



DISCOVERY
EDUCATIONAL TRUST



Security Measures

SECURITY MEASURES

An outline of the Organisational and Technical Security measures deemed appropriate by the Data Controller for the nature of the personal data processed by the Controller and any Data Processor acting on its behalf.

Description of Security Measures Employed to Safeguard the Processing of Personal Data

1. Organisational

a. Policies and Documented Procedures

Policies relating to Information Governance issues are drafted by employees with detailed knowledge of legal requirements and the processes of the Discovery Educational Trust (DET) and its Schools.

All policies have documented review dates and ownership is assigned. Reviews are held ahead of the expiry date or sooner where there is an identified issue.

All policies follow a governance route for approval, being approved by one of the following:

Local School Committee (LSC)
Audit and Risk Committee (ARC)
Finance and Resources Committee (FRC)
Trust Board (TB)

Key policies are published to the DET/School websites, as appropriate, for transparency.

b. Roles

DET/Its Schools have a named Data Protection Officer who is Lauri Almond. This Officer executes the role by reporting the outcome of statutory process to:

Chase High School – Jamie Foster – Headteacher (HT)
Larchwood Primary School – Steve Bowsher – HT
St. Martin’s School – Ian Smyrk – HT

who act as the Senior Information Risk Owners (SIRO) for the respective DET Schools.

c. Training

DET and its Schools regularly review employee roles to ensure that training and awareness messages are appropriate to the nature and sensitivity of the data processing undertaken. Induction processes ensure that new employees receive appropriate training before accessing personal data, and all other employees

receive refresher training annually. All training received is documented for evidence purposes.

d. Risk Management & Privacy by Design

DET and its Schools identify information compliance and governance risks on a central DET Risk Register.

Risks are assigned clear ownership, scored against a 5x5 matrix and appropriate mitigations and control measures are identified.

The Risk Register is reviewed twice each term by the HTs, once each term by ARC and, at least, annually by the TB.

e. Contractual Controls

All Data Processors handling personal data on behalf of DET/its Schools have given assurances about the compliance of their processes; either through procurement assurances/evidence, contractual agreement controls, risk assessments or supplementary statements.

f. Physical Security

All employees or contractors, who have access to DET/School premises where personal data is processed are provided with Identity Cards, which validate their entitlement to access. DET and its Schools operate processes, which ensure that only those individuals, who have an entitlement to access premises, are able to.

Access to physical storage, holding sensitive personal data, is further restricted either through lockable equipment with key or code control procedures or through auditable access to specific rooms/areas of buildings.

g. Security Incident Management

DET/its Schools maintain a Security Incidents Policy which, with the support of appropriate training, defines what constitutes a breach of these security measures to facilitate reporting of incidents.

The process covers investigation of incidents, risk rating and decisions over whether to notify an incident to the Information Commissioner's Office (ICO) within the statutory timescale.

Incidents are reported to HTs and the Executive Headteacher (EHT) and actions are consistently taken and lessons learned implemented.

Additionally, DET has a Reporting Serious Incidents Procedure, which encompasses Data Protection breaches.

2. Technical

a. Data at Rest

i. Use of Hosting Services

Some personal data is processed externally to DET/School-managed environments by third parties in data centres under agreed terms and conditions, which evidence appropriate security measures.

ii. Firewalls

Access to DET/School-managed environments is protected by maintained firewalls.

Business needs to provide access through the firewall go through a strictly documented change control process, which includes risk assessment and approval.

iii. Administrator Rights

Enhanced privileges associated with administrator accounts are strictly managed.

Administrator activities are logged and auditable to ensure activity can be effectively monitored.

iv. Access Controls

Access permissions to personal data held on IT systems is managed through role-based permissions.

Managers of appropriate seniority inform IT professionals of additions, amendments and discontinuation of individual accounts within permission groups.

Managers are periodically required to confirm that current permissions for which they are the authoriser and employees associated with these permissions are accurate.

v. Password Management

DET/its Schools require a mandatory password complexity combination of minimum length and characters, plus a required change of password after 90 days.

vi. Anti-Malware & Patching

DET/its Schools have a documented Change Control process, which facilitates the prompt implementation of any security updates provided by the suppliers of active software products.

vii. Disaster Recovery and Business Continuity

As part of the individual DET Schools' Business Continuity Plans, there is provision to ensure that effective processes are in place to both safeguard personal data during a service outage incident and to re-establish secure access to the data to support data subject rights in ongoing service provision.

viii. Penetration Testing

An annual penetration test is carried out to identify any weaknesses and potential areas of exploitation to maximise the security of the data we hold.

b. Data in Transit

i. Secure email

DET/its Schools have access to secure email software for communicating with some third parties where licensing agreements permit this. Sensitive data is sent using such tools where available.

Where software is not available, a system of password protecting sensitive data in email attachments is employed.

ii. Secure Websites

DET/its Schools have access to third party websites, which allow for secure upload of personal data. DET/its Schools use these facilities to fulfil statutory obligations to report personal data to other public authorities.

iii. Encrypted Hardware

Devices, which store or provide access to personal data are secured by password access.

Removable media such as memory sticks are encrypted.

iv. Hard-Copy Data

The removal of personal data in hard-copy form is controlled by DET/School policy, which requires employees to take steps to conceal the data and appropriately secure the data during transport.

These security measures are reviewed annually and approved as accurate and appropriate by ARC.