MissionGrove
PRIMARY SCHOOL
RESPECT YOURSELF RESPECT OTHERS

Digital and ICT Security Policy

Mission Grove Primary School

This Policy has been written for and adopted by
the Governing Body of Mission Grove Primary School, adopted from the London Borough of Waltham Forest Policy, dated 2019

VISION STATEMENT

For the children at Mission Grove to become well rounded individuals who have drive, passion and the confidence to do their best. Who leave with the skills to succeed and flourish in life. Staff have high expectations of themselves and others and are reflective practitioners. Mission Grove provides security, opportunities and enjoyment for all.

Date Written :

Approved by Governing Body

Date : December 2023

Review Date : Annually

DIGITAL AND ICT SECURITY POLICY

VERSION HISTORY

Version	Date Issued	Brief Summary of Change	Author
4.0	07/02/2013	Revised to align with current council business strategy and processes	Ikenna Akpom
4.1	19/03/2013	Updated with comments from the Audit and Anti-fraud unit	Ikenna Akpom
4.2	16/04/2013	Released document following approval	Ikenna Akpom
4.3	06/08/2015	Revised to align with current council business strategy and processes	Claire Brookes-Daniels
4.4	2709/2016	Revised to align with current council business strategy and processes	Paul Ubaka
4.5	18/11/2019	Revised to align with current council business strategy and processes	Matthew Crabb

DOCUMENT APPROVAL

Version	Date Approved	Description of Approval	Approver
4.3	06/08/2015	Approved by CIO Chair of IG Board in the interim until IG Board met in Sept	Paul Golland
4.5	04/12/2019	Annual review	IGB

DOCUMENT LOCATION

Document Location	File Name
S:\	

Contents

Introduction

Digital and ICT has developed significantly in the last decade and the local authority and Mission Grove Primary School are embracing the opportunities offered by existing and new technology for delivering services, enhancing engagement and communicating with staff, pupils and all stakeholders.

Information security means safeguarding information from unauthorised access or modification to ensure its;

- **Confidentiality;** ensuring the information is accessible only to those authorised to have access.
- **Integrity;** safeguarding the accuracy and completeness of information by protecting against modification.
- **Availability;** ensuring that authorised users have access to information and associated assets when required.

Information is an important asset, Mission Grove Primary School is committed to preserving the confidentiality, integrity and availability of our information assets;

- For decision making;
- To deliver quality services;
- To comply with the law;
- To meet the expectations of our stakeholders;

Purpose

The purpose of the Information Security policy is to protect the school's information, to manage risk and reduce it on an acceptable level, while facilitating reasonable use of information in supporting normal business activity and that of our stakeholders.

This will be achieved by:

- Ensuring the confidentiality, integrity and availability of information and information assets belonging to Mission Grove Primary School;
- Maintaining compliance with relevant UK Legislation;
- Maintaining compliance with third party Codes of Connection, for example Public Services Network;
- Ensuring all staff are aware of their responsibilities relating to the security of information;

Scope

This policy applies to all staff, permanent and temporary, contractors, and agents who use or have access to school information, computer & mobile devices, or ICT facilities.

This policy applies throughout the lifecycle of the information from creation, storage and use to disposal. It applies to all information including:

- Information stored electronically on databases or applications e.g. email.
- Information stored on computers, laptops, mobile devices, printers or removable media such as hard disks and memory sticks and other similar media.
- Visual and photographic material including CCTV.
- Information transmitted on network and other communication networks.

- Spoken, face-to-face, voicemail & recorded conversations.

Objective

The main objective of this policy is to describe the measures in place to manage information security appropriately to support the council's capacity to deliver efficient services. The policy comprises the following:

- Measures in place to ensure national legal compliance
- State information security policy measures in place
- Good information security assurance mechanisms are in place
- Duties and responsibilities are in place

Legal Requirements

Users of the school's information assets will abide by UK legislation relevant to information security including:

- Data Protection Act 2018
- Computer Misuse Act 1990
- Electronic Communications Act 2000, Copyright, Designs and Patent Act 1998
- Human Rights Act 1998 Regulation of Investigatory powers Act 2000
- Telecommunications (Lawful Business Practices) regulation 2000
- Civil Contingencies Act 2000
- Freedom of Information Act 2000

And any specific protection standards relevant to the schools business such as the Payment Card Industry Data Security Standards (PCI DSS). This list is not exhaustive and may change over time

Supporting policies, standards and guidance

This policy is supported by more detailed policies, standards and guidance; these include but are not limited to the following:

Acceptable Usage Policy
Access Control Policy

All supporting policies, standards and guidance can be found on the Intranet.

compliance

All staff, and anyone who delivers services on the school's behalf, contractors, or other third parties with access to the school's assets have a responsibility to promptly report any suspected or observed security breach.

Security breaches that result from a deliberate or negligent disregard of any security policy requirements may, result in disciplinary action being taken against that employee. In the event that breaches arise from the user who is not a direct employee of the school, the school shall take such punitive discretion that it deems appropriate.

The school may, in its absolute discretion refer the matter of any breach of the security policy requirements to the police for investigation and (if appropriate) the instigation of criminal proceedings if the reasonable opinion of the council such breach has likely or is likely to lead to the commissioning of a criminal offence.

Roles, responsibilities and duties

This section describes the expected responsibility in relation to Information Security:

Role	Responsibilities
Headteacher	The Headteacher is responsible for Information security relating to IT.
Senior Information Risk Officer (SIRO)	The SIRO has responsibility for managing information risk on behalf of the Headteacher and the Senior Management Team, setting strategic direction and ensuring policies and procedures are in place for the safe management of information.
Directors	Have the responsibility for understanding and addressing information risk within their service area, assigning ownership to Information Asset Owners (IAO) and ensuring that within their service area are appropriate arrangement in place to manage information risk, and to provide assurance on the security and use of these assets.
Information Asset Owners (IAO)	Undertake risk assessments, implement appropriate controls, recognise actual or potential security incidents and ensure that policies and procedures are followed.
Technical Design Authority (TDA)	The TDA is a specialist group that will quality assure that all system development is consistent with the ICT Strategy, TDA and security principals and standards. The TDA acts to improve control over the way systems are procured, tested and implemented.

Information Security Governance

The local authority has an established forum for the management of information governance and security, the Information Governance Board (IGB). The Board is chaired by the Data Protection Officer (DPO) and includes senior representatives of all directorates and key services.

Approach to risk management

Information risk will be managed with the Risk Management policy. The SIRO, ICT Security Architect and the Information Governance Board will have oversight of the information risk and the information risk management processes.

In accordance with the schools Risk Management Policy, the School Business Manager are responsible for ensuring critical information assets and systems are subject to information risk analysis on a regular basis. The risk assessment will ensure that; threats and vulnerabilities are identified, risks are assessed, and appropriate decisions are made regarding risk that are accepted and those to mitigate by control measures to reduce the risk to an acceptable level.

Asset Management

The school has an Asset Management Policy; for both hardware and software, which clearly defines the Digital and ICT processes and procedures endorsed by all staff in the school to ensure the safeguarding of IT Assets. The policy includes the procurement and contract requirements of third-party managed services.

User Access Management

There are documented policies and procedures for access control and privileged account management based on business role and security requirements and are reviewed on a regular basis.

The Access Management Policy contains password requirements in line with the PSN requirements and all ICT processes relating to new starters, movers and leavers for Network, Application and System access.

Network Security

Specialist security tools and techniques are in place to protect the school's network infrastructure including:

- Remote control tools for problem solving and software management
- Network monitors to detect attacks and analyse traffic
- Encryption of data to maintain confidentiality
- Restricted routing per user or network address
- Role based access control to allow only authorised users
- Protocol controls to restrict access to services and ensure data integrity

The school's IT provider shall provide the school with comprehensive documentation for network designs, security requirements and ensure these are included in service agreements, whether these services are provided in-house or outsourced.

dissemination and implementation

This policy will be made available to all staff.

The policy will be supported by additional policies and procedures to support implementation.

Monitor and review of the policy

This policy will be reviewed on annual basis, and in accordance with the following on an as and when required basis:

- In Legislative or case law changes;
- Changes or release of good practice or statutory guidance;
- Identified deficiencies, risk or following significant incidents reported;
- Changes to organisational infrastructure.