Orton Wistow Primary School

Mobile Device Policy

Status	Other
GB Monitor	FGB
Staff Lead	HT/DHT
Senior Lead	DHT
Publication Date	Spr 18
Next Review	Spr 20

Date Agreed:	
Headteacher:	
Chair of Governors:	

Purpose:

This policy relates to Smart Phones and Tablets, which will be hence forth referred to as 'Mobile Devices'. These Mobile Devices will be covered from two perspectives; 'Bring Your Own' (BYOD) devices and equipment owned by the school.

'Bring Your Own' mobile devices:
If an Employee is to be permitted by the school to have contact through his/her smart phone s/he is responsible for the physical security of the phone. The use of these devices must be considered as a privilege rather than a right of employment, which is allowed in line with the eight principles of the Data Protection Act. Breaches of this policy may result in the loss of said privilege. Where permitted, it is understood that usage of these devices is subject to the following:

- The device must be protected with a secure password and at no time must this be shared with anyone, especially anyone from outside of the school environment.
- Physical access to Device must be protected at all times. If lost/stolen this must be reported to the SLT at the earliest opportunity. Where possible, the employee must have taken reasonable measures to install 'remote lock and wipe' functionality on the device, or have investigated the services that their mobile provider offers in this respect.
- If relevant, the device should have Anti-Virus software installed. If the employee believes that the device has been infected then they must disable the wireless connection and report it to the SLT immediately.
- Use of the school's internet connection is primarily for educational and management purposes, therefore personal downloads are not permitted during standard working hours.
- At no point should the device be used to take and store photos of the children, access on-line education systems, or store any personal data relating to any pupils or staff at the school. If an exception is made to this then it will be temporary in nature and with the written permission of the SLT.
- Insurance and maintenance of these devices is the responsibility of the employee.
- Mobile Devices should not be used in a space where children are present/might be present e.g. Classroom, playground, after school clubs, corridors.
- Staff must have their Devices on 'silent' or switched off during class time.
- Staff may not make or receive calls during teaching time.
- If there are extreme circumstances (e.g. acutely sick relative) the member of staff may request via the SLT that they leave their Device on during working hours to receive emergency calls.
- Devices must be kept out of sight (e.g. drawer, handbag, pocket) when staff are with children and not on display.
- Calls/ texts must be made/ received in private during non-contact time.

Parents & other visitors:

- We request that parents and other visitors do not use Mobile Devices in the school building or grounds.
- Should contractors working on site need to use a Mobile Device this should only be done where children are not present and with the express permission of the member of staff accompanying them.
- Mobile Devices must never be used to take photographs in the school building or grounds without the permission of the SLT (e.g. Whole school assemblies, school performances or other such public events).

School-owned mobile equipment:
The following applies to any tablet device that it used for anything other than the exclusive use the children:

- The device must be protected with a secure password and at no time must this be shared with anyone, especially anyone from outside of the school environment. If the device is configured with named user accounts, the passwords must not be shared and changed immediately if they become known.
- Where there is shared access to the device, care should be taken to clear down the browser cache periodically.
- Where there is the possibility of school's data being held on the device for school use, the employee must request the installation of anti-virus and/or device encryption software. Any data retained on the device should only be done so in line with the school's Data Retention and ICT policies.
- No software must be installed by the employee without permission from the SLT.
- At no point should any security software installed on the mobile device be disabled, as this may compromise the device and any data held. As with all other ICT equipment, only the school's IT provider will ever ask you to carry out any tasks. Any other requests made whilst connected to the internet must be referred to the SLT.

Pupil Mobile Phones & Anti-Bullying
Pupils should not bring mobile phones onto the school site, except under exceptional circumstances when individual arrangements will be made.

Confidentiality and Data Protection statement:
The Employee is responsible for safe storage and security of equipment, records and systems. Data integrity and security must be maintained. It cannot be emphasised too strongly that the school deals with sensitive personal information on students and staff that could be damaging if such information became known to unauthorised people. As such all school data is open to abuse. It is the user's responsibility to prevent unauthorised access to school data and resources. Passwords are not to be recorded, or in any way communicated to unauthorised people.

The Employee must comply with procedures for disposal of confidential document waste: any confidential printed documents should be returned to the school for shredding, not disposed of at home. Any actual breach of confidentiality or suspicion that it may have occurred must be reported to the SLT immediately, who will inform the Chair of Governors.