Mobile Device Policy

Policy review Date	**March 2018**
Date of next Review	**March 2020**
Who reviewed this Policy?	**Trust Governing Body**

Purpose

The widespread ownership of mobile devices by staff requires that schools take steps to ensure that mobile devices are used responsibly with the School services.

This policy ensures those potential issues involving mobile devices can be clearly identified and addressed, ensuring the benefits that mobile devices provide can continue to be utilised, balancing security with accessibility.

Staff must read and understand this policy before they sign and are given permission to use mobile devices linked to school services internally and externally and where sensitive data and information is downloaded to a mobile device.

Rationale

It is understood that staff will want to use their mobile devices to access School services such as e-mail and calendars when not connected to the internet.

There is the concern that although mobile devices are very useful they also pose a risk in relation to data security and information governance. When sensitive information is downloaded onto the phone and it is accessed by a third party.

Responsibility

It is the responsibility of staff that have mobile devices in school to abide by the guidelines set out in this document.

SLT should be informed and permission given if you wish to use a school or personal mobile device for School services that downloads data to the device.

Permission to have a mobile device using School services at school is contingent on permission in the form of a signed copy of this policy.

SLT may revoke approval at any time.

Staff are responsible for keeping the school informed of their current mobile device if any school software or services are installed on the device.

Mobile Device Policy

Acceptable Uses

Mobile devices must have a complex password containing capital letters, numbers and symbols.

All e-mails or information stored on the mobile device that relate directly to sensitive school data must be in encrypted format.

Staff members need to know how to remotely wipe their device to factory defaults if it is lost or stolen.

Staff should protect the security of their mobile device by never sharing log on details, regularly changing the complex password and locking the device when not in use.

Staff must have read the most up to date ICO phone guidance http://www.ico.org.uk/for_the_public/topic_specific_guides/online/smartphone_security

Staff should regularly back up their mobile device.

Lost or Stolen

Staff should wipe their mobile device to factory defaults if it is lost or stolen for more than 12 hours, and follow their device provider's guidance on security.

Staff should keep their mobile device locked away or concealed in a safe place that cannot be accessed by a third party.

The school accepts no responsibility for replacing lost, stolen or damaged mobile phones.

Mobile Device Policy

School Permission:

I have read and understand the above information about appropriate use of mobile phones at schools within the MAST Academy and I understand that this form will be kept on file at the school. I will be solely responsible for ensuring that my mobile phone is used appropriately and correctly as outlined in this document.

Staff Member name (print)

_____

Staff Member signature

_____

Date _____

SLT name (print)

_____

SLT signature

_____

Date _____