General Data Protection Regulation (GDPR)
Remote Access Mobile Computing Policy

DOCUMENT PROVENANCE			
Status	Draft	Current version no.	1.0
Organisation	NCC/NST	Version date	September 2023
Author	Jeremy Lyn-Cook/NST	Approved by (If applicable)	
Audience	Anyone	Approval date	October 2024
Security classification	OFFICIAL	Next review date	Annually

DOCUMENT CHANGE HISTORY			
Revision date	Version no.	Author of changes	Summary of changes
25.02.2021	1.1	A Williams	NST policy adapted for Southwold Primary School

Contents

Remote Access Mobile Computing Policy

1. Introduction

Southwold Primary School recognises that advances in technology around computers, tablets, mobile phones, etc. mean that these devices are becoming everyday business tools. Because the devices are highly portable and can be used anywhere, they are vulnerable to loss or theft and their unsecured operating systems means they may be hacked or used to distribute malicious software. As mobile computing becomes more common, the school needs to address the security issues it raises in order to protect its information resources.

2. Purpose

The purpose of this policy is to establish an approved method for controlling mobile computing and storage devices which contain or access Southwold Primary School's information resources.

3. Scope

All those who use mobile computing and storage devices on the school network are covered by this policy. This includes employees, pupils, consultants, contractors, visitors, etc.

4. Policy

General Policy

It is Southwold Primary School's policy that mobile computing and storage devices accessing school information resources must be approved before connecting to the school's information systems. This applies to all devices connecting to the Southwold Primary School network regardless of ownership.

Mobile computing and storage devices include, but are not limited to: laptop / tablet computers, mobile phones, plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), memory sticks/flash drives, modems, handheld wireless devices, wireless networking cards and any other existing or future mobile computing or storage device, either personally owned or school owned, that may connect to or access the information systems at the school. An assessment for each new device/media type will be conducted and documented prior to its use or connection to the network at the school unless the device/media type has already been approved.

Southwold Primary School has introduced SharePoint as a secure cloud storage system. All staff can access the school staff share drive remotely.

Mobile computing and storage devices are easily lost or stolen, presenting a high risk for unauthorised access and introduction of malicious software to the school network. These risks must be mitigated to acceptable levels before connection to the school network will be allowed.

Portable computing devices and portable electronic storage media containing confidential, personal or sensitive school information must wherever possible use encryption or other strong measures to protect the data while it is being stored.

Unless written approval has been obtained from the Data Protection Officer (DPO) and the Head Teacher databases, spreadsheets or tables of data in other applications or parts thereof, which sit on the network at Southwold Primary School, shall not be downloaded to a mobile computing or storage device.

Procedures

To report lost or stolen mobile computing and storage devices, staff should notify the school DPO. Staff members must notify the Data Protection Officer/ Head Teacher directly by phone on 0115 9155756 or by e-mail on admin@southwold.nottingham.sch.uk / headteacher@southwold.nottingham.sch.uk;

of any potential data incidents as soon as the incident occurs and in any event within 24 consecutive hours after occurrence. **It is important you receive acknowledgement of your email within 24 hours from one of the above email accounts.**

The DPO and Head Teacher shall approve all new mobile computing and storage devices that may connect to information systems at the school.

Before a non-school owned device can access the school network it must first be assessed and passed as compliant by the school's IT Support Team or such personnel working on the school's behalf.

Roles & Responsibilities

Users of mobile computing and storage devices must protect such devices from loss of equipment and disclosure of private information belonging to or maintained by the school. Before connecting a mobile computing or storage device to the network at school, users must ensure it is on the list of approved devices issued by the school's approver.

The DPO must be notified immediately upon detection of a security incident, especially where a mobile device may have been lost or stolen.

Overall the school's Governing Body is responsible for the mobile device policy at the school. On a day to day basis the school's Headteacher is responsible for the operation of the policy and they shall authorise appropriate risk analysis work to document safeguards for each media type to be used on the network or on equipment owned by the school.

They are also responsible for developing procedures for implementing this policy. The school will hold a list of approved mobile computing and storage devices.

5. Policy Compliance Measurement

The DPO and Head Teacher will verify compliance with this policy through various methods, including but not limited to, periodic school walk-throughs, video monitoring, business tool reports, internal and external audits, etc.

6. Exceptions

Any exception to the policy must be sanctioned and recorded by the Headteacher and DPO in advance.

7. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

8. Related Standards, Policies and Processes

This Policy should be read in conjunction with the following:

Data Protection Policy
Data Incidents and Breaches Policy
Freedom of Information Policy
Acceptable Use Policy
Subject Access Request Policy
Email Policy
Mobile Computing Policy
Safeguarding Policy and Guidance