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

    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 Lauri Almond (IGS). This Officer executes the role by reporting the outcome of statutory process to Saffron Academy Trust Executive Headteacher who acts as the organisation's Senior Information Risk Owner.

    Each school in the Trust has a Data Protection Lead 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 Identity Cards 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 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 senior leaders 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 documented change control process which include risk assessment and approval.
The organisation will carry out monthly penetration testing, done by a third party company. Recommended changes will then be implemented.

iii. Administrator Rights

Enhanced privileges associated with administrator accounts are strictly managed. Only Managers have access to this.

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 365 days. A password change is required periodically.

vi. Anti-Malware & Security Updates

Anti-malware programs scan our computer system to prevent, detect and remove malware. The organisation has an automatic update process that checks and scans for security updates and automatically applies these out of hours on a daily basis.

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.

viii. Penetration Testing

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 networks.

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

The organisation does not allow for data to be stored on hardware that is portable. 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.