GENERAL DATA PROTECTION POLICY

UK Laboratory Services Ltd

UK GDPR | Data Protection Act 2018 | ISO 9001:2015 Clause 7.5

1. Purpose and Scope

UK Laboratory Services Ltd is committed to protecting the privacy, confidentiality and integrity of personal data relating to its customers, employees, contractors and other contacts. This policy sets out how the company collects, uses, stores and protects personal data in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This policy applies to all staff employed by or contracted to UK Laboratory Services Ltd who handle personal data in any form, whether in paper or electronic format, on-site or off-site.

2. Applicable Legislation

This policy has been prepared in accordance with the following legislation and guidance:

- UK General Data Protection Regulation (UK GDPR) - retained in UK law via the Data Protection Act 2018
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations 2003 (PECR), where applicable
- Guidance issued by the Information Commissioner's Office (ICO)

3. Roles and Responsibilities

3.1 Directors

The Directors of UK Laboratory Services Ltd hold overall accountability for data protection compliance across the organisation. They are responsible for ensuring adequate resources are allocated to support this policy and that appropriate governance structures are in place.

3.2 Data Protection Coordinator

The nominated Data Protection Coordinator holds operational responsibility for the implementation, monitoring and review of this policy. The Coordinator acts as the primary point of contact for data protection matters, subject access requests, and ICO communications. The role and name of the current Coordinator shall be maintained in the associated Roles and Responsibilities Register.

3.3 All Staff

All staff - whether employed or contracted - are responsible for:

- Handling personal data only in accordance with this policy and any associated procedures.
- Keeping personal data secure and not disclosing it to unauthorised parties.
- Reporting any suspected data breach or near-miss to the Data Protection Coordinator immediately.
- Completing data protection awareness training as required by the company.

EUROPEAN UNION
European Social Fund

4. ICO Registration

UK Laboratory Services Ltd is registered with the Information Commissioner's Office (ICO) as a data controller. Registration details are maintained by the Data Protection Coordinator and renewed annually as required.

5. Data Protection Principles

All staff who process or handle personal data must ensure compliance with the following principles. Personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (data minimisation).
- Accurate and, where necessary, kept up to date. Reasonable steps must be taken to ensure that inaccurate data is erased or corrected without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed.
- Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

6. Lawful Basis for Processing

UK Laboratory Services Ltd will only process personal data where a lawful basis relied upon by the company include:

- Contract - processing is necessary for the performance of a contract with the data subject (e.g. employment contracts, customer service agreements).
- Legal obligation - processing is necessary to comply with a legal obligation (e.g. payroll, health and safety records).
- Legitimate interests - processing is necessary for the legitimate interests of the company, provided these are not overridden by the rights of the data subject.
- Consent - where none of the above applies, explicit consent will be sought and documented before processing.

7. Data Subject Rights

Under UK GDPR, individuals have the following rights in relation to their personal data. UK Laboratory Services Ltd is committed to upholding these rights and will respond to all valid requests within one calendar month of receipt.

Data Subject Right	How UK Laboratory Services Ltd Will Respond
Right of Access	Individuals may request a copy of the personal data held about them (Subject Access Request). UK Laboratory Services Ltd will respond within one calendar month.
Right to Rectification	Individuals may request correction of inaccurate or incomplete personal data.
Right to Erasure	Individuals may request deletion of their personal data where there is no legitimate reason for its continued processing.

Right to Restrict Processing	Individuals may request that processing of their personal data is restricted in certain circumstances.
Right to Data Portability	Individuals may request their personal data in a structured, commonly used and machine-readable format where processing is based on consent or contract.
Right to Object	Individuals may object to processing of their personal data for direct marketing or where processing is based on legitimate interests.
Right to Withdraw Consent	Where processing is based on consent, individuals may withdraw that consent at any time without detriment.

8. International Data Transfers

Personal data will not be transferred outside the United Kingdom unless an appropriate level of protection is in place.

The company will not transfer personal data to a country or territory that does not provide an adequate level of protection without prior authorisation from the Data Protection Coordinator and, where required, the ICO.

9. Third Party Disclosure

Personal data will not be disclosed to third parties except in the following circumstances:

- Where required by law or by a relevant statutory or regulatory body (e.g. HMRC, Health and Safety Executive).
- Where the data subject has provided documented, informed consent before disclosure.
- Where disclosure is to a contracted data processor acting under a Data Processing Agreement with UK Laboratory Services Ltd.

In all cases, the minimum necessary personal data shall be shared, and a record of the disclosure shall be maintained.

10. Security and Control Measures

The following controls must be observed by all staff at all times:

10.1 Physical Security

- All personal data held in paper format must be stored in lockable cupboards or drawers when not in active use.
- Personal data must not be left on unattended desks or in areas accessible to unauthorised individuals.
- Paper records containing personal data must be disposed of by secure shredding.

10.2 Electronic and Device Security

- All devices (laptops, PCs, mobile phones, tablets) must be protected by a PIN or password of a minimum of six characters.
- Applications containing sensitive personal data must be further protected by access permissions granted by management, with passwords of a minimum of eight characters comprising upper case, lower case and special characters, combined with Multi-Factor Authentication (MFA) if needed.
- Screen locks must be activated on all unattended ICT equipment.
- The same password must not be reused across accounts or systems. Passwords must not be written down. The use of an approved password manager is permitted.

- ICT equipment used off-site must be password-protected at all times.
- Data files on portable media (USB drives, memory sticks, CDs) or email attachments containing personal data must be encrypted or password-protected.

11. Data Breach Notification

A personal data breach is any security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

In the event of a suspected or confirmed data breach:

- The member of staff who identifies the breach must report it to the Data Protection Coordinator immediately and without undue delay.
- The Data Protection Coordinator will assess the severity and nature of the breach.
- Where a breach is likely to result in a risk to the rights and freedoms of individuals, it must be reported to the ICO within 72 hours of the company becoming aware of it.
- Where a breach is likely to result in a high risk to individuals, those individuals must also be notified directly without undue delay.
- All breaches, regardless of severity, must be recorded in the company's Data Breach Register.

12. Data Retention

Personal data will not be retained for longer than is necessary for the purpose for which it was collected. UK Laboratory Services Ltd maintains a separate Data Retention Schedule which sets out the categories of data held, the basis for retention, and the applicable retention periods.

The Data Retention Schedule is reviewed annually by the Data Protection Coordinator and is available on request.

13. Training and Awareness

All staff are required to complete data protection awareness training upon commencement of employment or engagement, and at regular intervals thereafter as determined by the Data Protection Coordinator. Records of training completion are maintained by the company.

14. Policy Review

This policy will be reviewed sooner in the event of significant changes to legislation, ICO guidance, or the company's operations. The Data Protection Coordinator is responsible for initiating and managing the review process. Any amendments must be approved by the Managing Director prior to issue.

Authorisation

This policy has been reviewed and approved by the Managing Director of UK Laboratory Services Ltd.

Signed: 

Name: Richard Feeney

Position: Managing Director, UK Laboratory Services Ltd

Date: 20 May 2026