SECURITY MEASURES

Date of Issue	July 2024

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 Processors 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 Basildon Academies website for transparency.

    b. Roles

    The Basildon Academies has a named Data Protection Officer who is Lauri Almond. This Officer executes the role by reporting the outcome of statutory process to Mr Gary Smith who acts as the organisation's Senior Information Risk Owner.

    c. Training

    The Basildon Academies 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 Basildon Academies 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. Security Incident Management

The Basildon Academies 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 breaches. The process covers investigation of breaches, risk rating and decisions over whether to notify a breach to the Information Commissioner's Office (ICO) within the statutory timescale. 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

Some of the Academies data is cloud based, the Data is currently stored within the EU, (Ireland) and in the UK. The providers meet current EU guidelines for data security.

ii. Firewalls

Access to The Basildon Academies managed environment is protected by maintained firewalls. These systems are maintained by the provider to ensure that the connections are secure.

iii. Administrator Rights

Enhanced privileges associated with administrator accounts are strictly managed. MIS logs all access by users according to their access level. Email system is provided via Office 365, this platform logs all admin access, 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 departments inform IT support of changes to staff roles, changes to permissions are applied accordingly, amendments or discontinuation of individual accounts are carried out by the appropriate systems administrators eg, Finance, HR, Progresso etc.

v. Password Management

We recommend that when choosing a password it should meet the following minimum requirements.
a, At least eight characters long
b, Contains at least one upper case character
c, Contain one of the following “£ $ % & @ # , ; ~”
Staff can are able to change their password at any time.
All new accounts are force to change the default password.
All users are able to change their password at any time.

vi. Anti-Malware & Patching

New deployment builds are created as they become available from Microsoft, this reduces the number of updates needed to patch any one system. Our Firewall is configured to block unwanted connections. Our Firewall and antivirus systems are maintained by the appropriate providers.

vii. Disaster Recovery & Business Continuity

As part of the Basildon Academies business continuity plan, there is provision to ensure effective processes are in place to 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

Penetration tests are carried out at regular intervals 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 Digital Communications

The academy 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

The Basildon Academies 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 should be protected with a password. Removable media such as memory sticks should be encrypted with a system such a Bit Locker.

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.