The Engineering Development Trust (EDT)

Data Protection Policy – March 2026

DOCUMENT CONTROL		Document No.	2026/1
Sub-Committee	Audit, Risk and Investments		
Author	David Sobo	**Version no.**	1.1
Reviewer	Paul Senior	**Implementation date**	March 2026
Scope	Trust wide		
Status	Approved	**Next review date**	February 2027
Approved by	Board of Trustees	**Last review date**	February 2026

Contents

Data Protection Policy Statement

EDT is committed to a policy of protecting the rights and privacy of individuals from whom EDT needs to collect and use personal data in order to carry out our work. This policy provides a framework to ensure compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Privacy and Electronic Communications Regulations (PECR), and relevant amendments introduced by the Data (Use and Access) Act 2025 (DUAA).

EDT complies with the six data protection principles as outlined by the ICO (Information Commissioner's Office) to ensure that personal data is;

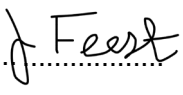
- processed fairly and lawfully, and shall only be processed in line with EDT's privacy notice
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes
- adequate, relevant, and limited to what is necessary.
- accurate and where necessary, kept up to date
- not kept for longer than is necessary
- kept safe and secure.

To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law. Our staff have access to the EDT staff handbook, EDT's privacy notices and operational procedures and guidance to give them appropriate direction on the application of the data protection legislation.

A copy of this statement, which forms part of the employment contract, will be issued to all staff and volunteers in the organisation and will be included in induction packs.

This policy will be reviewed for its effectiveness on an annual basis with other incremental changes as required.

Signed…….. Date 27/02/2026
Chair of Trustees



Signed…….. ……. Date 27/2/26…….
Chief Executive

Key statutory updates since February 2025 (summary)

- Automated decision-making (ADM): UK GDPR restrictions have been relaxed (except where special category data is involved). EDT must provide safeguards: inform individuals, enable human intervention, allow representations, and permit challenges to decisions.
- Subject Access Requests (SARs): the one-month period starts after identity verification; the deadline may pause while EDT seeks clarification; searches must be reasonable and proportionate; where exemptions (e.g., legal privilege) apply, EDT will explain the exemption used.
- Recognised legitimate interests: EDT may rely on new recognised legitimate interests for certain processing (e.g., safeguarding, network and information systems security, direct marketing and necessary intra-group transfers).
- International transfers: adequacy assessments use the 'not materially lower' standard under DUAA (as determined by the Secretary of State).
- PECR penalties: note increased maximum penalties for PECR infringements (up to £17.5m or 4% of global annual turnover).
- Regulator: the ICO remains the UK regulator but is expected to transition to an Information Commission in due course; EDT will update references as the change takes effect.

EDT Data Protection Policy: Commitment and implementation

The EDT is committed to transparent, lawful, fair and proportionate processing of personal data. This includes all personal data we process about stakeholders, staff or those who work or interact with us.

Privacy Notice/s - we publish a privacy notice on our website. We track and make available any changes in our privacy notice. We publish a staff privacy notice internally.

Responsibility - the responsibility for Data Protection rests with the Board of Trustees who delegate responsibility to the CEO and to the Executive Team for the practical implementation of this policy statement. We ensure appropriate delegation for day to day responsibilities for implementation of this policy are agreed, communicated and reviewed. A senior member of the team is appointed as Data Protection Lead and member of the Board is appointed as Trustee lead.

Training - All staff undertake data protection training on induction, with refresher training provided when legislation (including DUAA 2025), systems or procedures change.

Breaches - We take personal data breaches seriously and maintain incident reporting and escalation procedures. We assess whether breaches must be reported to the ICO and, where appropriate, notify affected individuals. Regulatory action will follow the law in force at the time of the incident, consistent with regulator guidance.

Information Rights - we have a process to handle subject access requests and other information rights requests. We ensure transparency over the reasons we are collecting data, and for those individuals to have the right to rectify, delete, restrict or object to their personal data being processed. We take appropriate technical and organisational security measures to safeguard personal information. This will include the information and records related to data subjects being stored securely and only accessible to authorised employees. We ensure that personal information is not transferred outside the organisation without suitable safeguards.

Subject Access Requests – The one-month response period begins once EDT has verified the requester's identity. Where clarification is required, the response period may be paused until clarification is received. EDT will conduct searches that are reasonable and proportionate. Where we rely on an exemption (e.g., legal privilege), we will explain which exemption is used and why.

Automated Decision-Making – Where EDT makes decisions based solely on automated processing that have legal or similarly significant effects, we will inform individuals and provide safeguards, including enabling human intervention, allowing representations, and facilitating challenges to the decision. Automated decision-making involving special category data remains subject to stricter controls.

Recognised Legitimate Interests – EDT may rely on recognised legitimate interests introduced by DUAA for specific purposes, such as safeguarding, network and information systems security, direct marketing and necessary intra-group administrative transfers. Where we rely on legitimate interests, we balance those interests against the rights and freedoms of individuals.

International Transfers – When transferring personal data internationally, EDT will assess adequacy against the DUAA standard of 'not materially lower' protection, as determined by the Secretary of State, and will use appropriate safeguards where required (e.g., IDTAs or Article

46 mechanisms).

Reporting - we have a reporting mechanism to monitor compliance across the organisation including reports to the Board

Communications, information and guidance - we encourage all staff adopt a proactive approach to data protection, providing appropriate information and guidance to staff within the staff handbook, induction documentation and training and administer clear communications.

Contracts - The Operations Director, (in consultation with the Data Protection Lead, where appropriate) reviews relevant contracts to ensure they contain appropriate data protection clauses (including processor obligations under UK GDPR as amended).

Implementation teams – we designate team members with responsibility for data protection, establishing an agreed communications timeline for updates, feedback and reporting.

Data Protection Delegation of Responsibilities

The Trustees delegate day to day responsibility for practical implementation of this policy to the Executive team who will further delegate responsibility to a member of each team (where appropriate).

	Responsible for:
Trustees	• A Data Protection Policy Statement that is compliant with current legislation • Sign off: Data Policy Statement • Lead Trustee: Paul Senior
Operations Director	• Compliance updates to Audit and Risk Committee • Ensuring appropriate EDT offices have the facilities to store hard copies of personal and sensitive data securely and to dispose of data confidentially • Named Data Protection Lead • Review and updates of Policy Statement and Privacy Notices • Responsibility assigned for implementation
HR	• Onboarding and induction to include training and policy information
All Directors	• Confirmation of compliance • Implement audit checklist
IT	• Responsibility for Data Protection procedures and IT related policies and procedures (Acceptable use of IT, Business Continuity Plan (in development) and Critical Incident Policy (awaiting approval). • Ensuring all employees have access to secure equipment and processes required • Ensuring EDT teams have the facilities to store soft copies of personal and sensitive data securely and to dispose of data confidentially.
Marketing	• Ensures adherence to PECR for electronic communications and cookies • Administration of data inbox • ensures that direct marketing relies on a valid lawful basis and respects opt-outs/unsubscribes. (Note: DUAA has increased maximum PECR penalties; see References.)
Delivery / Operational Team Representatives	• Completion of data protection checklist • Ensuring adherence to Privacy Notice through processes and procedures including managing unsubscribes for points of contact

Related documents

Document	Date	Location
EDT Data Protection Policy Statement	March 2026	Internal Policies Folder
EDT Privacy Notice	March 2026	Website
Staff Handbook	June 2025	Internal Policies Folder
IT Policies	February 2025	Internal Policies Folder
Employee Privacy Notice	June 2025	Internal Policies Folder – section 2.6 of Staff Handbook

Review of this document: annually by the Director of Operations

Policy Date: March 2026

Next review date: January 2027

References (for legislative updates)

• GOV.UK – Data (Use and Access) Act 2025: data protection and privacy changes: https://www.gov.uk/guidance/data-use-and-access-act-2025-data-protection-and-privacy-changes

• ICO – How we will regulate as the Data (Use and Access) Act commences: https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/how-we-will-regulate-as-the-data-use-and-access-act-commences/

• Freeths – Data protection legislation: key changes under UK post-Brexit reforms (2026): https://www.freeths.co.uk/insights-events/legal-articles/2026/data-protection-legislation-the-key-changes-under-uk-post-brexit-reforms/

• Fox Williams – The new UK data protection reforms are here – now what? (2025): https://www.foxwilliams.com/2025/07/09/the-new-uk-data-protection-reforms-are-here-now-what/