



# General Data Protection Regulation (GDPR) Nottingham School Trust Mobile Computing Policy

May 2018

# 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

# General Data Protection Regulation (GDPR)

## Remote Access Mobile Computing Policy

### Remote Access Mobile Computing Policy

#### 1. Introduction

Nottingham Schools Trust (“the Trust”) 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 NST 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 Trust’s information resources.

#### 3. Scope

All those who use mobile computing and storage devices on the NST network are covered by this policy. This includes employees, consultants, contractors, visitors, agents and any other person or third party operating for and on behalf of the NST.

#### 4. Policy

##### ***General Policy***

It is the Trust’s policy that mobile computing and storage devices accessing the Trust’s information resources must be approved before connecting to the Trust’s information systems. This applies to all devices connecting to the NST 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 NST owned, that may connect to or access the information systems at the Trust. An assessment for each new device/media type will be conducted and documented prior to its use or connection to the network at the Trust unless the device/media type has already been approved. The Trust 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 NST network. These risks must be mitigated to acceptable levels before connection to the NST 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 NST 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 CEO in person, databases, spreadsheets or tables of data in other applications or parts thereof, which sit on the network at the NST, 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 NST on 0115 915 3701 as soon as possible. If there is an associated risk of a data breach, then NST should be informed in accordance with our Data Incident and Breach Policy, which states that the DPO must be notified **within 24 hours** on [dpo@nottinghamschoolstrust.org.uk](mailto:dpo@nottinghamschoolstrust.org.uk).

The CEO shall approve all new mobile computing and storage devices that may connect to information systems at the NST. Where the CEO feels it necessary, he/she reserves the right to have the device assessed and passed as compliant by the NST's IT Support Team or such personnel working on the NST's behalf.

#### ***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 Trust. Before connecting a mobile computing or storage device to the network at NST, users must ensure it is on the list of approved devices issued by the NST'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.

On a day to day basis the NST's CEO 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.

The NST will maintain a list of approved mobile computing and storage devices.

## **General Data Protection Regulation (GPDR)**

### **Remote Access Mobile Computing Policy**

#### **5. Policy Compliance Measurement**

The NST's Senior Management Team will verify compliance with this policy through various methods, including but not limited to, periodic NST 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 NST's CEO 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 May 2019 and then annually thereafter.