Data Retention Policy

ProvisionIQ Ltd — How Long We Keep Data and How We Delete It

Document	Data Retention Policy
Company	ProvisionIQ Ltd
Version	1.0
Effective Date	22 May 2026
Next Review	22 May 2027
Policy Owner	CTO
Applies to	All personal data processed by ProvisionIQ Ltd, including pupil data held on behalf of licensed schools and local authorities
Compliance	UK GDPR · DPA 2018 · ISO 27001 · Cyber Essentials Plus · ICO Records Management Guidance

Why This Policy Matters

Retaining data longer than necessary is a breach of the UK GDPR data minimisation and storage limitation principles (Article 5(1)(c) and (e)). Over-retention of pupil SEND data carries particular risk given its sensitive nature.

This policy sets out precisely how long ProvisionIQ retains each category of personal data, the legal basis for each retention period, and the secure deletion procedures we apply at the end of each retention period.

Where ProvisionIQ acts as Data Processor (for pupil and school data), retention decisions are ultimately directed by the Data Controller (school/LA). This policy reflects our default retention schedules and the deletion procedures we apply on instruction.

Version	Date	Summary
1.0	May 2026	Initial policy — platform launch

1. Retention Principles

ProvisionIQ's approach to data retention is governed by the following UK GDPR principles:

Principle	How ProvisionIQ Applies It
Storage limitation (Art. 5(1)(e))	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Data minimisation (Art. 5(1)(c))	We collect only what is necessary and delete data promptly when its purpose is fulfilled
Purpose limitation (Art. 5(1)(b))	Data is retained only for the purposes for which it was collected; it is not retained "just in case" for unspecified future uses
Integrity and confidentiality (Art. 5(1)(f))	Retained data is protected with the same security measures as active data throughout its retention period
Accountability (Art. 5(2))	We document our retention decisions, maintain a Record of Processing Activities (RoPA), and can demonstrate compliance on request

Retention periods have been determined by reference to: (a) the purpose of processing and the operational need; (b) statutory and regulatory requirements (including school records guidance, HMRC requirements, and Companies Act obligations); (c) ICO guidance on retention for education data; (d) relevant sector-specific guidance (including DfE and NASEN recommendations); and (e) contractual obligations to our school and LA customers.

2. Scope and Responsibilities

2.1 Scope

This policy applies to all personal data processed by ProvisionIQ Ltd, including:

- Data held within the ProvisionIQ platform on behalf of licensed schools, trusts, and local authorities (as Data Processor)
- Data held by ProvisionIQ in its capacity as Data Controller (account data, financial records, marketing data, support records)
- Data held in backup systems, archives, and disaster recovery environments
- Data held by sub-processors on ProvisionIQ's behalf

2.2 Responsibilities

Role	Responsibility
Data Protection Officer (DPO)	Owns this policy; reviews it annually; advises on retention decisions; manages the RoPA; oversees disposal processes
Head of Engineering	Implements technical retention controls; manages automated deletion schedules; maintains backup and disposal procedures
Customer Success Team	Notifies schools/LAs of approaching data deletion events; processes manual deletion requests from Data Controllers
All Staff	Comply with this policy; report any suspected breaches of retention rules to the DPO
Data Controllers (Schools/LAs)	Determine retention periods for pupil data within the parameters set by ProvisionIQ's platform; instruct ProvisionIQ on deletion; maintain their own retention policies

3. Retention Schedule — Pupil and SEND Data (Processed as Data Processor)

The following retention schedule applies to data held on behalf of licensed schools and local authorities. ProvisionIQ applies these as default retention periods; individual Data Controllers may instruct shorter retention periods via the platform administration settings.

Data Category	Default Retention Period	Legal Basis / Reference
Active pupil ISP / Individual Support Plan	Retained for the duration of the school's active licence	Contractual obligation; school as Controller
Pupil ISP data post-licence-expiry	30-day export window; then permanently deleted unless school requests extension (max 90 days)	DPA 2018 Art. 5(1)(e); contract term
Archived / historical ISP versions	Retained alongside live ISP during licence; deleted with it	Version control requirement; same basis
Pupil SEND register / profile data	Duration of licence + 30-day export window	Same as above
Safeguarding concern records	Minimum 7 years from date of record (or until the pupil reaches age 25, whichever is later); Data Controller may extend	Children Act 1989; Keeping Children Safe in Education (KCSIE); Ofsted requirements
EHCP / ISP supporting documents (uploaded reports, assessments)	Duration of licence + 30-day export window; original documents remain with the school	Contract; DfE school records guidance
Evidence uploads (observations, photographs, reports)	Duration of licence + 30-day export window	Same as above
Parent / carer contact data (portal access)	Duration of school's licence; deleted when pupil record is deleted	Contract; data minimisation
Multi-agency professional data (EP reports, specialist referrals)	Duration of licence + 30-day export window; originals with the professional's organisation	Contract; professional records guidance
Deleted pupil records (soft-delete)	30-day recovery window; then permanently purged from all systems including backups within 90 days	DPA 2018 Art. 17 (right to erasure); Art. 5(1)(e)

Safeguarding Records — Special Consideration

Safeguarding records carry the longest retention requirement. Under KCSIE (Keeping Children Safe in Education) guidance and the Children Act 1989, safeguarding records should typically be retained for a minimum of 7 years after the last entry, or until the child reaches age 25 — whichever is later.

ProvisionIQ's platform flags safeguarding records with a minimum retention marker. These records cannot be deleted by any user (including administrators) during the statutory retention period without DPO authorisation.

Schools should record their safeguarding data retention decisions in their own DPIA and retain a copy of the original records independently, not solely on the ProvisionIQ platform.

4. Retention Schedule — Data Held as Data Controller

The following retention schedule applies to data for which ProvisionIQ is the Data Controller.

Data Category	Retention Period	Legal Basis
User account data (active employees / platform users)	Duration of employment / active licence subscription	Contract; legitimate interests
User account data (post-departure / account closure)	30 days for recovery; then permanently deleted	DPA 2018 Art. 5(1)(e); Art. 17
Audit logs (user access, actions, changes)	7 years from date of log entry	Regulatory obligation; ISO 27001 A.12.4; Cyber Essentials; legal evidence requirement
Security incident logs	7 years from incident closure	Legal obligation; ICO breach notification requirements; litigation hold
Invoices and financial records	6 years from the end of the accounting year in which the transaction occurred	Companies Act 2006; HMRC / VAT Act 1994 s.73
Contract records (licence agreements, DPAs)	6 years after contract expiry	Limitation Act 1980 (6-year limitation period for contract claims)
Support ticket records	3 years from ticket closure	Legitimate interests; customer service improvement; product development
DPIAs (Data Protection Impact Assessments)	Indefinitely (living documents, reviewed annually)	DPA 2018 / UK GDPR accountability obligation; ICO guidance
Data subject rights requests (SARs, erasure, etc.)	3 years from response date	Accountability; defence against regulatory action
Data breach records	3 years from breach closure	ICO guidance; regulatory obligation; defence against claims
Marketing contact data (with consent)	Until consent is withdrawn or 2 years' inactivity (whichever is sooner), then deleted	DPA 2018; PECR; Art. 7(3) (right to withdraw consent)
Website analytics data (anonymised)	26 months rolling (industry standard for trend analysis)	Legitimate interests; fully anonymised
DBS check records	Stored as date and reference number only (never a copy of the certificate); deleted 6 months after employment ends	DBS Code of Practice; ICO guidance

Employment / HR records	6 years after employment ends	Employment Rights Act 1996; HMRC; Limitation Act 1980
Board minutes and governance records	Permanently retained	Companies Act 2006; corporate governance best practice

5. Backup and Archive Retention

5.1 Backup Schedule

Backup Type	Retention Period
Daily automated backup	Retained for 30 days; oldest backups deleted as new ones are created
Weekly backup	Retained for 13 weeks (3 months)
Monthly backup	Retained for 12 months
Annual backup (year-end snapshot)	Retained for 3 years; then reviewed for deletion

5.2 Backup Deletion Protocol

When a school or LA instructs ProvisionIQ to delete pupil data (e.g. on contract termination, data subject erasure request, or Data Controller instruction), the deletion proceeds as follows:

1. Live data is deleted from active systems within 5 business days of the confirmed instruction
2. The deletion event is recorded in the immutable audit log
3. Daily and weekly backups containing the deleted data are overwritten and purged within 30 days (next backup cycle)
4. Monthly backups are overwritten within 90 days
5. Annual backups are reviewed and the relevant records isolated and deleted within 6 months
6. Written confirmation of deletion is provided to the Data Controller within 10 business days of the final purge

Backup vs Live Deletion

It is technically impractical to delete specific records from encrypted backup files immediately. The law recognises this: ICO guidance accepts that data in backups may persist for a short period after deletion from live systems, provided backups are not accessed or restored during that window.

ProvisionIQ's backup deletion protocol complies with ICO guidance. Backup data is never restored to live systems after a deletion request unless the Data Controller withdraws the deletion instruction within the 30-day live-data recovery window.

All backup storage is encrypted (AES-256) and held in a separate UK facility with restricted access.

6. Secure Deletion Procedures

6.1 Methods of Deletion

Method	When Applied
Cryptographic erasure (crypto-shredding)	Primary method for cloud-stored data. The encryption key for the relevant data is destroyed, rendering the data permanently inaccessible and unrecoverable. Applied for all routine and on-instruction deletions.
Secure overwrite (DoD 5220.22-M or equivalent)	Applied where physical media must be decommissioned (e.g. hardware rotation). All storage media is securely wiped before disposal or repurposing.
Physical destruction	Applied to any physical media that cannot be securely overwritten. Carried out by a certified data destruction company with a certificate of destruction retained for 3 years.
Database record deletion	For application-level deletions, records are permanently removed from all tables and any referential data. Soft-delete (30-day recovery) is used for accidental deletions before permanent purge.

6.2 Deletion Triggered by Contract Termination

When a school or LA's licence with ProvisionIQ expires or is terminated:

7. ProvisionIQ sends a written notification to the Data Controller 30 days before expiry, confirming the data available for export and the deletion timeline
8. The Data Controller has 30 days post-termination to export their data via the platform's export tools
9. At day 30, all non-safeguarding pupil data is moved to a secure archive pending final deletion
10. At day 60, the secure archive is deleted using cryptographic erasure, unless a written extension has been agreed (maximum 90 days total)
11. Safeguarding records subject to mandatory minimum retention periods are retained in an encrypted, isolated environment and notified to the Data Controller
12. ProvisionIQ provides written confirmation of deletion within 10 business days of the final purge

6.3 Deletion on Data Subject Erasure Request

When a Data Controller instructs ProvisionIQ to delete a specific individual's data following a valid Right to Erasure request:

13. ProvisionIQ acknowledges the instruction within 2 business days
14. Live data is deleted within 5 business days

15. Where deletion is not possible (e.g. because legal retention obligations apply), ProvisionIQ notifies the Data Controller with the specific reason and the date when deletion will become possible
16. Backup deletion follows the schedule in Section 5.2
17. Confirmation of deletion is provided in writing within 10 business days of the live deletion event

7. Policy Review and Governance

7.1 Review Cycle

This policy is reviewed:

- Annually, as part of ProvisionIQ's review cycle
- Following any material change to UK data protection law or ICO guidance
- Following any significant data incident that reveals a gap in retention practices
- Following any change to the categories of data processed or the systems used to process them

7.2 Record of Processing Activities (RoPA)

ProvisionIQ maintains a Record of Processing Activities (RoPA) as required by UK GDPR Article 30. The RoPA documents all processing activities, including the retention period and deletion procedures for each data category. The RoPA is reviewed by the DPO quarterly and made available to the ICO on request.

7.3 Data Protection Impact Assessments

Before introducing new data processing activities or significantly changing existing ones, ProvisionIQ conducts a Data Protection Impact Assessment (DPIA) as required by UK GDPR Article 35. DPIAs consider the appropriate retention period for the new processing activity and are documented and retained permanently.

7.4 Compliance Monitoring

Compliance with this policy is monitored through:

- Automated retention monitoring: the platform generates alerts when data approaches its scheduled deletion date
- Quarterly DPO review of deletion activity logs
- Annual internal audit of a sample of data records to confirm retention rules are being applied
- Annual ISO 27001 surveillance audit covering data lifecycle controls
- Annual Cyber Essentials Plus assessment covering data handling procedures

Non-Compliance

Any breach of this Data Retention Policy is treated as a potential personal data breach and assessed under ProvisionIQ's Incident Response Procedure.

Staff who knowingly retain data beyond the specified retention periods, or who fail to securely delete data when required, may face disciplinary action.

ProvisionIQ will self-report to the ICO where a retention failure constitutes a notifiable personal data breach under UK GDPR Article 33.

8. Associated Policies and Documents

Document	Location
Privacy Policy	provisioniq.org/policies
Data Processor Addendum (DPA) Template	Provided to all licensed customers; available at provisioniq.org
Sub-Processor List	provisioniq.org/policies— updated within 14 days of any change
Information Security Policy	Available to customers on request; dpo@provisioniq.co.uk
Incident Response Policy	Available to customers on request; dpo@provisioniq.co.uk
Record of Processing Activities (RoPA)	Available to ICO on request; summary available to Data Controllers on request
DPIA Register	Available to ICO on request
ISO 27001 Certificate	www.provisioniq.org/about/policies/
Cyber Essentials Plus Certificate	www.provisioniq.org/about/policies/

This Data Retention Policy is approved by the Board of ProvisionIQ Ltd and takes effect from 22 May 2026. It supersedes all previous retention schedules and data lifecycle policies.