MELLERS PRIMARY SCHOOL

GDPR-REMOTE ACCESS AND MOBILE COMPUTING POLICY

MAY 2018

Remote Access Mobile Computing Policy

Contents

Remote Access Mobile Computing Policy

1. Introduction

Mellers Primary, ("the 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, 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 the 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 the 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 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. 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 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.

Staff may access school emails on their mobile devices as long the following security procedures are adhered to:

- The device is registered with the schools IT technician and is listed as authorised for access to the network
- It has a 6 digit passcode or fingerprint recognition access
- In the event that a device is lost whilst containing a school email account it should be reported to the DPO and then to SchoolsIT who will disable the school email account from the device.

Unless written approval has been obtained from Amanda Dawson, Headteacher, databases, spreadsheets or tables of data in other applications or parts thereof, which sit on the network at the 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 call the Data Protection Officer.

The Headteacher in conjunction with the school's IT technician 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 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 school's Governing Body and 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’s approving authority will maintain a list of approved mobile computing and storage devices and may make the list available on the school’s intranet.

5. Policy Compliance Measurement

The school’s Senior Management Team 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 school’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

9. Review

This policy will be reviewed annually.