Mobile Computing Policy (UK GDPR)

January 2026

Remote Access Mobile Computing Policy

Contents

Remote Access Mobile Computing Policy

1. Introduction

Greenfields Community 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 (in its broadest sense) becomes more common, Greenfields Community 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 the school's information resources.

3. Scope

All those who use mobile computing and storage devices on Greenfields Community School's network are covered by this policy. This includes employees, contractors, visitors, supply staff and any other person or third party operating for and on behalf of Greenfields Community School.

4. Policy

General Policy

It is the school's policy that mobile computing and storage devices accessing the school's information resources must be approved before connecting to the school's information systems. This applies to all devices connecting to Greenfields Community 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 Greenfields Community 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. The school 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 Greenfields Community School network. These risks must be mitigated to acceptable levels before connection to the Greenfields Community School network will be allowed.
Portable computing devices and portable electronic storage media containing confidential, personal or sensitive Greenfields Community School information must wherever possible use encryption or other strong measures to protect the data while it is being stored.

Unless prior verbal approval has been obtained from the Headteacher, databases, spreadsheets or tables of data in other applications or parts thereof, which sit on the network at Greenfields Community 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 Data Protection Office/Headteacher on 0115 9153762 along with Schools IT on 0115 9150900 as soon as possible.

The Headteacher shall approve all new mobile computing and storage devices that may connect to information systems at Greenfields Community School. Where the Headteacher feels it necessary, he/she reserves the right to have the device assessed and passed as compliant by Schools IT Support Team.

Roles and 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 Greenfields Community School.

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

On a day to day basis the 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 Trust.

Greenfields Community School will maintain a list of approved mobile computing and storage devices.

Greenfields Community School's Senior Management Team will verify compliance with this policy through various methods, including but not limited to, periodic Greenfields Community 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 in advance.

7. Non-Compliance

Any 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

9. Review

This policy will be reviewed in January 2027 and then annually thereafter.