Security Measures Procedures

2025 - 2026

Version	**4**
Document authors	**Sam Proctor**
Other contributors	**IGS**
Procedures produced (date)	**December 2025**
Procedures to be reviewed (date)	**December 2026**
Other related policies	**Data Protection Policy** **Data Handling Security Policy** **Data Breach Policy** **Complaints Policy** **Procedures for Reporting and Handling Security Incidents Policy** **Whistle-blowing Policy**

Change Log

Changes made in February 2025
1.d – Addition of DPIA for any new technologies that complete sensitive processing 1.e – Changes made 2 B i.v - Further clarification has been added.
Changes made in December 2023
1.f – Further clarification has been added. 2.a.i Further clarification has been added. 2.a.ii Firewall Section has been added. 2.a.viii Penetration Testing / Vulnerability Scanning section has been added. 3.b - Data in Transit – Further clarification has been added. Reference of Security Incident Policy has been removed and replaced with Data Breach Policy
Changes made in December 2022
New policy created.

Roles within the school

Data Protection Officer (DPO) - IGS

Senior Information Risk Owner (SIRO) - Mr. S. Proctor

Information Champion (IC) - Mrs. J. Pitcher

Information Governance Governor - Mrs. S. Stronach

1. Organisational

a. Policies & Documented Procedures

Policies relating to information governance issues are drafted by employees with detailed knowledge of legal requirements and the Organisation's processes. 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. Key policies are published to the organisation's website for transparency.

b. Roles

The organisation has a named Data Protection Officer who is IGS. This Officer executes the role by reporting the outcome of statutory process to Mr. S. Proctor who acts as the organisation's Senior Information Risk Owner (SIRO). Mrs. S. Stronach is the school's Information Governor.

The school has a Data Protection Lead (DPL) Mrs. J. Pitcher who ensures the school complies with all data protection policies and procedures and manages the administration of data protection matters, reporting to the SIRO.

c. Training

The organisation regularly reviews our employee roles to ensure that training and awareness messages are appropriate to the nature and sensitivity of the data processing undertaken. Induction processes ensure 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

The organisation identifies information compliance risks on its risk register. Risks are assigned clear ownership, rated against a consistent schema; appropriate mitigations are identified and are annually reviewed. Data Protection Impact Assessments are completed for any sensitive processing or any new technologies.

e. Contractual Controls

All Data Processors handling personal data on behalf of the school are subject to contractual obligations or other legally binding agreements.

f. Physical Security

All employees or contractors who have access to our premises where personal data is processed are provided with Staff or Visitors' badges which validate their entitlement to access. The organisation operates processes which ensure 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. Data Breach Management

The organisation maintains a security incident process (Security Incident 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 the school's SIRO (Mr. S. Proctor) or the DPL (Mrs. J. Pitcher) and actions are consistently taken and lessons learned implemented.

2. Technical

a. Data at Rest

i. Use of Hosting Services

Some personal data is processed externally to the organisation's managed environment by third parties in data centres under agreed terms and conditions which evidence appropriate security measures and compliance with the law.

ii. Firewalls

Access to the Organisation's managed environment is protected by maintained firewalls. Business needs to provide access through the firewall go through a strictly documented change control process which include 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. Members of the Senior Leadership Team and key administrative staff (including the school's IT technician) are the only personnel that have access to the administrator accounts.

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

The organisation requires a mandatory password complexity combination of minimum length and characters, plus a required **change of password after each term** (approximately 90 days).

vi. Anti-Malware & Security Updates

The organisation IT support assistant promptly implements any security updates provided by the suppliers of active software products. Anti-malware programs scan our computer system to prevent, detect and remove malware. The organisation has 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 & Business Continuity

As part of the organisation's business continuity plan, there is provision to ensure 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. The business continuity plan is reviewed and updated on an annual basis. Copies of the plan are kept one is located in the school safe, OneDrive and kept a copy is kept securely off-site (Belmont Castle).

viii. Penetration Testing / Vulnerability Scanning

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

Our broadband connections have vulnerability scanning in place to detect and protect our network.

b. Data in Transit

i. Secure email

The organisation has access to secure email software for communicating with some third parties where licensing agreements permit this. Sensitive data will be 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

The organisation has access to third party websites which allow for secure upload of personal data. The organisation uses 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 organisational 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 the organisation's governance process.

School Data Protection Role Contact Details

Role	Name	Email contact
Data Protection Officer (DPO)	IGS	IGS@essex.gov.uk
Senior Information Risk Owner (SIRO)	Mr. S. Proctor	admin@westthurrockacademy.co.uk
Data Protection Lead (DPL)	Mrs. J. Pitcher	admin@westthurrockacademy.co.uk
Information Governance Governor	Mrs. S. Stronach	Chair@westthurrockacademy.co.uk