Great Baddow High School

Approved by	Business Manager
Date Approved	24.05.18
Version	1.0

DATA SECURITY STATEMENT

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 knowledge of legal requirements and the school 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 school website for transparency.

    b. Roles

    The school has a Data Protection Officer - Lauri Almond (Essex County Council) and our Senior Information Risk Owner is the Headteacher

    c. Training

    The school 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 school identifies information compliance risks on its risk register. Risks are assigned clear ownership, rated against a consistent scheme, appropriate mitigations are identified and are annually reviewed

    e. Contractual Controls

    All Data Processors handling personal data on behalf of the school have given assurances about the compliance of their processes; either through procurement assurances/ evidence, contractual agreement controls, risk assessments or supplementary statements.

f. Physical Security

All Employees, Sixth Form students not in uniform and all contractors and visitors are garnished with an identification cards, some with photo ID. The school operates policies which ensure only those individuals who have an identification card are able to access the premises. Individuals without visible identification cards are challenged.

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.

Portable devices are to be locked away in appropriate locations or secured with security cables to prevent theft.

Hardcopy data is stored securely in lockable cabinets, cupboards and offices. Access is restricted to high risk data areas. Hardcopy is disposed of using secure shredding methods.

g. Security Incident Management

The school 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

All 3rd-party data hosts are vetted under the standard policies in place for data storage. Data hosting is preferred in the UK where possible, else can only be stored in a European Union member state(s) under GDPR guidelines.

ii. Firewalls

The school utilises firewalls to ensure integrity of its systems, these firewalls must have active support contracts in-place to ensure the latest security exploits and vulnerabilities are patched and the school has third-party support as and when required.
Individual devices when leaving the school premises will have localised software firewalls in place provided by the host operating system.

iii. Administrator Rights

Are restricted to one small team. No one team member has over-all control.
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 seniority inform network managers 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

For our core systems, passwords must meet minimum complexity criteria.
Where applicable this is applied to other systems where technically possible.
Additional security on users' own device is enforced when connected to our e-mail or other hosted systems.
Where passwords are required for additional systems hosting sensitive data a separate password is require which is not the same as primary passwords.

vi. Anti-Malware & Patching

All applicable systems have anti-virus/malware software installed which is centrally managed for compliance and updating purposes.

vii. Disaster Recovery & Business Continuity

As part of the school 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.

b. Data in Transit

i. Secure email

Any e-mail marked with it sensitivity level as Confidential and sent to any external addresses will automatically be marked and secured by our secure e-mail software platform.

ii. Secure Websites

SSL encryption enforced by default on all public facing website and digital services.

iii. Encrypted Hardware

Encryption tehcnologies are enforce on all laptops that hold personal data, we also enforce encryption of removable devices on staff laptop and desktop machines. Other mobile devices will have encryption enable depended on its usage and likely hood to store personal data. Personal devices use to connect to our e-mail system will be forced to encrypt their device before they can retrieve e-mails.

iv. Hard-Copy Data

The removal of personal data in hard-copy form is controlled by school policy which requires employees to take steps to conceal the data and appropriately secure the data during transport.

Copyright Statement