THE HEATH ACADEMY TRUST

BRING YOUR OWN DEVICE POLICY

inspire transform together

Summary	
Policy Reference Number:	026
Category:	Data Protection
Authorised By:	Board Of Directors
Committee Responsible:	Board Of Directors
Version:	2019-1
Status:	21/03/2018: Approved at Full Trust Board. December 2018: Review of policy carried out by Trust DPO's (Jo Lolley & Selina White) 30/01/2019: Approved At Full Trust Board.
Next Review Date:	30/01/2020

The Heath Academy Trust
Registered Address: St Ives Primary & Nursery School, Sandy Lane, St. Ives, Ringwood, Hampshire, BH24 2LE
Registered in England and Wales
Registration Number: 09809895

Contents

Definitions
Note: These terms are standard throughout all policy documents and are designed to provide clarity.

Section 1: The MAT

"the Academy Trust" *and* "Trust"	mean the Heath Academy Trust Company.
"the Board"	means the Board of Directors of the Heath Academy Trust Company.
"the Directors"	refers to the group of (up to 12) Directors who make up the Board, and who are also the Heath Academy Trust's "Trustees" under charity law.
"Finance Committee"	refers to the Finance and Audit Committee formed by the Board to manage the financial affairs of the Trust.
"Accounting Officer"	is a role held by the Chief Executive Officer ("CEO") of the Trust, and one which includes a personal responsibility for the financial resources under the Trust's control. He is accountable for the Trust's financial affairs.
"Chief Finance Officer" (CFO)	is the Trust's finance director, and also the Trust Business Manager, to whom the Accounting Officer delegates responsibility for delivery of the Trust's financial processes and reports , and for the oversight and consolidation of the Academies' financial data.
"Trust Business Manager" ("TBM")	Fulfils the CFO role within the Trust, including compliance and statutory returns, as described in the Academies' Financial Handbook.
"Leadership Team"	is a team representing the Academies, consisting of the Headteachers and the CEO, and the TBM.

A full description of the positions listed and their responsibilities will be found in the current Academies' Financial Handbook.

Section 2: The Schools

"Academy"	One of the six schools making up the Heath Academy Trust.
"Academies"	All of the six Academies.
"School"	means an Academy within the Trust.
"Finance Officer"	The person responsible for the day to day management of an Academy's financial operations.
"Governor"	means a formally elected and appointed member of a School's Governing Body (generally referred to as the LGB).
"Headteacher"	means the senior person at an Academy who may also be an Executive Headteacher and/or elected as a Director of the Board.
"School's Leadership Team"	A group within each School consisting of the Headteacher, senior staff and the local Governing Body.

1. Introduction

1.1 The Heath Academy Trust recognises the benefits of mobile technology and is committed to supporting staff in the acceptable use of mobile devices.

1.2 This policy describes how non-school owned electronic devices, e.g. laptops, smart phones and tablets, may be used by staff members and visitors to the school. This practice is commonly known as 'bring your own device' or BYOD, and these devices are referred to as 'personal devices' in this policy. If you are unsure whether your device is covered by this policy, please check with the Trust's Data Protection Officers (DPO's/Data Protection Controller (DPC) for your school.

2. Organisational Arrangements

2.1 Overall Responsibility

2.1.1 The Board of Trustees of the Heath Academy Trust is responsible for the approval of this policy and for reviewing its overall effectiveness. The Local Governing Body of each school will formally adopt this policy and monitor its effectiveness within their school.

2.1.2 It is the policy of all schools within the Heath Academy Trust to provide staff with the equipment needed to access information away from the work place. Personal devices should not be used except in emergencies in school.

2.2 Roles & Responsibilities

2.2.1 The School will:

- ensure that members of staff who need to access information away from the work place are provided with the appropriate equipment (iPad or laptop) to do so securely thus reducing the need for any member of staff to use their own personal equipment for work purposes.
- be responsible for ensuring that the relevant security features are installed and regularly updated.
- it is the responsibility of the headteacher to ensure that budget forecasting includes sufficient funds for a rolling programme of replacement of equipment used by staff.
- the equipment will remain the property of the school at all times.

2.2.2 Members of staff will:

- familiarise themselves with the device provided and its security features so that they can ensure the safety of school information.
- Ensure relevant security features are installed and maintain the device appropriately.
- Set up passwords, passcodes, passkeys or biometric equivalents on the device being used.
- Set up remote wipe facilities if available, and implement a remote wipe if they lose the device.
- Ensure documents or devices are encrypted as necessary.
- Report the loss of any device containing school information, or any security breach immediately to the DPC for their school.
- Ensure that no school information is left on any personal device indefinitely. Particular care must be taken if a device is disposed of/sold/transferred to a third party.

2.2.3 Visitors will:

- familiarise themselves with this Trust policy on the use of personal devices
- only use personal devices for agreed purposes at the school and with parental or the relevant permission.
- not share information from personal devices via social media and will not keep school information indefinitely.

3. Detailed Arrangements & Procedures

3.1 Use Of Personal Devices At The School

3.1.1 Staff and visitors to the school may use their own devices in the following locations:

- in the classroom with the permission of the teacher.
- in the school environments e.g. libraries, sports pitches and outdoor spaces.

3.1.2 Personal devices must be switched off when in a prohibited area, and/or at a prohibited time, and must not be taken into controlled assessments and/or examinations unless special circumstances apply.

3.1.3 The school reserves the right to refuse staff and visitors permission to use their own device on school premises.

3.2 Use Of Cameras & Audio Recording Equipment

- Parents and carers may take photographs, videos or audio recordings of their children at school events for their own personal use unless notified otherwise by the school.
- Other visitors and staff may use their own personal devices to take photographs, video, or audio recordings in school provided they have checked that parental permission has been received by the school. This includes people who may be identifiable in the background.
- Photographs, video or audio recordings made by staff on their own devices should be deleted as soon as reasonably possible after they have been used, e.g. uploaded for use on one of the school's social media sites. Photographs, video or audio recordings to be retained for further legitimate use, should be stored securely on the school network.
- Photographs, video or audio recordings should not be published on blogs, social networking sites or in any other way without the permission of the people identifiable in them.
- Devices must not be used to record people at times when they do not expect to be recorded, and devices must not be used that would enable a third party acting remotely to take photographs, video or audio recordings in school.

3.3 Access To The School's Internet Connection

3.3.1 The school provides a wireless network that staff and visitors to the school may use to connect their personal devices to the internet. Access to the wireless network is at the discretion of the school and the school may withdraw access for anyone it considers is using the network inappropriately.

3.3.2 The school cannot guarantee that the wireless network is secure and staff and visitors use it at their own risk. The school is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the school's network. The school will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the school's network.

3.4 Access To The School's Systems

3.4.1 Staff are permitted to connect to or access the following school services from the device provided by the school:

- The school email system
- Google Drive
- Staff Shared Drive

3.4.2 Staff may use the systems to view school information via their iPad or laptop, including information about pupils. Staff must not access or store the information on their personal devices, or on cloud servers linked to their personal device. In some cases, i.e. emergency, it may be necessary for staff to download school information to their personal devices in order to view it (e.g. an email attachment). Staff shall delete this information from their device as soon as they have finished viewing it.

3.4.3 Staff must only use the IT systems and any information accessed through them for work purposes. School information accessed through these services is confidential, in particular information about pupils. Staff must take all reasonable measures to prevent unauthorised access to it. Any unauthorised access to, or distribution of, confidential information should be reported to the school as soon as possible.

3.4.4 Staff must not under any circumstances send school information to their personal email accounts.

3.5 Monitoring The Use Of Personal Devices

3.5.1 The school and/or the Trust may use technology that detects and monitors the use of personal and other electronic or communication devices which are connected to or logged on to the school's wireless network or IT systems. By using a device on the school's network, staff and visitors agree to such

detection and monitoring. The school's use of such technology is for the purpose of ensuring the security of its IT systems and tracking school information.

3.5.2 The information that the school may monitor includes, (but is not limited to): the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms, information uploaded or downloaded from websites and school IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

3.5.3 Staff who receive any inappropriate content through school IT services or the school internet connection should report this to the school as soon as possible.

3.6 Security Of Staff Personal Devices

3.6.1 Any member of staff wishing to use their own device must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption. This should be more than a simple password protection.

3.6.2 Staff must ensure that personal devices are set to lock with encrypted passcodes to prevent unauthorised access. The device should be locked if they are unattended or set to auto-lock if it is inactive for a period of time.

3.6.3 Staff must never attempt to bypass any security controls in school systems or others' own devices.

3.6.4 Staff must ensure that appropriate security software is installed on their personal devices and must keep the software and security settings up-to-date.

3.6.5 Staff must ensure that passwords are kept securely and are not accessible to third parties. Automated log on processes to store passwords must not be used.

3.7 Support

3.7.1 The school and the Trust takes no responsibility for supporting staff's own devices, nor does the school and the Trust have a responsibility for conducting annual PAT testing of personal devices. However, the school will support staff in ensuring that they have the appropriate knowledge to keep themselves compliant with this policy.

3.8 Compliance, Sanctions & Disciplinary Matters For Staff

3.8.1 Non-compliance of this policy exposes both staff and the school to risks. If a breach of this policy occurs, the Staff Disciplinary Policy will be applied.

3.9 Incidents & Reporting

3.9.1 The Trust and schools take any security incident involving a staff member's or visitor's personal device very seriously and will always investigate a reported incident. Loss or theft of the device should be reported to the school office in the first instance. Data protection incidents should be reported immediately to the school's DPC.