Information Governance Support

Essex County Council

Approved by	Local Information Board
Review Date	Review in line with IGS requirements

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 Experts with detailed knowledge of legal requirements and East Tilbury Primary 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 East Tilbury Primary School website for transparency.

    b. Roles

    East Tilbury Primary School ‘s Data Protection Officer executes the role by reporting the outcome of statutory process to The Headteacher who acts as East Tilbury Primary School’s Senior Information Risk Owner. The school also has a number of Information Champions and a local Information GovernanceBoard.

    c. Training

    East Tilbury Primary School regularly reviews 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 is the online EVERY system where staff sign documents electronically to say they have read and understood.

    d. Risk Management & Privacy by Design

    East Tilbury Primary School 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 East Tilbury Primary 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. East Tilbury Primary 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 either through lockable equipment with key or code control procedures or through auditable access to specific rooms/ areas ofbuildings.

g. Data Breach Management

East Tilbury Primary School 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 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 East Tilbury Primary 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 East Tilbury Primary School's managed environment is protected bymaintained firewalls. Business needs to provide access through the firewall go through a strictly documented change control process which includes 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

East Tilbury Primary School requires a mandatory password complexity combination of minimum length and characters, plus a required change of password after 6 months.

vi. Anti-Malware & Security Updates

East Tilbury Primary School has a documented change control process whichfacilitates the prompt implementation of any security updates provided by the suppliers of active software products. Anti-malware programs scan our computer system to prevent, detect and remove malware.

vii. Disaster Recovery & Business Continuity

As part of East Tilbury Primary 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.

viii. Penetration Testing

An annual vulnerability test is carried out to identify any weaknesses and potential areas of exploitation to maximise the security of the data we hold.

b. Data in Transit

i. Secure email

East Tilbury Primary School has access to secure email software for communicating with some third parties where licensing agreementspermit 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

East Tilbury Primary School has access to third party websites which allow for secure upload of personal data. East Tilbury Primary School uses these facilities to fulfil statutory obligations to report personal data to otherpublic authorities.

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 allowed on the school network.

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 East Tilbury Primary School's governance process.