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

    [Your approach to developing policy and procedures, approving, publishing and reviewing]

    [Example:] 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

    [Confirm that key roles are assigned, including DPO, SIRO etc and include role profiles]

    [Example:] The organisation has a named Data Protection Officer who is [Insert name]. This Officer executes the role by reporting the outcome of statutory process to [Insert name] who acts as the organisation's Senior Information Risk Owner.

The school has a Data Protection Lead [insert name] 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

[Induction training and refresher training. Training needs identification and reviews. Monitoring of mandatory training]

[Example:] 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 staff receive mandatory cyber security training annually. All training received is documented for evidence purposes.

d. Risk Management & Privacy by Design

[Risk assessments and Risk Register. Review of risks. Privacy Impact Assessment process. Approval. Reviews]

[Example:] 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

[Standard contract clauses. Policy requirements for suppliers. Procurement process. Non-Disclosure Agreements]

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

f. Physical Security

[Provisions for restricting access to the premises. Restricting access to paper records and data storage hardware]

[Example:] 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

[Policy and process around incident management]

[Example:] The organisation 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 incidents, risk rating and decisions over whether to notify a breach to the Information Commissioner's Office (ICO) within the statutory timescale and the National Cyber Security Centre (NCSC) for cyber security incidents. Breaches 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

[Confirm if data is hosted by a 3rd party and in which country their datacentres are located. Their basic provisions for securing data]

[Example:] 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

[Whether you have data protected by maintained firewalls]

[Example:] 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

[The management of accounts which have high levels of control over the data and other accounts]

[Example:] 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

[The management of who can access what data and how their activities are controlled]

[Example:] 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

[Statement on password complexity and frequency of change]

[Example:] The organisation requires a mandatory password complexity combination of minimum length and characters, plus a required change of password after 90 days.

vi. Anti-Malware & Security Updates

[Statement on how software is maintained to reduce external threats]

[Example:] 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

[Confirm that arrangements are in place to continue delivery of services in the event of a major disruption, and recovery plans]

[Example:] 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 / Vulnerability Scanning

[Confirm that arrangements are in place to carry out an annual penetration test]

[Example:] 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.

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

ix. Multi-Factor Authentication (MFA)

[Confirm that arrangements are in place to set up MFA]

[Example:] MFA is enabled on all employee accounts and across all applicable systems/cloud-based systems.

x. Network Backups

[Confirm that arrangements are in place for the network to be backed up]

[Example:] Network backups are kept off site in a separate location, segregated from our live environment.

b. Data in Transit

i. Secure Digital Communications

[Availability of specialist email services to securely transfer data]

[Example:] The organisation has access to software which supports secure digital communication. 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

[Use of secure features of websites which allow you to upload and download data securely]

[Example:] 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

[Use of encryption on portable hardware such as laptops, tablets, mobile phones, memory sticks, hard drives etc]

[Example:] 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

[Steps taken to secure paper records in transit]

[Example:] 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.