Davenant Foundation School

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 & Documented Procedures

Employees, with detailed knowledge of legal requirements and Davenant Foundation School's processes; draft policies relating to information governance issues. (IGS templates to support) 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 on the organisation's website for transparency.

b. Roles

Davenant Foundation School has a named Data Protection Officer who is Lauri Almond from Essex County Council. This Officer executes the role by reporting the outcome of statutory process to Adam Thorne (Head Teacher) who acts as Davenant Foundation School's Senior Information Risk Owner (SIRO).

The school has a Data Protection Lead, Genevieve Casson (Compliance Officer) 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

Davenant Foundation School regularly reviews 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

Davenant Foundation School identifies information compliance risks on its risk register. Risks are assigned clear ownership, rated against a consistent schema, (IGS approved) appropriate mitigations are identified and are annually reviewed.

Davenant Foundation School has a robust Privacy Impact Assessment Process and Data Privacy Impact Assessments (DPIA) are completed, where required.

e. Contractual Controls

All Data Processors handling personal data on behalf of Davenant Foundation 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 Identity Lanyards, which validate their entitlement to access. Davenant Foundation School operates processes, which ensure only those individuals who have an entitlement to access our 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 and/or areas of buildings.

g. Data Breach Management

Davenant Foundation School maintains a data breach process, 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 breaches, risk rating and decisions over whether to notify an incident to the Information Commissioner's Office (ICO) within the statutory timescale. Breaches are reported to senior leaders, 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 Davenant Foundation School'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 Davenant Foundation School managed environment is protected by maintained firewalls.

iii. Administrator Rights

Enhanced privileges associated with administrator accounts are strictly managed. (For example: Management Information System -SIMS) Managers of appropriate seniority hold administrator rights.

iv. Access Controls

3. Access permissions to personal data held on IT systems is managed through the IT department on a user-by-user requirement basis. Managers of appropriate seniority inform IT professionals of additions, and amendments of staff accounts, where required. Davenant Foundation School staff work to the principle of **HOURS.** Data is:

Held securely and confidentially
Obtained fairly and efficiently
Used effectively and ethically
Recorded accurately and reliably

Shared appropriately and lawfully.

i. Password Management

Davenant Foundation School requires a mandatory password complexity combination of minimum length and characters (the minimum number of characters is now set to 12.)

ii. Anti-Malware & Security Updates

Davenant Foundation School operates a best practice of an ‘as and when’ requirement process, highlighted by users of the system (for example: SIMS), which facilitates the prompt implementation of any security updates and/or feature updates provided by the suppliers of active software products.

iii. Disaster Recovery & Business Continuity

As part of Davenant Foundation School’s Incident Management Plan, there is provision to ensure, effective processes are in place, to safeguard personal data during a service outage incident. (Physical lockdown of data) Network security from a secondary location may be required to re-establish secure access for processing data services and systems access (permissions, data and servers) subject to re-location.

iv. Penetration Testing / Vulnerability Scanning

Penetration testing is carried out to identify any weakness and potential areas of exploitation to maximise the security of the data we hold.

Davenant Foundation is a member of the Police Cyber Alarm helping the school to better secure our systems through active cyber intelligence.

b. Data in Transit

i. Secure Digital Communications

Davenant Foundation School 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

Davenant Foundation School has access to third party websites, which allow for secure upload of personal data. Davenant Foundation School uses these facilities to fulfil statutory obligations to report personal data to other public authorities. (For example: work force census)

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 Davenant Foundation School's Data Handling Security 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.