



MOBILE COMPUTING POLICY - GDPR

Committee/Person Responsible for Policy	Headteacher/SLT
Date Approved by SLT/Headteacher	11th January 2023
Next Review Date:	January 2025 – updated if new guidance comes into effect

Remote Access Mobile Computing Policy

Contents

1. Introduction
2. Purpose
3. Scope
4. Policy
5. Policy compliance measurement
6. Exceptions
7. Non-compliance
8. Related policies and processes
9. Review

Remote Access Mobile Computing Policy

1. Introduction

Foxwood Academy ("the Academy") 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 (in its broadest sense) becomes more common, the Academy 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 the Academy's information resources.

3. Scope

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

4. Policy

General Policy

It is the Academy's policy that mobile computing and storage devices accessing Academy information resources must be approved before connecting to the Academy's information systems. This applies to all devices connecting to the Academy 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 Academy owned, that may connect to or access the information systems at the Academy. An assessment for each new device/media type will be conducted and documented prior to its use or connection to the network at the Academy unless the device/media type has already been approved. The Academy will maintain a list of approved mobile computing and storage devices.

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

General Data Protection Regulation (GPDR)

Remote Access Mobile Computing Policy

Portable computing devices and portable electronic storage media containing confidential, personal or sensitive Academy 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 Headteacher at Foxwood Academy, databases, spreadsheets or tables of data in other applications or parts thereof, which sit on the network at the Academy, shall not be downloaded to a mobile computing or storage device.

Procedures

To report lost or stolen mobile computing and storage devices, staff should call the Academy Business Manager.

The IT technician shall approve all new mobile computing and storage devices that may connect to information systems at the Academy.

Before a non-Academy owned device can access the Academy network it must first be assessed and passed as compliant by the Academy's IT Support Team or such personnel working on the Academy'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 Academy. Before connecting a mobile computing or storage device to the network at Academy, users must ensure it is on the list of approved devices issued by the Academy's approver.

The IT Support Team (or equivalent) must be notified immediately upon detection of a security incident, especially where a mobile device may have been lost or stolen.

Overall, the Academy's Governing Body and is responsible for the mobile device policy at the Academy. On a day-to-day basis the Academy'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 Academy.

They are also responsible for developing procedures for implementing this policy. The Academy's approving authority will maintain a list of approved mobile computing and storage devices and may make the list available on the Academy's intranet.

General Data Protection Regulation (GPDR)

Remote Access Mobile Computing Policy

5. Policy Compliance Measurement

The Academy's Senior Management Team will verify compliance with this policy through various methods, including but not limited to, periodic Academy 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 Academy's Headteacher 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

Acceptable Use Policy

Data Protection Policy