GDPR Strategy Messing Primary School

Approved by	LGB
Date Approved	Spring 2022
Version	1
Review Date	Spring 2024 (Unless updated)

Contents

1. Introduction

Information is a valuable asset that requires effective management. This strategy is intended to assist the organisation to manage information appropriately and get best value from information assets.

The benefits of the strategy are:

- Efficiency through the more effective use of physical, electronic and human resources
- Better service delivery through improved access to relevant information making requests easier to handle in a shorter time.
- Environmental benefits by reducing reliance on paper files and physical storage.
- A better working environment through the removal of irrelevant information and documentation allowing staff easier access to the information required to perform their work.
- Improved compliance with legal requirements boosting reputation.

The IG Strategy aims to:

- Standardise the processing of information throughout its lifecycle
- Minimise the number of locations and formats in which information is created and retained
- Ensure that staff, Governors/Trustees, partners and the public have easy access to information in accordance with their rights of access
- Ensure that information is retained only if it serves a legal or business requirement.

2. Scope

The IG Strategy provides a framework for implementing IG Policy. The implementation and delivery of the IG Strategy, however, is the responsibility of all employees. IG cannot be viewed as a purely as an IT or legal compliance issue.

3. Roles & Responsibilities

Every employee creates recorded information and so all are responsible for its effective management. Without the engagement and involvement of employees at all levels, this strategy will fail. This can be achieved through establishing clear responsibilities for information management, effective communications and performance management.

IG also requires a clear management hierarchy to ensure that implementation of the strategy is given strategic direction, policies can receive appropriate approval and performance is monitored. Roles and their responsibilities are essential to successful delivery.

Senior Information Risk Owner (SIRO) – usually the Headteacher

- Risk Management Lead
- Strategic Direction
- Determines response to legislative and other developments
- The monitoring of Information Management (IM) performance and development of standards
- Co-ordination with related Projects/initiatives

Data Protection Lead

- Lead for IG issues and communications
- Responsible for operational IG issues and first instance guidance on information policies
- Identifying and reporting IG issues/concerns
- Report to Governing Board on Information Management matters when required
- Key stakeholder for Internal/ External Data Protection Audits
- Record, manage and report on security incidents

Oversight Board – Governors/Trustees

- The oversight and approval of implementation of this Strategy and compliance with information legislation
- The monitoring of IM performance and development of policy/procedures
- Review and approve IG policies

Data Protection Officer (IGS)

- Monitor compliance with information legislation
- Provide advice & guidance on same
- Provide an annual audit & report on compliance
- Oversee training and awareness for staff
- Support serious security incident process
- Approve Data Protection Impact Assessments and Information Sharing Protocols
- Act as first point of contact for supervisory authority (ICO)
- Provide advice to the organisation on data protection complaints from the public

4. Policy Framework

The IG Policy Framework includes the following policies:

Statutory Requests for Information

- Providing for public requests for access to information held under FOIA, DPA/GDPR and EIR.
- It will also support the Transparency agenda

Data Protection

- Regulating and monitoring the processing of personal data

Data Handling Security

- How data should be handled to best ensure its security

Records Management

- Ensuring records are managed in line with legal and business requirements

Security Incident

- Handling a security incident involving the organisations information

Acceptable Personal Use

- Acceptable use of the organisations resources and assets, including IT facilities and covering personal use

Biometric (where applicable)

- Responsibilities for the collection and management of biometric information

A review of policies should take place annually and any changes need the approval of the Headteacher and Governors/Trustees.

Staff should agree in writing annually that they have read, understood and agree to abide by the organisations policies. This may be achieved as part of the sign in process at the start of each academic year.

Action Required

- Annual Review of policies, taking into account any security incidents related to the policy and any feedback from staff
- Updates as required to be captured on the policy log
- Documentary evidence that staff have read, understood and agree to abide by the organisations policies.

5. Records Management

The cornerstone of good IG is effective records management. Records management means the systems adopted to control and manage the creation, use, retention and

disposal of information in a way that is administratively and legally compliant but also serves operational needs. Effective records management will ensure that information is available when and where it is needed, in an organised and efficient form and that unneeded information is filed, archived or disposed of as appropriate. Conversely, poor records management results in the superfluous retention of redundant electronic and paper information, the loss of information and poor access to relevant information.

Our information policies ensure that we set the correct expectations for our staff, who are required to confirm that they will comply with them.

Effective records management requires us to accurately know what information we hold at any point in time. The Freedom of Information Act 2000 requires us to have a publication scheme of all publicly available information held. To ensure consistency and reduce duplication, an Information Asset Register is required which will:

- Comply with the organisation's retention period and necessary action at disposal (e.g. destroy or pass to the local Archive facility, for example if a school closes they should offer records to the Essex Records Office for public archiving). (See D8 – Retention Schedule)
- Detail the flows of personal data and establishing whether the processing complies with the requirements of the GDPR (see H1 RoPA)

6. Communications and Training

There are clear benefits to effective IG but it will involve time and effort by all employees. Communications and training are required to:

- Raise awareness of the strategy
- Engage and involve staff
- Train on new policies and procedures as they are implemented
- Establish annual refresher training on Information Governance/Data Protection
- Ensure training is role based to ensure an effective level of training is received

7. Monitoring and Review

An annual review should be conducted to ensure that your day to day management of information aligns to the requirements of this strategy and information policies.