Acceptable Use Policy

ProvisionIQ Ltd — Governing Safe and Responsible Use of the Platform

Document	Acceptable Use Policy (AUP)
Company	ProvisionIQ Ltd
Policy Owner	Chief Technology Officer (CTO)
Version	1.0
Effective Date	July 2026
Next Review	July 2027
Applies to	All platform users including school staff, SENCO leads, LA officers, specialist professionals, parents and carers, and any individual accessing the ProvisionIQ platform under a school, trust, or LA licence
Compliance basis	UK GDPR / DPA 2018 · Children and Families Act 2014 · Cyber Essentials Plus · ISO 27001:2022 · Keeping Children Safe in Education (KCSIE)
Replaces	N/A — Initial version

Statement of Intent

ProvisionIQ processes some of the most sensitive data in the UK education system, including EHCPs, Individual Support Plans, health records, and safeguarding flags for children with SEND. Every person who uses this platform is a trusted steward of that data. This Acceptable Use Policy sets out what responsible, lawful use of the platform looks like, and what is never permitted. Compliance is mandatory. Breach may result in suspension of access, termination of licence, and referral to relevant authorities, including the ICO.

Version History

Version	Date	Summary
1.0	July 2026	Initial version — published at platform launch

1. Purpose, Scope, and Objectives

1.1 Purpose

This Acceptable Use Policy (AUP) defines the rules and responsibilities that govern the use of the ProvisionIQ platform by all authorised users. It exists to protect the children and young people whose data is processed on the platform, to protect the schools and local authorities who have placed their trust in ProvisionIQ, and to ensure that every user understands the boundaries of lawful, ethical, and responsible platform use.

This policy operates alongside the ProvisionIQ Privacy Policy, Information Security Policy, and any Data Processor Agreement in place between ProvisionIQ Ltd and the licensed school, trust, or local authority.

1.2 Scope

This policy applies to all individuals who access the ProvisionIQ platform in any capacity, including:

- School staff: SENCOs, teachers, teaching assistants, senior leaders, and administrative staff with platform accounts
- Local authority officers, educational psychologists, specialist support professionals, and any other professional accessing the platform
- Parents and carers accessing the Parent Portal
- Contractors, consultants, and third parties granted access by a school administrator
- ProvisionIQ Ltd staff and contractors who access customer data for support, maintenance, or development purposes

It applies to access via all channels: the web platform at platform.provisioniq.org, the ProvisionIQ mobile application (where available), API integrations, and any other interface provided by ProvisionIQ.

1.3 Objectives

- Protect the confidentiality, integrity, and availability of pupil SEND data, EHCPs, ISPs, health records, and safeguarding information
- Ensure all platform use complies with UK GDPR, DPA 2018, KCSIE, and the Children and Families Act 2014
- Prevent misuse, unauthorised disclosure, or inappropriate processing of children's personal data
- Define clear responsibilities for authorised users at every role level
- Establish a proportionate and consistent response to policy breaches
- Maintain the trust of pupils, parents, schools, and local authorities who rely on the platform

2. Authorised Use

2.1 Permitted Use

The ProvisionIQ platform is provided solely for the purposes of managing SEND provision for pupils within the licensed school, trust, or local authority. Authorised use includes:

Permitted Activity	Notes
Creating and managing Individual Support Plans (ISPs) and EHCPs	For pupils enrolled at the licensed school or within the licensed LA area
Recording observations, outcomes, interventions, and evidence	Only for pupils the user has been granted access to

Accessing and contributing to multi-agency collaboration records	Within the user's professional role and scope of responsibility
Using the Parent Portal to share, co-produce, and review plans	With authenticated parents and carers of the relevant pupil
Generating compliance reports, analytics, and governance documentation	Using only data within the user's authorised scope
Accessing AI-assisted provision planning suggestions	Advisory use only; all AI outputs must be reviewed by a qualified professional before acting on them
Using MIS-integrated data to support SEND provision planning	Read-only where configured; no manipulation of MIS source data via the platform
Raising and responding to support tickets with ProvisionIQ	Via designated support channels; do not include unnecessary personal data in support queries

2.2 Role-Based Access Responsibilities

Access to the platform is role-based. Each user must operate strictly within the permissions assigned to their role. Users must not attempt to access data or functionality beyond their assigned permissions, and must not request elevated permissions without documented justification approved by their school or LA administrator.

Role	Responsibilities Under This Policy
SENCO / Platform Administrator	Responsible for configuring user accounts, permissions, and access controls within their school; must ensure all users are made aware of this AUP; must not grant access beyond what is justified by professional role
Class Teacher / Teaching Assistant	May access only the pupil records they have been assigned; must not browse records of pupils outside their professional responsibility
Senior Leader	Read-level access to school-wide data is permitted for governance and oversight; must not share or export data beyond what is needed for that purpose
Local Authority Officer	Access limited to pupils within their LA remit and professional scope; bound by this AUP and any additional LA data governance requirements
Specialist Professional (EP, SALT, OT, etc.)	Access limited to specific pupils they are actively supporting; must not retain copies of pupil data outside the platform
Parent / Carer	Access limited to their own child's records; must not share login credentials or signed share-links with any third party
ProvisionIQ Support Staff	Access to customer data only when required to investigate a reported issue; access must be logged and time-limited; no access to pupil data for any commercial purpose

3. Prohibited Use

3.1 Absolute Prohibitions

The following actions are strictly prohibited for all users, regardless of role or circumstance. Breach of any absolute prohibition will result in immediate suspension of access pending investigation, and may result in referral to the ICO, the relevant Local Authority Designated Officer (LADO), or law enforcement.

Prohibited Action	Why It Is Prohibited
Sharing login credentials with any other person	Undermines accountability, creates security vulnerabilities, and violates UK GDPR accountability requirements
Accessing pupil records without a legitimate professional reason	Constitutes unlawful processing of children's personal data under UK GDPR
Downloading, exporting, or printing pupil data outside your professional role	May constitute a data breach; all exports are audit-logged
Sharing pupil personal data via unsecured channels (personal email, WhatsApp, AirDrop, etc.)	Violates the platform's security controls and UK GDPR data integrity obligations
Using pupil data for any purpose other than supporting that pupil's SEND provision	Constitutes unlawful secondary use of special category personal data
Attempting to access, modify, or delete records you are not authorised to view	A criminal offence under the Computer Misuse Act 1990 in addition to a GDPR violation
Uploading or processing data relating to pupils not enrolled at your licensed school	Outside the scope of the Data Processor Agreement; constitutes unlawful processing
Using AI-assisted suggestions as professional assessments without independent review	AI features are advisory only; unreviewed outputs must not be presented as professional recommendations
Attempting to circumvent, disable, or test security controls without written authorisation	A criminal offence under the Computer Misuse Act 1990
Uploading malicious code, exploits, or content designed to disrupt the platform	Criminal offence; may result in prosecution
Using the platform to harass or discriminate against any data subject	Violates the Equality Act 2010, KCSIE, and ProvisionIQ's data use terms
Accessing the platform from an unmanaged device not meeting minimum security standards	Violates ProvisionIQ's Information Security Policy and the school's data security obligations

3.2 Additional Prohibitions Relating to Children's Data

Given the heightened sensitivity of special category data processed on behalf of children with SEND, the following additional prohibitions apply:

- Never photograph, screenshot, or capture pupil records or safeguarding flags on any personal device
- Never discuss individual pupils' SEND records, health data, or safeguarding information via any channel outside the platform that could be intercepted
- Never share signed parent portal share-links with any person other than the intended parent or carer
- Never use a pupil's data to train, fine-tune, or evaluate any external AI or machine learning system not provided by ProvisionIQ

- Never retain copies of exported pupil data on personal or unmanaged devices beyond the immediate purpose for which the export was authorised

4. Account Security and Credential Management

All users are personally responsible for the security of their platform credentials. The following requirements apply to all accounts:

Requirement	Detail
Password strength	Minimum 12 characters; must include uppercase, lowercase, a number, and a special character; must not be reused from other services
Multi-factor authentication (MFA)	Mandatory for all accounts with access to RESTRICTED data; mandatory for all administrator accounts; must not be disabled
Credential sharing	Strictly prohibited; each user must have their own individual account
Session management	Users must log out when leaving a workstation or device; sessions timeout automatically after 30 minutes of inactivity on RESTRICTED data
Suspicious activity	Any suspected compromise of credentials must be reported to the school's platform administrator and to ProvisionIQ support (support@provisioniq.org) immediately
Leavers	When a user leaves their role, the school administrator must disable the account within 2 hours of confirmed departure
Device lock	Devices used to access the platform must auto-lock after no more than 5 minutes of inactivity and require a PIN, password, or biometric to unlock

5. Data Handling and Confidentiality

5.1 Classification of Data on the Platform

All data processed via the ProvisionIQ platform is classified according to ProvisionIQ's Information Classification Scheme. Users must handle data in accordance with the classification assigned:

Classification	Examples on Platform	Handling Requirements
RESTRICTED	Pupil SEND records, ISPs, EHCPs, health data, safeguarding flags, MIS-sourced pupil data, AI outputs referencing individual pupils	Access strictly controlled by role; no external sharing without explicit authorisation; encrypt all exports; audit logging mandatory
CONFIDENTIAL	School-level analytics, internal support correspondence, configuration data	Need-to-know access; not to be shared outside the school or LA without justification
INTERNAL	General platform notifications, non-pupil-specific guidance, policy documents	Standard access controls; not for public distribution

PUBLIC	Published ProvisionIQ documentation, policy summaries, product guides	No additional restrictions

Default Classification

Any pupil personal data received via MIS integration, entered by platform users, or generated by AI features is automatically classified as RESTRICTED regardless of labelling. When in doubt, treat data as RESTRICTED.

5.2 Data Export and Printing

- Exports of pupil data are permitted only for legitimate professional purposes directly related to SEND provision for that pupil
- All exports are recorded in the platform's audit log
- Exported data must be stored on school or LA managed systems only, with appropriate access controls
- Printed pupil records must be stored in locked cabinets and securely shredded (cross-cut) when no longer required
- Physical records must not be left unattended or taken off school premises without a documented reason and appropriate safeguards

5.3 Third-Party Sharing

Sharing of pupil data with third-party professionals must be conducted via the platform's built-in multi-agency collaboration tools where possible. Where data must be shared outside the platform:

- Sharing must be authorised by the school's SENCO or data lead
- The recipient must have a legitimate professional role in the pupil's provision
- Data must be sent via encrypted, secure channels only (never via personal email or unencrypted file transfer services)
- A record of the sharing must be retained by the school

6. AI Feature Use

ProvisionIQ provides AI-assisted features to support provision planning, outcome drafting, and analytics. These features are designed to save professional time, not to replace professional judgement. All AI features on the ProvisionIQ platform are subject to the following rules:

Requirement	Detail
Human review mandatory	All AI-generated suggestions, provision recommendations, and draft content must be reviewed, verified, and approved by a qualified professional before use. AI outputs must never be shared with parents, pupils, or multi-agency partners without professional review.
No automated decisions	No AI feature on the ProvisionIQ platform makes decisions with legal or similarly significant effect for any individual pupil. AI features are advisory only.

No external AI use with pupil data	Users must not copy pupil data from the platform into external AI tools (e.g. ChatGPT, Copilot, Gemini, or any similar service). Only ProvisionIQ's approved AI features may process pupil data.
Transparency to parents	Where AI-assisted content forms part of an ISP or EHCP shared with parents or professionals, it must be clearly identified as AI-assisted and reviewed by a named professional.
AI suggestions are not clinical advice	AI-generated provision suggestions do not constitute medical, psychological, therapeutic, or legal advice. All clinical and specialist decisions must be made by appropriately qualified professionals.

7. Safeguarding Obligations

The ProvisionIQ platform handles safeguarding records. All users with access to safeguarding data must be aware of the following:

Safeguarding takes precedence

Safeguarding takes precedence over all other data handling rules. If a user identifies information on the platform that gives rise to a safeguarding concern, they must follow their school's or LA's safeguarding procedures immediately, regardless of any data confidentiality obligation.

- Safeguarding records on ProvisionIQ are immutable, they cannot be deleted or modified by any platform user, including school administrators
- Access to safeguarding flags and records is restricted to Designated Safeguarding Leads (DSLs) and above, as configured by the school administrator
- Any unauthorised access to, disclosure of, or interference with safeguarding records must be reported to the DSL immediately and to ProvisionIQ support
- The platform's safeguarding features are a tool to support, not replace, the school's statutory safeguarding procedures. Schools must maintain their own records and processes in accordance with KCSIE

8. Monitoring and Audit

ProvisionIQ maintains comprehensive, immutable audit logs of all significant platform activity, including:

- All login and logout events, including failed authentication attempts
- All access to RESTRICTED data (pupil records, health data, safeguarding flags)
- All data exports, downloads, and print events
- All modifications to pupil records, including who made the change and when
- All account creation, permission changes, and account deactivation events
- All AI feature usage, including the professional who reviewed and approved any AI-assisted content

Audit logs are retained for a minimum of 7 years in accordance with ProvisionIQ's data retention policy. They cannot be modified or deleted by any platform user.

Monitoring Notice

By using the ProvisionIQ platform, users consent to the monitoring and logging of their platform activity for the purposes of security, compliance, and safeguarding. Audit logs may be reviewed by ProvisionIQ Ltd in response to a reported security incident, data breach, or safeguarding concern, and may be shared with the school, the ICO, the police, or other relevant authorities where legally required.

9. Reporting Obligations

9.1 What Users Must Report

All users are responsible for reporting the following incidents promptly:

Incident Type	Who to Report To and When
Suspected data breach (accidental disclosure, unauthorised access, lost device containing pupil data)	Report to school SENCO/data lead immediately; they must notify ProvisionIQ via dpo@provisioniq.org within 24 hours. ProvisionIQ will assess ICO notification obligations within 48 hours.
Suspected compromise of platform credentials (phishing, shared password, account takeover)	Report to school administrator immediately and to ProvisionIQ support (support@provisioniq.org); change password immediately; report within 1 hour
Observed AUP breach by another user	Report to school SENCO or administrator in the first instance; if it involves safeguarding data, also notify the DSL
Platform security vulnerability or unexpected system behaviour	Do not attempt to exploit or investigate independently; report immediately to support@provisioniq.org with a description of the behaviour
Safeguarding concern identified via the platform	Follow school safeguarding procedures immediately; notify DSL; use the platform's built-in safeguarding flag where appropriate

9.2 No-Blame Reporting Culture

ProvisionIQ and participating schools are committed to a no-blame culture for reporting in good faith. Users who promptly and honestly report an incident will not face disciplinary action for the initial incident, provided they act in good faith and cooperate fully with any investigation. The exception is deliberate or reckless misuse of pupil data, which will be treated as a serious disciplinary matter regardless of self-reporting.

10. Consequences of Breach

Breaches of this Acceptable Use Policy are taken seriously. The response to a breach will be proportionate to its nature, severity, and whether it was deliberate or accidental.

Breach Severity	Examples	Potential Consequences

Minor — Accidental, no harm caused	Accessing a pupil record by mistake and immediately logging out; forgetting to lock workstation; sharing a report via standard school email	Immediate access correction; refresher training; logged on record; no further action if no harm caused
Moderate — Negligent or repeated	Repeated failure to use MFA; sharing credentials without malicious intent; exporting data to a personal device without authorisation	Formal warning; mandatory retraining; temporary suspension of access; reported to school leadership; may be reported to DPO
Serious — Deliberate or reckless	Deliberately accessing pupil records without authorisation; sharing pupil data externally without justification; using external AI tools with pupil data; circumventing security controls	Immediate suspension of access; full investigation; referral to ICO; referral to LADO (if safeguarding-related); potential termination of employment or contract; may result in criminal prosecution
Critical — Malicious	Exfiltrating or selling pupil data; deliberately deleting or corrupting safeguarding records; uploading malware; identity fraud using platform credentials	Immediate account termination; referral to police; ICO notification; possible civil and criminal proceedings; full licence termination

11. Training and Awareness

Awareness of and compliance with this policy is a condition of platform access. Schools are responsible for ensuring their staff and authorised users complete appropriate data protection and platform security training before accessing RESTRICTED data.

Requirement	Detail
Induction training	All new users must complete ProvisionIQ's platform induction materials (including data protection and AUP overview) before accessing pupil data
Annual refresher	All users with access to RESTRICTED data must complete annual data protection refresher training, evidenced in their school's training record
AUP acknowledgement	By activating a ProvisionIQ account, users confirm they have read, understood, and agree to comply with this Acceptable Use Policy. Schools must retain records of AUP acknowledgement for all platform users.
KCSIE compliance	All staff with access to safeguarding records must have completed their school's annual KCSIE training and be familiar with the school's safeguarding policies

12. Governance and Review

12.1 Policy Ownership

Role	Responsibility
Chief Technology Officer (CTO)	Policy owner; approves all revisions; accountable for AUP enforcement across the ProvisionIQ platform

Data Protection Officer (DPO)	Reviews policy annually for UK GDPR compliance; advises on material changes; manages breach reports that engage data protection law
School SENCO / Data Lead	Responsible for communicating and enforcing this AUP within their school; managing user accounts; and reporting breaches to ProvisionIQ
All Platform Users	Responsible for reading, understanding, and complying with this policy as a condition of platform access

12.2 Review Cycle

This policy will be reviewed annually by the CTO and DPO, or sooner if:

- A material data breach or security incident occurs that reveals a gap in this policy
- Significant changes are made to the ProvisionIQ platform, including new AI features, new MIS integrations, or new user roles
- Changes in applicable law or regulation require policy updates
- The ICO, a court, or a supervisory authority issues guidance that is material to platform use

Revised versions of this policy will be communicated to all licensed customers and will take effect 14 days after publication, except where legal requirements necessitate immediate effect.

12.3 Contact

Contact	Details
Data Protection Officer	dpo@provisioniq.org
Technical Support	support@provisioniq.org
General Enquiries	hello@provisioniq.org
Registered Address	ProvisionIQ Ltd, 2 Houlder Drive, Howden, DN14 7ZU
ICO Registration	No. ZC156305
Website	provisioniq.org

A final word

This Acceptable Use Policy is a living document. If you have a question about what is or is not permitted, contact your school's SENCO or ProvisionIQ's Data Protection Officer at dpo@provisioniq.org before taking any action you are unsure about. When in doubt, protect the child's data.