Information Governance Support

Essex County Council

Approved by	
Date Approved	13 February 2020
Version	1.0
Review Date	Feb 2021

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 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 the School Business Manager, supported by advice from Essex County Council's Information Governance Support service.
    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 school's website for transparency.

    b. Roles

    Howbridge Junior School has a named Data Protection Officer who is Lauri Almond at Essex County Council Information Governance Support. This Officer executes the role by reporting the outcome of statutory process to Lisa Dale (Head Teacher) who acts as the organisation's Senior Information Risk Owner.

    c. Training

    We regularly review 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

    We identify information compliance risks on our risk register. Risks are assigned clear ownership, rated against a consistent schema, appropriate mitigations are identified and are annually reviewed.

    e. Contractual Controls

    All Data Processors handling personal data on behalf of Howbridge Junior 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 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 school 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 through lockable equipment with key control procedures.

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

Some personal data is processed externally to the school's managed environment by third parties in data centres under agreed terms and conditions which evidence appropriate security measures.

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 strictly documented change control process which include risk assessment and approval.

iii. Administrator Rights

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

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 90 days.

vi. Anti-Malware & Patching

Schools Broadband maintain and periodically renew McAfee anti-virus software on the organisation's IT infrastructure.

vii. Disaster Recovery & Business Continuity

As part of the school'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.

b. Data in Transit

i. Secure email

The 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.
Currently used secure email software is Egress / Switch, used to communicate with some services within Essex County Council.

ii. Secure Websites

The school has access to third party websites which allow for secure upload of personal data. The school uses these facilities to fulfil statutory obligations to report personal data to other public authorities.
Currently used websites providing secure upload are sites within the DfE's Secure Access web facility.

iii. Encrypted Hardware

Devices which store or provide access to personal data are secured by password access. Removable media such as memory sticks are not to be used unless encrypted.
Our Data Handling Security policy lists the steps employees are required to take to keep data secure on portable hardware.

iv. Hard-Copy Data

The removal of personal data in hard-copy form is controlled by our 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 school's governance process.