GDPR & Data Protection Policy

Version Control

Version number	Date	Description of changes
V1.0	04 August 2026	Policy launch

Contents

1. Policy Statement 3
2. Purpose 3
3. Scope 3
4. Data Protection Principles 3
5. Lawful Basis for Processing 4
6. Individual Rights 4
7. Information Security 5
8. Data Retention and Disposal 5
9. Data Sharing 5
10. International Transfers 5
11. Personal Data Breaches 6
12. Training and Awareness 6
13. Roles and Responsibilities 6
14. Compliance and Monitoring 7
15. Policy Review 7

GDPR & Data Protection Policy

1. Policy Statement

1.1. ETL Systems Ltd ("ETL") is committed to protecting the privacy, confidentiality, integrity and security of personal data. ETL processes personal information in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and other applicable data protection legislation.

1.2. This policy establishes the principles and requirements for handling personal data within ETL and applies to all employees, contractors, temporary workers, consultants and third parties acting on behalf of the company.

2. Purpose

2.1. The purpose of this policy is to:

2.1.1. Ensure compliance with UK GDPR and Data Protection Act 2018 requirements.
2.1.2. Protect the rights and freedoms of individuals whose data is processed by ETL.
2.1.3. Define responsibilities for managing personal data.
2.1.4. Reduce the risk of data breaches and regulatory non-compliance.
2.1.5. Promote a culture of privacy and information security.

3. Scope

3.1. This policy applies to:

3.1.1. All personal data processed by ETL.
3.1.2. Electronic, paper and verbal information.
3.1.3. Customer, supplier, employee, candidate and visitor information.
3.1.4. All ETL business locations, systems, applications and third-party service providers processing data on behalf of ETL.

4. Data Protection Principles

ETL will ensure personal data is processed in accordance with the seven UK GDPR principles:

1. **Lawfulness, Fairness and Transparency**
   Personal data shall be processed lawfully, fairly and transparently.

2. **Purpose Limitation**
   Personal data shall only be collected for specified, explicit and legitimate purposes.

3. **Data Minimisation**
   Only data necessary for defined business purposes shall be collected and processed.

4. **Accuracy**
   Personal data shall be kept accurate and up to date.

5. **Storage Limitation**
   Personal data shall not be retained longer than necessary.

6. **Integrity and Confidentiality (Security)**
   Appropriate technical and organisational measures shall protect personal data.

7. **Accountability**
   ETL shall be able to demonstrate compliance with all applicable data protection obligations.:

5. Lawful Basis for Processing

5.1. ETL will only process personal data where a lawful basis exists, including:

5.1.1. Performance of a contract.
5.1.2. Compliance with a legal obligation.
5.1.3. Legitimate business interests.
5.1.4. Consent where required.
5.1.5. Protection of vital interests.
5.1.6. Public task where applicable.

5.2. The lawful basis for processing shall be documented and reviewed periodically.

6. Individual Rights

6.1. ETL respects and supports the rights of individuals under UK GDPR, including the right to:

6.1.1. Be informed about the processing of their personal data.
6.1.2. Access their personal information.
6.1.3. Rectify inaccurate information.
6.1.4. Erase data where applicable.
6.1.5. Restrict processing.
6.1.6. Object to processing.
6.1.7. Data portability.
6.1.8. Protection from solely automated decision-making where applicable.

6.2. Requests relating to these rights should be submitted to the Corporate Compliance Manager or designated Data Protection contact. The lawful basis for processing shall be documented and reviewed periodically.

7. Information Security

7.1. ETL shall implement appropriate security controls to protect personal data, including:

7.1.1. Access controls and user authentication.
7.1.2. Role-based permissions.
7.1.3. Password management requirements.
7.1.4. Encryption where appropriate.
7.1.5. Secure backup procedures.
7.1.6. Anti-malware and endpoint protection.
7.1.7. Monitoring and logging of critical systems.
7.1.8. Secure destruction of records and media.

7.2. Employees must ensure personal data is only accessed for legitimate business purposes and is protected from unauthorised disclosure.

8. Data Retention and Disposal

8.1. ETL shall:

8.1.1. Process data in line with the required retention and disposal requirements.
8.1.2. Retain records only for as long as required by business, legal or regulatory requirements.
8.1.3. Ensure secure disposal of personal data when retention periods expire.
8.1.4. Maintain evidence of disposal where appropriate.

9. Data Sharing

9.1. Personal data may only be shared:

9.1.1. When there is a legitimate business requirement.
9.1.2. Under a documented contract or data processing agreement.
9.1.3. Where appropriate safeguards are in place.
9.1.4. In accordance with legal and regulatory requirements.

9.2. Third-party suppliers processing personal data on behalf of ETL must provide adequate assurances regarding privacy and security.

10. International Transfers

10.1. Where personal data is transferred outside the United Kingdom, ETL shall ensure appropriate safeguards are implemented in accordance with UK GDPR requirements.

11. Personal Data Breaches

11.1. All actual or suspected personal data breaches must be reported immediately to the **Data Protection Officer** and **IT Security function.**

11.2. ETL Will:

11.2.1. Investigate reported incidents promptly.
11.2.2. Assess risks to affected individuals.
11.2.3. Implement corrective actions.
11.2.4. Notify the Information Commissioner's Office (ICO) where legally required.
11.2.5. Inform affected individuals when required by law.

12. Training and Awareness

12.1. ETL will provide appropriate data protection and information security training to employees and relevant contractors.

12.2. All personnel are responsible for:

12.2.1. Understanding this policy.
12.2.2. Protecting personal information.
12.2.3. Reporting concerns or incidents immediately.
12.2.4. Completing mandatory training requirements.

13. Roles and Responsibilities

13.1. Senior Management

13.1.1. Responsible for ensuring adequate resources and support for data protection compliance.

13.2. Corporate Compliance Manager:

13.2.1. Responsible for:

13.2.2. Oversight of GDPR compliance activities.
13.2.3. Policy maintenance and review.
13.2.4. Corporate oversight of data protection incident response activity. Accountabilities are within functions and territories.
13.2.5. Monitoring compliance and supporting audits.

13.3. Managers

13.3.1. Responsible for ensuring compliance within their teams.

13.4. Employees and Contractors

13.4.1. Responsible for complying with this policy and protecting personal data in their possession.

14. Compliance and Monitoring

14.1. Compliance with this policy is monitored through:

14.1.1. Internal audits.
14.1.2. Risk assessments.
14.1.3. Incident reviews.
14.1.4. Supplier assessments.
14.1.5. Management reviews.

14.2. Failure to comply with this policy may result in disciplinary action and, where applicable, legal consequences.

15. Policy Review

15.1. This policy shall be reviewed annually or sooner where there are significant changes in legislation, business operations, technology, or identified compliance requirements.

Approved by: 

Name: Kevin Dunne

Position: CEO

Date: 4/8/26

Document Owner: Corporate Compliance Manager
Effective Date: 4th August 2026
Review Date: 4th August 2027