCP/ISP), primary and secondary area of need, SEND history	Sensitive — education records
ISP / support plan content	Needs taxonomy, outcomes (SMART targets), interventions, review notes, evidence uploads, observation logs	Sensitive — SEND records
Health and medical data	Medical conditions, diagnoses, medication, therapy requirements where recorded in ISP	Special category — health data (UK GDPR Art. 9)
Safeguarding data	Concern flags, safeguarding notes, referral records (where platform feature is used); immutable; access restricted to DSL and above	Special category — safeguarding (high sensitivity)
Family and contact data	Parent/carers names, contact details, relationship to pupil, co-production contributions via Parent Portal	Standard personal data
Assessment and progress data	Baseline assessments, progress metrics, external specialist reports (where uploaded), AI-assisted provision suggestions (always labelled as such)	Sensitive — education records
MIS-integrated data	Pupil identifiers, class and group data, attendance records received via direct MIS integration (read-only by default; only fields required for SEND provision retained)	Standard to sensitive personal data
Equity and analytics data	Aggregated data by gender, ethnicity, FSM status, EAL status — used only for school-level SEND equity reporting; never used for individual profiling or any purpose beyond supporting SEND provision	Sensitive (ethnicity: special category where individually identifiable)

Data Minimisation

ProvisionIQ is designed on a data minimisation principle. We only collect and hold the data that is genuinely necessary for the delivery of ISP management and SEND support services. Schools can configure which fields are mandatory and which are optional. Sensitive fields (health data, safeguarding data) are access-controlled by role. MIS integration data is filtered at ingestion — only fields required for SEND provision are retained; raw MIS payloads are not stored.

3.3 Data Collected via Our Website

Data Type	Detail
Contact enquiries	Name, email, organisation, message content — collected via our contact form

Demo requests	Name, email, job title, school/trust name, phone number (optional)
Newsletter sign-ups	Email address and subscription preferences
Website analytics	Anonymised page views, referral sources, device type, session duration — via privacy-respecting analytics (no third-party tracking cookies without consent)
Cookies	See Section 6 for full cookie policy

4. How We Use Your Data — Lawful Bases

Under UK GDPR, we must have a lawful basis for processing personal data. The table below sets out our lawful bases for each type of processing activity.

Processing Activity	Lawful Basis	Detail
Providing the platform to licensed schools and LAs	Contract (Art. 6(1)(b)) — as Processor on behalf of the Controller	Processing is necessary to perform our contract with the school/LA; the school/LA's own lawful basis applies to pupil data
Creating and managing user accounts	Contract (Art. 6(1)(b))	Account data is necessary to provide platform access under the licence agreement
Sending service notifications (maintenance, security alerts, updates)	Legitimate interests (Art. 6(1)(f)) — essential service communications	We have a legitimate interest in keeping customers informed of matters affecting their use of the platform
Providing customer support	Contract (Art. 6(1)(b)) / Legitimate interests	Support is part of the contracted service; ticket data retained to improve service quality
Billing and invoicing	Contract (Art. 6(1)(b)) + Legal obligation (Art. 6(1)(c))	Necessary to perform the contract and comply with accounting law (Companies Act 2006, HMRC requirements)
Marketing communications (existing customers)	Legitimate interests (Art. 6(1)(f))	Soft opt-in under PECR; opt-out available at any time
Marketing communications (new prospects)	Consent (Art. 6(1)(a)) / PECR	Opt-in consent required for electronic marketing to individuals
Website analytics	Legitimate interests (Art. 6(1)(f)) — anonymised, privacy-respecting	Anonymised analytics only; no cross-site tracking; does not require consent when fully anonymised

Processing pupil SEND data on behalf of schools (as Processor)	Determined by the Controller (school/LA); typically Public Task (Art. 6(1)(e)) + substantial public interest (Art. 9(2)(g)) or vital interests	Schools must document their own lawful basis; ProvisionIQ processes only on their documented instructions
AI-assisted provision planning features	Determined by the Controller; ProvisionIQ's AI features are advisory only; no automated decisions are made; AI outputs always reviewed by a human professional	No AI feature makes a decision with legal or similarly significant effect for any individual pupil
Fraud prevention, security monitoring, and incident investigation	Legitimate interests (Art. 6(1)(f)) + Legal obligation	Security monitoring necessary to protect all users' data; mandatory under Cyber Essentials Plus and ISO 27001 obligations

5. Special Category Data

Special category data requires additional protection under UK GDPR Article 9. ProvisionIQ processes the following special category data on behalf of our school customers:

Special Category	How We Handle It
Health data (disabilities, diagnoses, medication, therapy)	Access-controlled by role; only accessible to authorised users with appropriate permissions; encrypted at rest (AES-256) and in transit (TLS 1.3); not included in any export without explicit authorisation; not used as input to AI features without DPO approval and school consent
Safeguarding data (concern flags, referral records, safeguarding notes)	Immutable audit trail; access restricted to Designated Safeguarding Lead and above; cannot be deleted by any platform user (including school administrators); records generate automatic alerts to nominated safeguarding leads; retained for the period specified in Section 10
Data revealing racial or ethnic origin (equity analytics)	Collected only where necessary for SEND equity provision planning; processed in aggregate for school-level reporting; access-controlled; not used for individual profiling; not shared with any third party for any commercial purpose

The additional condition relied upon by schools for processing special category pupil data is typically: Substantial Public Interest — Education, Training and Educational Support (Schedule 1, paragraph 35, Data Protection Act 2018). Schools must document this in their own DPIA and Privacy Notice.

6. Data Protection Impact Assessments (DPIAs)

ProvisionIQ conducts Data Protection Impact Assessments (DPIAs) for all processing activities that are likely to result in high risk to individuals, as required by UK GDPR Article 35. Given the nature of our platform — processing special category data about children at scale — DPIAs are a routine part of our development process, not an exception.

6.1 DPIA Triggers

A DPIA is conducted before launching or materially changing:

- Any new feature that processes special category pupil data (health, safeguarding, ethnicity)
- Any new AI or machine learning feature, regardless of whether it directly handles personal data
- Any new MIS integration or data pipeline that ingests pupil data from an external system
- Any new third-party sub-processor or AI provider that will process RESTRICTED data
- Any material change to data retention periods, data sharing arrangements, or access control structures
- Any new feature affecting the Parent Portal or multi-agency collaboration workspace

6.2 DPIA Availability to Data Controllers

ProvisionIQ recognises that schools and LAs, as Data Controllers, may need to sight our DPIAs to fulfil their own accountability obligations. We operate the following disclosure approach:

- Summary DPIA outputs (covering processing purpose, data categories, risks identified, and controls applied) are available to Data Controllers on request.
- Full DPIA documents are shared with Data Controllers under a confidentiality agreement where there is a legitimate need.
- Schools' DPOs are encouraged to contact dpo@provisioniq.org to request DPIA documentation relevant to their deployment.
- ProvisionIQ will proactively notify Data Controllers when a new DPIA is completed for a feature they are using.

7. Cookies and Tracking Technologies

Cookie Type	Detail
Strictly necessary	Session cookies required to keep you logged in and maintain platform security (Keycloak session management). Cannot be disabled — the platform does not function without them.
Functional	Remembers your preferences (display settings, notification preferences). Set only after login; no consent required under legitimate interests.

Analytics (first-party)	Privacy-respecting analytics to understand how the platform is used and improve it. Anonymised; no cross-site tracking; no fingerprinting. Consent not required when fully anonymised (ICO guidance).
Marketing/tracking	We do not use third-party marketing cookies or tracking pixels on the platform. Our public website uses a consent banner before setting any non-essential cookies.

You can manage cookie preferences via the cookie settings link in the platform footer. Blocking strictly necessary cookies will prevent you from logging in.

8. How We Share Your Data

ProvisionIQ does not sell your data or share it for advertising purposes. We share data only in the limited circumstances described below.

Recipient	Purpose and Basis
Other platform users (within your school/LA)	Sharing within the platform is controlled by role-based permissions set by your organisation's administrator. ProvisionIQ does not control which users within an organisation can access which data — that is the school's/LA's responsibility as Data Controller.
Multi-agency professionals (via Experts at Hand / MDT portal)	Where a school initiates a Targeted Plus referral or MDT collaboration, relevant pupil data is shared with the nominated professional within the secure platform workspace. The school, as Data Controller, authorises this sharing. ProvisionIQ enforces role-based access to ensure professionals see only the data they are authorised to see.
Parents and carers (via Parent Portal)	Parents access their own child's support plan data via the Parent Portal or signed share-link, as authorised by the school. ProvisionIQ does not share pupil data with parents beyond what the school has permitted.
Sub-processors (cloud infrastructure, security tools)	We use a limited number of carefully vetted sub-processors (list at provisioniq.org/policies). All are contractually bound to GDPR-equivalent standards and audited annually. UK-based data storage only.
AI service providers	Where AI-assisted features are used, anonymised or pseudonymised data may be processed by approved AI providers under strict contractual controls. Identifiable pupil data is never sent to an AI provider without DPO approval, school consent, and a signed DPA. See Section 9 for full AI data use rules.
Safeguarding bodies (if legally required)	We may be required to disclose information to LADO, police, or children's services in genuine safeguarding emergencies. We will notify the Data Controller (school/LA) unless doing so would prejudice the investigation.

Law enforcement / regulatory authorities	Only where compelled by a valid legal order. We will challenge orders we believe are unlawful or disproportionate and will notify the Data Controller where permitted.
Auditors and insurers	Limited data shared under strict confidentiality agreements for audit, legal, or insurance purposes.
Prospective acquirers (if sold)	In the event of a business sale or merger, personal data may be transferred to a successor entity. We will notify users and provide opt-out options where legally required. Any acquirer must honour this Privacy Policy or provide equivalent protection.

We Never Sell Your Data

ProvisionIQ does not sell, rent, or trade personal data — including pupil data — to any third party for any commercial purpose. We do not use pupil data for advertising, profiling, or any purpose unrelated to the delivery of SEND management services. We do not share data with AI training datasets or use pupil data to train or improve any AI model without explicit written consent from the Data Controller. Equity analytics data is processed in aggregate for school-level reporting only and is never shared at individual level with any third party.

9. Artificial Intelligence — How We Use Data in AI Features

ProvisionIQ incorporates AI-assisted features including provision planning support and automated compliance reporting. The following rules govern how personal data is handled in the context of these features:

Rule	Detail
Advisory only	All AI features are advisory. No AI feature makes or records an automated decision that has legal or similarly significant effects for any individual pupil. AI-generated suggestions are always reviewed and approved by a qualified professional before being saved.
Clear labelling	All AI-generated content on the platform is clearly labelled as AI-assisted in the user interface, so school staff can distinguish AI suggestions from human-authored records.
No identifiable data to third-party models	Identifiable pupil personal data is not sent to any external AI model provider without: (a) anonymisation or pseudonymisation verified by the DPO, (b) explicit written consent from the Data Controller (school/LA), and (c) a signed DPA with the AI provider confirming UK or approved data residency and prohibition on training data use.
No training on pupil data	ProvisionIQ does not use identifiable pupil data to train, fine-tune, or evaluate any AI model. This prohibition is contractually enforced with all AI providers.

AI-specific audit log	Every invocation of an AI feature that accesses or references RESTRICTED pupil data is logged with: timestamp; user ID; feature name; data categories accessed; and whether the AI output was accepted, modified, or rejected by the user.
DPIA for every AI feature	A DPIA is conducted before any AI feature is deployed to production. Summary outputs are available to Data Controllers on request (see Section 6).

10. International Transfers

All ProvisionIQ personal data is stored and processed on UK-based servers. We do not transfer personal data outside the United Kingdom as a matter of standard operation.

Our sub-processors are contractually required to process data in the UK or, where an EU sub-processor is used for a specific function, under a UK International Data Transfer Agreement (IDTA) or equivalent safeguard. A list of sub-processors and their data locations is available at provisioniq.org/policies

UK Data Residency Commitment

ProvisionIQ commits that all pupil personal data, ISP content, safeguarding records, and MIS-integrated data are stored exclusively on UK-based servers. This commitment is built into our sub-processor contracts and is audited as part of our ISO 27001 and Cyber Essentials Plus certifications. If any change to data residency is required, we will notify all Data Controllers (schools/LAs) with at least 60 days' notice before any change takes effect.

11. How We Keep Your Data Secure

ProvisionIQ is built with security as a foundational principle. Our technical and organisational security measures include:

11.1 Technical Measures

Measure	Detail
Encryption at rest	AES-256 encryption for all data stored on ProvisionIQ servers, including S3-backed evidence and observation file storage. Encryption keys managed separately and rotated regularly.
Encryption in transit	TLS 1.3 for all data in transit between users' browsers/devices and our servers. Older TLS versions disabled. HSTS enforced.
Authentication	Keycloak OIDC with PKCE flow for all platform authentication. MFA mandatory for all administrator accounts and all access to RESTRICTED pupil data.

Access controls	Role-based access control (RBAC) with the principle of least privilege. Eight defined user roles. Granular permission templates per role.
Audit logging	Immutable, tamper-evident audit logs of all user actions across all entities. Logs retained for 7 years. Cannot be deleted by any user, including administrators.
Vulnerability management	Regular automated vulnerability scanning. Penetration testing by an independent CREST-accredited firm annually, with scope including the Parent Portal, MIS integration endpoints, and AI feature attack surface.
Network security	Web Application Firewall (WAF), DDoS mitigation, intrusion detection, and network segmentation. Cyber Essentials Plus certified.
Backups	Automated hourly backups with point-in-time recovery. Backups encrypted and stored in a separate UK facility. Recovery tested quarterly.
Secure development	OWASP-aligned secure development lifecycle. Code reviews, SAST, DAST, and dependency vulnerability scanning in CI/CD pipeline. AI prompt injection testing for AI features.

11.2 Organisational Measures

Measure	Detail
Cyber Essentials Plus	Certified to Cyber Essentials Plus (the UK government's highest cybersecurity standard). Certificate renewed annually.
ISO 27001:2022	Full Information Security Management System (ISMS) implemented and certified. Annual surveillance audit by accredited certification body.
Staff training	All staff complete mandatory information security and data protection training on joining and annually thereafter. AI security and MIS integration security included in annual training.
Background checks	Enhanced DBS with Children's Barred List check for all staff with regular access to pupil personal data.
Data Protection Officer	An independent, qualified DPO is appointed to advise on GDPR compliance, conduct DPIAs, maintain the AI Register, and act as the ICO point of contact.
Incident response	A documented Incident Response Plan is tested at least annually. P1 incidents trigger ICO notification assessment within 2 hours. Personal data breaches reported to the ICO within 72 hours where required.
Supplier security	All third-party sub-processors and AI providers subject to security due diligence before onboarding and annual review. Security requirements contractually enforced.

Business continuity	A Business Continuity and Disaster Recovery Plan maintained and tested annually. RTO: 4 hours; RPO: 1 hour.
---------------------	---

12. How Long We Keep Your Data

We retain personal data only for as long as necessary for the purposes for which it was collected, taking into account legal obligations, regulatory guidance, and legitimate business need.

Data Category	Retention Period	Basis
Active pupil ISP and SEND records	Duration of school's licence, then 30 days for export/deletion by school	Contractual; school instructs deletion as Data Controller
Safeguarding records (concern flags, referral records, safeguarding notes)	Retained until the pupil's 25th birthday, or for the duration of any ongoing investigation (whichever is later); schools may request earlier deletion where no investigation is ongoing and there is no statutory barrier	DfE Records Management Code of Practice; ICO guidance on safeguarding records; the heightened sensitivity of safeguarding data requires longer retention than standard SEND records
Archived pupil records (post-deletion request)	Securely deleted within 30 days of request (except safeguarding records subject to above rule)	Contractual; UK GDPR Art. 17
User account data (active)	Duration of employment at the licensed school	Contractual
User account data (after account closure)	30 days for recovery, then deleted	Legitimate interests (service continuity)
Audit logs (security and access logs)	7 years	Regulatory obligation; ISO 27001; ICO guidance
AI feature invocation logs (RESTRICTED data)	3 years from date of invocation	Accountability obligation; DPIA requirement
Financial records (invoices, payment data)	6 years	Companies Act 2006 / HMRC requirement
Support ticket records	3 years from ticket closure	Legitimate interests (service quality, legal defence)
Marketing contact data	Until opt-out received, or 2 years of inactivity (whichever sooner)	Consent / Legitimate interests; PECR
Website analytics (anonymised)	26 months rolling	Legitimate interests

Data breach and incident records	3 years from closure of investigation	UK GDPR Art. 33; ICO accountability obligation
----------------------------------	---------------------------------------	--

Safeguarding Record Retention

Safeguarding records held on the ProvisionIQ platform are subject to the DfE Records Management Code of Practice and ICO guidance. These records are retained until the pupil's 25th birthday as a default. They are immutable (cannot be deleted by any platform user) and access-restricted to Designated Safeguarding Lead and above. Schools wishing to delete safeguarding records before the default retention period should contact dpo@provisioniq.org with their request and the relevant legal basis for early deletion.

13. Your Rights Under UK GDPR

Under UK GDPR, you have the following rights in relation to your personal data. These rights apply differently depending on whether ProvisionIQ is acting as Data Controller or Data Processor. All rights requests should be directed to dpo@provisioniq.org.

Right	What It Means	How to Exercise It
Right of Access (SAR)	You can request a copy of the personal data we hold about you and information about how it is used	Email dpo@provisioniq.org . We will respond within one calendar month.
Right to Rectification	You can ask us to correct inaccurate or incomplete data	Email dpo@provisioniq.org . Where ProvisionIQ is the Processor, we will direct you to the relevant Data Controller (your school/LA).
Right to Erasure	You can ask us to delete your data in certain circumstances (data no longer necessary; consent withdrawn; no legitimate interest)	Email dpo@provisioniq.org . Note: we may be unable to delete safeguarding records or audit logs where there is a legal obligation to retain them.
Right to Restriction	You can ask us to restrict processing of your data while a complaint is being resolved or accuracy is disputed	Email dpo@provisioniq.org . Restriction applied within 72 hours of confirmation.
Right to Data Portability	You can request your data in a structured, machine-readable format (JSON/CSV) where processing is based on consent or contract	Use the Export function in the platform, or request via dpo@provisioniq.org .
Right to Object	You can object to processing based on legitimate interests,	Email dpo@provisioniq.org . Marketing opt-outs processed

	including profiling and direct marketing	immediately. Legitimate interests objections reviewed within one month.
Rights re automated decisions	You have the right not to be subject to a decision based solely on automated processing that produces significant legal or similarly significant effects	ProvisionIQ does not make automated decisions about individuals. All AI outputs are advisory and reviewed by a qualified professional.

Pupil Rights (Data Subjects)

Where ProvisionIQ processes pupil personal data on behalf of a school or LA, the school/LA is the Data Controller and is responsible for handling data subject rights requests from pupils and their families. If a pupil or parent submits a rights request directly to ProvisionIQ, we will acknowledge it within 5 business days and forward it to the relevant Data Controller (school/LA) for action. ProvisionIQ will provide technical assistance to the school/LA in fulfilling rights requests (e.g. extracting specific data, applying restrictions, or deleting records on instruction).

14. Children's Privacy

ProvisionIQ processes personal data about children (under 18) exclusively in the context of delivering SEND management services to licensed schools and local authorities. We do not collect data directly from children. All pupil data is provided by the licensed school or LA, acting as Data Controller, under their own legal authority and Privacy Notice.

The ProvisionIQ platform is not directed at children and does not include features intended for direct use by pupils. Parent Portal access is for parents and carers (adults), not the children themselves. We apply enhanced protections to all pupil data, including:

- Access restriction by role with the principle of least privilege
- Encryption at rest (AES-256) and in transit (TLS 1.3) for all pupil data
- No use of pupil data for profiling, advertising, or any commercial purpose
- No use of identifiable pupil data in AI model training without explicit Data Controller consent
- Strict retention limits aligned to DfE guidance and the ICO's Age Appropriate Design Code principles
- Immediate action on deletion requests from the Data Controller
- Immutable safeguarding records with restricted access

15. Changes to This Policy

We review this Privacy Policy at least annually and whenever there is a material change to how we process data. When we make significant changes, we will:

- Update the "Effective Date" at the top of this policy
- Notify all licensed schools and LAs by email at least 30 days before the change takes effect

- Display a prominent notice on the platform dashboard
- For material changes affecting pupil data processing or AI features, seek explicit re-confirmation from Data Controllers

The current and all previous versions of this Privacy Policy are archived at provisioniq.org/policies.

16. Complaints

If you have a concern about how we handle your personal data, please contact our Data Protection Officer in the first instance:

Contact	Detail
DPO email	dpo@provisioniq.org
DPO post	Data Protection Officer, ProvisionIQ Ltd, 2 Houlder Drive, Howden, DN14 7ZU
Response time	We aim to acknowledge all complaints within 3 business days and respond fully within one calendar month.

If you are not satisfied with our response, or if you believe we are processing your data unlawfully, you have the right to lodge a complaint with the Information Commissioner's Office (ICO):

ICO Contact	Detail
Website	ico.org.uk
Telephone	0303 123 1113
Post	Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

We Take Complaints Seriously

Every data protection complaint is reviewed by our DPO and logged in our complaints register. We use complaints to identify systemic issues and improve our practices. Complaint statistics are reviewed at Board level quarterly. Complaints do not affect your right to continue using the platform.

Version History

Version	Date	Author	Changes
---------	------	--------	---------

1.0	May 2026	DPO	Initial policy published on platform launch
2.0	July 2026	DPO	Added DPIA disclosure statement (§6); safeguarding record retention with DfE basis (§12); AI data use rules (§9); MIS integration data disclosure (§3.2); Parent Portal and multi-agency data sharing (§8); equity analytics data use clarification; corrected all DPO contact references to single address dpo@provisioniq.org; AI labelling and audit log obligations