edt

# Data Protection Policy

All policies and procedures are version controlled.
The most up to date versions are all available on edt's Internal SharePoint site.
If you have questions about how to interpret this policy, please ask the Policy Owner.

# Document Control

| Document Control | |
|---|---|
| Title: | Data Protection Policy |
| Reference: | CG-POL-001 |
| Version: | 9.0 |
| Date: | 01/06/2026 |
| Status: | Approved |
| Owner: | General Counsel |
| Business Area: | Corporate Governance |
| Classification: | Internal & External |
| Date of next review: | 01/06/2027 |

# Document Distribution / Stakeholders

| Document Distribution / Stakeholders | | | | |
|---|---|---|---|---|
| Name | Organisation | Date issued | Version | Action |
| All staff | EDT | 12/06/26 | 9.0 | All staff to read the policy. Policy to be added to policy hub. Comms to be sent out. |
| | | | | |

# Document Revision History

| Document Revision History | | | |
|---|---|---|---|
| Version | Date | Author | Summary of changes |
| 9.0 | 01/06/26 | General Counsel | Approved. Minor updates made. Updated the bullet point on overseas transfer process for EU citizens' personal data to include a link to the UK International Data Transfer Agreement and Addendum. |
| 8.0 | 31/07/25 | General Counsel | Approved |
| 7.2 | 31/07/25 | A. Hawkins | Added to new policy template. |
| 7.1 | 25/07/25 | S. Clifton & A. Hawkins | Minor updates to incorporate any changes to legislation and practice. Data (Use and Access) Act 2025 (DUAA) was added, Related documents section added Digital Safeguarding, Information Classification, Information Security, Remote Access and Use of Personal Devices policies. |

# Scope

This policy governs the way we collect, store and process information about individuals. It reflects the requirements of the UK's Data Protection Act 2018 (the Act), incorporating the General Data Protection Regulation ("GDPR") and the Data (Use and Access) Act 2025 (DUAA) under which EDT is registered as a 'Data Controller'. The policy applies to all staff. Other organisations and individuals working with EDT who have access to personal information are expected to comply with this policy.

# Policy

- EDT will make clear to individuals (data subjects) how we handle their data – notably what data may be held and why. We will seek consent for processing the data unless there is another lawful basis for doing so. Any employee who breaches this Policy or the Act may be subject to disciplinary procedures. If in doubt about any aspect of this policy, contact the Data Protection Lead (DPL) for your business area or the Data Protection Officer (DPO).
- The DPL ensures a Data Protection Impact Assessment (DPIA) (Schedule 5) is done for every new project or activity where personal data will be collected; and that mitigations are implemented. Access to personal data must be restricted to those who need it for legitimate tasks in line with the relevant consent or exemption under the relevant DPIA.
- We will ordinarily seek an individual's specific, informed consent for handling of their personal data, and will ensure collection information is concise and accessible at all points of data collection. We normally require parental consent for a child under 16, subject to the circumstances. We will normally give the individual a Standard Data Collection Form (Schedule 2). Where the data is collected electronically, e.g. via a website, we will use the Privacy Notice (Schedule 7). If there is a justifiable case for reliance on legitimate interests, we will document and review our assessment to ensure processing is necessary, proportionate and does not override individuals' rights.
- Personal data may be processed without consent only in line with an exemption under the Act: each exemption must be approved by the local DPL or the DPO.
- We will avoid automated decision making and personal data profiling where possible. We will normally obtain consent for any such activity. We will review automated decisions on request by a data subject. Where automated decision making or profiling is used, we will ensure appropriate safeguards are in place, including the right to request human review, clear explanations of decisions and the ability to challenge outcomes.

- Where relevant, contracts must include the Standard Data Protection Clause (Schedule 1). Where we need another organisation to process personal data for us, we will use the Standard Data Processing Contract (Schedule 3), or equivalent.
- We will not ordinarily transfer personal data outside the European Economic Area (EEA) without the consent of the data subject. Where we need an organisation outside the EEA, including Group entities, to process personal data of EU citizens for us, we will use the Standard Commission Clauses as amended by the UK Addendum to the EU clauses or the International Data Transfer Agreement, found on the ICO website: What are standard data protection clauses (the UK IDTA and the Addendum)? | ICO. See schedule 4.
- We will provide marketing material only to individuals who have agreed to receive it using "opt in" consent where possible. Soft opt in (previous opt in being used for subsequent activities without update) must be approved by the DPO to ensure it complies with the Privacy in Electronic Communications Regulations.
- Breaches of data security must be escalated in accordance with Schedule 10.
- The DPL must consider retention of data at project design stage (recorded in the DPIA) and confirm at project close down, (Schedule 11).
- We will comply with data subject requests under the Act (Schedule 8).
- The DPO will review data protection at EDT annually. The DPO will report any issues identified and recommended actions to the Audit and Finance Committee.
- We will implement organisational and technological measures to ensure the security of data as set out in Schedule 14.

# Roles and Responsibilities

## All staff are responsible for:

- Reading and complying with this policy;
- Passing a request about personal data immediately to their DPL;
- Passing information on any potential incident / breach immediately to their DPL and/or the DPO.
- Completing mandatory data protection training annually.

## Data Protection Leads (DPLs) are responsible for:

- Promoting and monitoring compliance with this policy in their area – including through DPIAs, staff awareness, annual review and remedial actions;
- Notifying the DPO of any potential breach of data security or other concerns;
- Helping with Data Subject Access Requests (DSARs) (Schedule 8).

## Data Protection Officer (DPO) is responsible for:

- Monitoring compliance with this policy and approving lawful exemptions;

- Handling contact with the Regulator, breaches of data security and requests from individuals;
- Escalating systemic concerns to Executive Team or the Chair of Audit and Finance Committee;
- Co-ordinating the annual review.

### Senior Managers are responsible for:

- Supporting DPLs in their role.

### The Executive Team is responsible for:

- Supporting data protection initiatives to develop a culture of data protection awareness and compliance.

### The Audit and Finance Committee is responsible for:

- Overseeing the data protection environment on behalf of the Trustees.

# Related Documents

## Policies

- Data & IT Asset Disposal Policy
- Digital Safeguarding Policy
- Information Classification Policy
- Information Security Policy
- Remote Access Policy
- UK Records Management Policy
- Use of Personal Devices Policy
- Use of Social Media Policy
- Whistleblowing Policy

## Procedures / guidance / forms

- Schedule 1: Standard Data Protection Clause (all contracts)
- Schedule 2: Standard Data Collection Form (given to data subjects)
- Schedule 3: Standard Data Processing Contract (accompanies contracts requiring personal data processing)
- Schedule 4: Overseas Transfers
- Schedule 5: Data Protection Impact Assessment and link to online form.
- Schedule 6: ICO registration

- Schedule 7: Website Privacy Notice (must be added to websites)
- Schedule 8: Data Subject Access Request Definition and Procedure and link to online form
- Schedule 9: Data Retention
- Schedule 10: Data Security Breach Procedures and link to online form
- Schedule 11: Data Protection Close Down Form and link to online form.
- Schedule 12: Marketing and Electronic Communications Guidance
- Schedule 13: Security