Safeguarding Policy

Protecting children, young people and adults at risk

Document	Safeguarding Policy
Company	ProvisionIQ Ltd
Version	2.0
Effective Date	July 2026
Policy Owner	Chief Operating Officer
Approved By	Chief Executive
Next Review	July 2027
Applies To	All ProvisionIQ employees, contractors, partners and platform users with administrative access
Replaces	Version 1.0 (May 2026)

Version 2.0 — What has changed?

This version significantly strengthens the policy to reflect ProvisionIQ's role as a SaaS platform that processes special category pupil data (SEND records, EHCPs, ISPs) on behalf of schools and Multi-Academy Trusts. Key additions: dedicated Data Safeguarding chapter; AI Governance obligations; expanded DSL duties; school data processor responsibilities; updated UK legal framework; ICO breach notification procedures; and a Safeguarding Risk Register.

1. Policy Statement

ProvisionIQ is committed to safeguarding and promoting the welfare of children, young people and adults at risk. Safeguarding is everyone's responsibility. This policy applies to all employees, volunteers, contractors, third-party partners and any individual granted administrative access to the ProvisionIQ platform.

ProvisionIQ operates as a B2B SaaS platform used by UK schools and Multi-Academy Trusts to manage Special Educational Needs and Disabilities (SEND) provision. The platform stores, processes and transmits sensitive personal data about children — including Education, Health and Care Plans (EHCPs), Individual Support Plans (ISPs), health information, and multi-agency records. This creates a dual safeguarding responsibility:

- Direct safeguarding: preventing harm to any child, young person or adult at risk who may come into contact with ProvisionIQ staff.
- Data safeguarding: ensuring that sensitive pupil data held on the platform cannot be used to enable harm, exploitation or abuse.

Important — Platform Context

No commercial consideration, operational convenience or technical expedient will ever take priority over the safety and welfare of a child or vulnerable adult. Where doubt exists, the safeguarding of the individual comes first.

2. Scope and Application

This policy applies to:

- All ProvisionIQ employees (permanent, fixed-term, part-time and remote)
- Contractors, consultants and agency workers engaged by ProvisionIQ
- Third-party technology vendors, sub-processors and integration partners who have access to platform data
- Board members and senior advisers
- Any individual granted privileged or administrative access to school data held on the ProvisionIQ platform

It applies across all of ProvisionIQ's operating environments: the cloud platform (provisioniq.org), internal systems, development and staging environments, and any offline or exported data derived from the platform.

3. Legal Framework

Legislation / Guidance	Relevance to ProvisionIQ

Children Act 1989 and 2004	Framework for children's welfare; informs how concerns about children identified through platform use must be handled
Safeguarding Vulnerable Groups Act 2006	Regulated activity obligations; DBS requirements for roles with direct access to pupil data and school environments
Care Act 2014	Duties in respect of adults at risk, including SEND adults over 18 whose records may be held on the platform
Working Together to Safeguard Children 2023	Statutory multi-agency guidance; informs ProvisionIQ's responsibilities when facilitating multi-agency collaboration
Keeping Children Safe in Education 2023 (KCSiE)	Directly applies: ProvisionIQ provides services to schools and must align with their statutory safeguarding duties
UK GDPR / Data Protection Act 2018	Governs all personal data processing; special category data (health, SEND) requires explicit legal bases and heightened protection
Children and Families Act 2014	The legislative basis for EHCPs and SEND support frameworks — the core subject matter of the platform
Equality Act 2010	Non-discrimination obligations; disability is a protected characteristic central to ProvisionIQ's user base
Computer Misuse Act 1990	Informs obligations around preventing unauthorised access to pupil data held on the platform
Network and Information Systems (NIS) Regulations 2018	Cybersecurity obligations for digital services handling sensitive data
Online Safety Act 2023	Contextual awareness of online harms relevant to the digital environments ProvisionIQ creates for children's data

4. Definitions

4.1 Child

A person under the age of 18 years. For the purposes of this policy, this includes any pupil whose data is held on the ProvisionIQ platform regardless of whether they are currently enrolled in education.

4.2 Adult at Risk

An adult with care and support needs who is experiencing, or at risk of, abuse or neglect, and who — as a result of those needs — is unable to protect themselves against harm. This includes SEND learners over 18 whose transition and post-16 records may be held on the platform.

4.3 Abuse

Abuse may take many forms including: physical, emotional, sexual, neglect, financial, discriminatory, institutional, domestic, and online/digital abuse. In the context of a data platform, digital abuse includes the misuse of sensitive pupil data to enable grooming, stalking, exploitation or identity fraud.

4.4 Regulated Activity

Activity that requires an enhanced DBS check. For ProvisionIQ, this includes any role in which an individual has unsupervised access to the detailed personal, health and educational records of children held on the platform, or any role that involves direct attendance at school sites.

4.5 Special Category Data

Personal data that warrants heightened protection under UK GDPR Article 9. Data held on the ProvisionIQ platform that falls within this category includes: health data, data concerning disability, data relating to mental health or neurodevelopmental conditions, and data identifying membership of ethnic or religious groups. All SEND records must be treated as special category data.

4.6 Data Safeguarding Incident

Any event — accidental or deliberate — that results in the unauthorised access, disclosure, loss, alteration or destruction of pupil data held on the ProvisionIQ platform, where that event creates a risk to the rights, freedoms or safety of a child or vulnerable adult.

5. Designated Safeguarding Lead (DSL)

ProvisionIQ shall maintain a named Designated Safeguarding Lead at all times. The DSL is a member of the senior leadership team and holds ultimate operational responsibility for safeguarding at ProvisionIQ.

DSL Responsibility	Detail
First point of contact	All safeguarding concerns — whether arising from direct contact, platform use or data incidents — are reported to the DSL in the first instance
Legislation and procedure	Maintains current knowledge of safeguarding law, statutory guidance, ICO obligations and local safeguarding partnership procedures
Statutory liaison	Liaises with children's services, adult safeguarding authorities, the police and the ICO as required
Training oversight	Ensures all staff receive appropriate safeguarding and data safeguarding training at induction and on a rolling basis

Platform data risk oversight	Conducts quarterly reviews of data access logs, permission structures and data sharing agreements with schools
Record keeping	Maintains secure, confidential records of all safeguarding concerns, referrals, data incidents and actions taken
Vendor oversight	Reviews safeguarding and data protection compliance of all sub-processors and integration partners annually
DSL Training	Advanced safeguarding training every 2 years; annual safeguarding and data protection refresher
Deputy DSL	A named Deputy DSL is designated and trained to act in the absence of the DSL; contact details held by the CEO

6. Reporting a Safeguarding Concern

6.1 Concerns About an Individual

If any member of staff becomes concerned about the welfare of a child or adult at risk — whether through direct contact, through content on the platform, or through information shared by a school user — they must follow these steps without delay:

Step	Action	Important Note
1	Do not investigate the concern yourself or tell the child or adult you are reporting	Preserve evidence; avoid contamination of any subsequent investigation
2	Report to the DSL verbally as soon as possible and on the same day	Do not delay — it is not your role to decide whether abuse has occurred
3	Follow up with a written factual record within 1 hour using the Safeguarding Concern Form	Facts only — no interpretation, opinion or diagnosis
4	If the DSL is unavailable and there is immediate risk: call 999 or children's services directly	The child's safety takes absolute priority
5	Maintain strict confidentiality — share information only on a need-to-know basis	Safeguarding information may be shared without consent where there is a risk of harm; document the decision

6.2 Concerns Arising from Platform Data

Staff may encounter content within school data on the platform that gives rise to a safeguarding concern (e.g. a note in an ISP record, a flagged observation, or a message in the multi-agency portal). The same reporting process applies. ProvisionIQ staff must not modify, delete or share the data before reporting to the DSL.

Duty to Report

Failure to report a safeguarding concern is a serious disciplinary matter that may result in dismissal. The welfare of the child or adult at risk takes priority over all other considerations, including commercial relationships with school customers.

7. Data Safeguarding: Protecting Pupil Data

ProvisionIQ processes special category personal data relating to children with SEND as a data processor acting on behalf of schools and MATs (the data controllers). This chapter sets out the specific obligations that flow from that role.

7.1 Data Processing Principles

All pupil data must be processed in accordance with UK GDPR principles. In addition to standard data protection obligations, ProvisionIQ applies the following safeguarding-specific requirements:

- Data minimisation: the platform only captures and retains data that is directly necessary for the delivery of SEND provision support. No data is retained beyond the contracted period without explicit school instruction.
- Purpose limitation: pupil data is never used for product development, training of AI models, analytics or marketing without a lawful basis and explicit written agreement with the school.
- Accuracy: the platform provides version control and audit trails to ensure that SEND records remain accurate and attributable.
- Storage limitation: data retention schedules are aligned to the DfE Records Management Code of Practice. Schools are notified 90 days before scheduled deletion.
- Integrity and confidentiality: all data is encrypted at rest (AES-256) and in transit (TLS 1.3). Access is restricted by role-based permissions.

7.2 Role-Based Access Control (RBAC)

Access to pupil data is governed by a strict role-based access model. ProvisionIQ operates eight defined user roles (SENCO, Class Teacher, LA Officer, Multi-Agency Professional, Parent/Carer, Governor, School Administrator, ProvisionIQ Support). Each role has the minimum data access necessary for its function. ProvisionIQ staff are granted access to school data only where:

- Access is required to resolve a specific technical support issue, with the school's written authorisation;
- Access is required to investigate a safeguarding or data incident; or
- Access is required under a legal obligation.

All ProvisionIQ staff access to school data is logged, time-limited and reviewed by the DSL on a quarterly basis.

7.3 Data Sharing and Third-Party Sub-Processors

ProvisionIQ only shares pupil data with third parties in the following circumstances:

- The school has given written authorisation and a Data Processing Agreement (DPA) is in place;
- Sharing is required by law or for the prevention of harm to a child or vulnerable adult; or
- The third party is an approved sub-processor listed in ProvisionIQ's Sub-Processor Register, subject to a signed DPA.

All sub-processors are assessed against the ProvisionIQ Vendor Security and Safeguarding Questionnaire prior to onboarding and annually thereafter. The Sub-Processor Register is available to schools upon request.

7.4 Personal Data Breach and ICO Notification

ProvisionIQ has a legal obligation to notify the Information Commissioner's Office (ICO) of certain personal data breaches within 72 hours of becoming aware of them. Where a breach involves child data and creates a risk of harm, the school must also be notified without undue delay.

Breach Severity	Internal Response	External Notification
Low — minimal risk, no harm	DSL informed; incident logged; remediation documented	No ICO notification required; school notified within 5 business days
Medium — risk to rights/freedoms	DSL and DPO engaged; incident investigation commenced within 4 hours	ICO notified within 72 hours; school notified within 24 hours
High — risk of harm to child or vulnerable adult	DSL, DPO and CEO engaged; incident response team convened immediately	ICO notified within 72 hours; school notified immediately; police contacted if risk of harm

7.5 Pupil Data and AI Features

ProvisionIQ's platform incorporates AI-assisted features for provision planning and compliance reporting. The following rules apply to the use of AI in relation to pupil data:

- No pupil personal data is sent to third-party AI model providers (e.g. large language model APIs) without anonymisation, explicit school consent and a lawful basis under UK GDPR.
- AI-generated outputs relating to individual pupils are clearly labelled as AI-assisted and must be reviewed and approved by a qualified professional before being saved to a pupil record.
- AI models are not trained on identifiable pupil data without explicit consent from the school and compliance review.
- ProvisionIQ maintains an AI Register documenting all AI features, their data inputs, the model provider, and the safeguards applied.

8. Safe Recruitment

ProvisionIQ follows safer recruitment practices for all roles. The following requirements apply:

Requirement	All Roles	Roles with Data Access / School Visits
Right to work check	Yes	Yes
Identity verification	Yes	Yes
Employment references (min. 2)	Yes	Yes, including gap investigation
DBS check	Standard	Enhanced DBS with Children's Barred List check
Self-declaration of cautions / convictions	Yes	Yes, reviewed by DSL
Social media / online search	Yes	Yes, documented
Probationary review	3 months	3 months with DSL sign-off

Any role that involves regular access to identifiable pupil data (including SEND records, EHCPs and ISPs) is treated as a role involving regulated activity for DBS purposes. The DSL must sign off all appointments to such roles.

9. Training Requirements

Staff Group	Training Requirement	Frequency
All employees	Safeguarding awareness induction including data safeguarding module	On joining; refresher every 2 years
Staff with access to pupil data	Enhanced safeguarding training: UK GDPR, SEND data handling, breach response	Every 2 years; annual refresher
Engineering and product staff	Secure-by-design training, OWASP Top 10, data minimisation in product development	Annual
Customer-facing staff	Recognising safeguarding concerns raised by school users; escalation procedures; SEND context training	Annual
Designated Safeguarding Lead	Advanced DSL training; ICO liaison; data safeguarding governance	Every 2 years; annual update
Senior Leadership Team	Strategic safeguarding, governance responsibilities, regulatory obligations	Annual

10. Online Safety and Digital Conduct

ProvisionIQ's platform creates digital environments in which sensitive information about children is shared between schools, families and professionals. All ProvisionIQ staff and partners must:

- Never attempt to contact children, young people or their families directly through the platform or any other channel unless specifically instructed to do so by a school and authorised by the DSL.
- Report any inappropriate communication, unsolicited contact or unusual access patterns identified in platform logs to the DSL immediately.
- Ensure that test, staging and development environments never contain real pupil data without explicit DSL authorisation and appropriate technical safeguards.
- Comply with ProvisionIQ's Acceptable Use Policy in all use of company systems and the platform.

11. Managing Allegations Against Staff or Partners

If an allegation is made against a ProvisionIQ employee, contractor or partner — including allegations relating to misuse of pupil data — the following procedure applies:

1. The allegation must be reported to the CEO immediately. If the allegation is against the CEO, it must be reported to the Chair of the Advisory Board.
2. The CEO (or Chair) will notify the DSL and consider whether the individual should be suspended from duties pending investigation.
3. Where the allegation relates to harm or risk of harm to a child, the Local Authority Designated Officer (LADO) must be contacted within one working day.
4. Where the allegation involves a data breach or misuse of pupil data, the DPO and ICO will be notified as required.
5. A formal investigation will be conducted in accordance with ProvisionIQ's disciplinary procedure. The DSL will maintain records of all steps taken.
6. Outcomes will be reported to the relevant authority and recorded securely.

12. Safeguarding Risk Register

ProvisionIQ maintains a Safeguarding Risk Register reviewed by the DSL and senior leadership team quarterly. The register identifies risks specific to a SEND data platform, including:

Risk Area	Example Risk	Mitigating Control
Data breach	Unauthorised access to EHCP or health data enabling harm to a child	RBAC; encryption; access logging; breach response plan

Insider threat	Employee misusing pupil data or exfiltrating records	Least-privilege access; audit logs; DBS checks; secure offboarding
AI misuse	AI feature exposing pupil data to third-party models without consent	AI Register; data anonymisation; school consent requirement
Sub-processor failure	Third-party vendor breaching pupil data	Vendor due diligence; DPAs; annual review; contractual right to audit
School user error	School admin sharing pupil records with unauthorised party via platform	Role-based permissions; user training materials; audit trails
Ransomware / cyber attack	Platform data encrypted or exfiltrated by malicious actor	Cyber Essentials Plus certification; incident response plan; backups
Safeguarding concern in data	Staff identify evidence of abuse or neglect in platform records	Clear reporting escalation; DSL oversight; staff training
Transition data exposure	Post-16 SEND data disclosed to parties no longer authorised	Automated access expiry; school-controlled data retention settings

13. Confidentiality

Safeguarding information is held in strict confidence. ProvisionIQ operates a need-to-know principle: safeguarding concerns and records are shared only with those who require the information to protect the child or adult at risk. Staff must be aware that:

- Confidentiality is not absolute. UK GDPR permits and, in some cases, requires the sharing of personal data to protect life or prevent serious harm, even without the individual's consent.
- All decisions to share safeguarding information must be documented, including the reasoning and the legal basis applied.
- Staff who breach confidentiality outside of a legitimate safeguarding purpose may be subject to disciplinary action.

14. Policy Review and Governance

This policy is reviewed annually, or following any material change in ProvisionIQ's platform or data processing activities; a safeguarding incident or data breach; changes to relevant legislation or statutory guidance; or feedback from schools, regulators or safeguarding partners.

The DSL is responsible for monitoring developments in safeguarding law and practice and proposing updates to this policy. The CEO approves all revisions. The policy and its version history are held securely and made available to schools on request.

Related Policies

This policy should be read alongside: Data Protection and Privacy Policy · Information Security Policy · Acceptable Use Policy · Recruitment and DBS Policy · Disciplinary Policy · Whistleblowing Policy · Incident Response Plan · AI Governance Policy

Version History

Version	Date	Author	Changes
1.0	May 2026	COO	Initial policy
2.0	July 2026	CEO/ COO	Comprehensive revision: data safeguarding, AI governance, ICO breach notification, Safeguarding Risk Register, online safety, RBAC, sub-processor obligations