Security Measures Guidance

Date Drafted: **May 2018**

Date of Next Review: **Summer 2019**

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 organisation's website for transparency.

b. Roles

The organisation has a named Data Protection Officer who is

Postal Address	Essex County Council. County Hall. Chelmsford. CM1 1QH
Email	IGS@essex.gov.uk
Phone Number	03330322970

This Officer executes the role by reporting the outcome of statutory process to the Headteacher who acts as the organisation's Senior Information Risk Owner.

c. Training

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 training received is documented for evidence purposes.

d. Risk Management & Privacy by Design

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.

e. Contractual Controls

All Data Processors handling personal data on behalf of the organisations 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 Badges 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 organisation 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

School Data is hosted on the School premises
School website is hosted by e4education.

ii. Firewalls

The school firewall is provided and maintained by Daisy Updata on behalf of Essex County Council

iii. Administrator Rights

Administrator accounts are managed so that only the people that require administrator access know any login details.

A hardcopy of the access information is held in the school safe for emergency purposes.

iv. Access Controls

IT Administrators along with Management staff allow and restrict access as required for staff and pupils

v. Password Management

Passwords for staff are enforced and they are changed every 122 days, with a minimum of 6 characters.

vi. Anti-Malware & Patching

Anti Malware\Anti Virus software is installed on all Servers & Computers using Essex County Council supplied McAfee Total Protection

vii. Disaster Recovery & Business Continuity

Both Admin and Curriculum servers have daily local Bare Metal Recovery backups to external hard drives which are swapped on a weekly basis by a nominated staff member. The Admin network is also backed up daily to Attix 5 Online backup supplied by Essex County Council. ICT Support (DL Solutions) does periodic test restores from all three backups to ensure data is recoverable,

b. Data in Transit

i. Secure email

The school are implementing a system where any email attachments with potentially sensitive data will only be sent once zipped and encrypted using 7Zip or via the Egress system

ii. Secure Websites

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

School staff should use Encrypted Memory sticks and the ICT Support are currently upgrading all teacher laptops which go off site to Windows 10 and enabling BitLocker Encryption

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