

Data Security Policy

GP Liaison Services Ltd | Version 1.0 | Effective 26.10.2026

1. Purpose and Commitment

Direct Access Healthcare Group Limited and its trading division GP Liaison Services Ltd (GPLS) are committed to protecting the confidentiality, integrity and availability of all data we hold and process, including data entrusted to us by NHS and other healthcare clients. This policy sets out the commitments made in our internal information security and data protection policy framework, and applies to all of our services. It is reviewed and republished at least annually.

2. Scope

This policy applies to all GPLS directors, employees, contractors and subcontractors, and to all information, systems, devices and cloud services used to deliver our work. It covers personal data, pseudonymised patient data, NHS staff data, operational and logistics data, and commercially confidential information, in any format.

3. Legal and Regulatory Framework

We process data in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018; the Common Law Duty of Confidentiality and the Caldicott Principles; the NHS Data Security and Protection Toolkit (DSPT) and the National Data Guardian's data security standards; the Cyber Essentials scheme operated by the National Cyber Security Centre (NCSC); the NHS Records Management Code of Practice; and the Computer Misuse Act 1990 and the Privacy and Electronic Communications Regulations.

GPLS is registered with the Information Commissioner's Office (registration number ZB662441) and completes the NHS DSPT annually under organisation code G5B0T. Our published DSPT status can be viewed on the NHS DSPT website.

4. Roles and Responsibilities

The Managing Director holds overall accountability for data security and acts as Senior Information Risk Owner (SIRO). The Data Protection Officer advises on data protection compliance, oversees data protection impact assessments, and is the contact point for clients, data subjects and the ICO. The information governance lead maintains this policy and its supporting policies, procedures and registers. All staff and contractors must follow this policy, complete mandatory training and report any actual or suspected incident immediately. Our managed IT and cloud partners operate under written agreements requiring them to meet equivalent security standards.

5. Our Role When Handling Client Data

When we process data on behalf of NHS or other clients, GPLS acts as a data processor. We process data only on the documented instructions of the controller, under a written data processing agreement that meets Article 28 of UK GDPR. We do not use client data for any other purpose, we do not appoint sub-processors without the controller's prior written authorisation, and we return or securely destroy data at the end of the engagement. Where processing presents a high risk, we support the controller in completing a data protection impact assessment before processing begins.

6. Data Minimisation and Pseudonymisation

We request and retain only the minimum data needed for the agreed purpose. Wherever possible we work with pseudonymised or aggregated data and do not hold direct patient identifiers. Any data used to link records is held separately, with restricted access, and only for as long as it is needed. Outputs and dashboards are designed so that individuals cannot be identified, applying small number suppression where appropriate.

7. Data Location and Hosting

Production data services are hosted in Amazon Web Services in the UK (London region). Development and test environments are held in a separate account, isolated from production, and do not use live identifiable data. Email, document storage and collaboration use Microsoft 365, administered within our own tenancy. Client data is not transferred or stored outside the UK without the prior written agreement of the controller and appropriate safeguards.

8. Access Control

Access is granted on a least privilege, need to know basis and is approved by the Managing Director. Every user has a unique, named account and shared accounts are not permitted. Multi-factor authentication is enforced on Microsoft 365, our cloud hosting platform and all administrator accounts, and on other services wherever the service supports it. Administrator accounts are separate from everyday user accounts and are used only for administrative tasks. Access rights are reviewed regularly and removed promptly when a person leaves or changes role. Passwords must meet our password policy, and a company password manager is used for work credentials.

9. Encryption

Data is encrypted in transit using current versions of TLS, and files are exchanged with clients only by secure, agreed methods such as SFTP or secure portals. Data held in our cloud platforms and on company devices is encrypted at rest. Removable media is not used to store or transfer client data.

10. Devices, Networks and Remote Working

GPLS staff work remotely, and client data is accessed only from company-owned, centrally managed laptops. Devices are enrolled in mobile device management, with enforced screen lock, secure sign-in, disk encryption and controls that block auto-running software. Access to company services is through a secured, firewalled connection managed by our IT partner. Personal devices, phones and tablets are not used to access client data. Staff must keep screens private, lock devices when unattended, and not work on client data in public places.

11. Malware Protection, Patching and Monitoring

All devices run managed anti-malware protection, updated automatically. Operating systems, applications and firmware are kept on supported versions, with critical and high-risk security updates applied within 14 days of release. Firewalls and cloud security groups deny traffic by default and allow only what is required. Security events and audit logs are collected and reviewed, and external threat intelligence, including NHS and NCSC alerts, is monitored and acted on.

12. Backup and Business Continuity

Critical systems and data are backed up automatically to protected, separate storage within the UK, and backups are tested periodically. We maintain a business continuity and disaster recovery plan so that client services can be restored within agreed timescales following an incident.

13. Suppliers and Third Parties

Suppliers that handle data or provide IT services to GPLS are assessed before use and reviewed regularly. They must provide written assurance of appropriate security, such as Cyber Essentials, ISO/IEC 27001 or a published DSPT status, and are bound by written contracts with confidentiality and data protection terms.

14. Training and Confidentiality

All staff and contractors complete data security and information governance training at induction and at least annually, aligned with NHS data security awareness requirements. Everyone working for GPLS is bound by confidentiality obligations in their contract or agreement, which continue after the engagement ends.

15. Incident and Breach Management

Any actual or suspected security incident, data breach or near miss must be reported to the Data Protection Officer immediately. Incidents are contained, investigated and recorded in our incident log, with lessons learned and corrective actions tracked to completion. Affected clients are notified without undue delay, and in any case within 24 hours of GPLS becoming aware of a breach affecting their data, so that they can meet their own reporting duties. Where GPLS is the controller, reportable breaches are notified to the ICO within 72 hours and, where relevant, reported through the DSPT incident reporting tool.

16. Retention and Secure Disposal

Data is retained only for the period agreed with the client or set out in our retention schedule, in line with the NHS Records Management Code of Practice. At the end of that period, or at the end of an engagement, data is securely deleted or returned to the controller, and deletion is confirmed in writing on request. Redundant devices are securely wiped or destroyed by an approved provider.

17. Assurance and Review

Compliance with this policy is checked through internal audit, the annual DSPT assessment, independent Cyber Essentials Plus assessment by an accredited certification body, and periodic penetration testing. Information risks are recorded in our risk register and reviewed at board level as a standing agenda item. This policy is reviewed at least annually, or sooner following a significant incident, a change in law or a change to our services.

18. Related Documents and Contact

This policy is supported by our internal policies on data protection, information governance, network and firewall security, end-user device and email security, passwords and administrator access, malware protection, system monitoring, supplier security, change management, incident and breach management, training, and information risk management. Copies of relevant documents and assurance evidence can be provided to clients and prospective clients on request.

Questions about this policy, or requests for assurance evidence, should be sent to the Data Protection Officer at andrew@gp-liaison.com.

19. Approval

This policy was approved by the Board of Directors of Direct Access Healthcare Group Limited (Company No. 10201779), trading as GP Liaison Services Ltd, and is signed on its behalf by the Managing Director.

Andrew Turner

Managing Director, GP Liaison Services Ltd

Date: 26.10.2026