

BRING YOUR OWN DEVICE POLICY

This policy applies across Trust schools and services

**Document Management:**

Date Policy Approved: October 2024

Date Reviewed:

Next Review Date: October 2027

Version: 1

Approving Body: Finance & Resources Committee

|  |
| --- |
| **Change Log**  |
| **Update:**  | **New policy** |
| **Location:**  |   |
| **Summary Date:**  | **27/06/2024**  |
| **Completed by:**  | **Julian Kenshole**  |

**Using your own device (Bring Your Own Device)**

**Introduction**

We recognise that mobile technology offers valuable benefits to staff and students from a teaching and learning perspective and to visitors. Our Trust embraces this technology but requires that it is used in an acceptable and responsible way. The Trust will not compel staff to use their own personal devices to access school and Trust systems, but if staff choose to use their own devices, this policy should be adhered to.

Guest devices (any device which is not school owned or on the school asset list) should only be connected to a secure segregated network for access.

We recognise that certain advancements in technology will improve effectiveness and aid productivity within the Trust therefore authorised employees will be permitted to use their personal devices for work purposes. This includes email, file sharing and the use of Trust approved software and apps. The correct usage of these devices must be always ensured therefore there are standards and processes that apply to all staff authorised to use their personal device. It is imperative that employees deploy the same principles of data security when using their own devices as they would a Trust device. Employees must make themselves familiar with our Data Protection Policy and always adhere strictly to its principles and complete Cyber Security Training at induction.

**Related Policies**

* Health & Safety Policy
* Data Protection Policy
* Information Security Policy
* Working From Home Policy
* Display Screen Equipment Policy & Procedure
* Lone Worker Policy

**Employee responsibilities**

Any access to the Trust’s network must be approved and the following responsibilities always apply:

* Illicit materials must not be stored or transmitted from or to any device (Trust or personal).
* You must not use any device (Trust of personal) for Trust business whilst you are driving, unless doing so complies with current UK legislation.
* Apps deemed necessary for business use will be pushed remotely to the device by the IT Team upon agreement to the policy. Apps for private use will not be supported by the Trust.
* The Trust is not responsible for the day-to-day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates (except those deemed necessary for business use) or the resolution of hardware issues
* It is the employee’s responsibility to ensure that all devices and personal data are backed up in the event that this data is lost and the device wiped.
* If your personal mobile device is lost or stolen, you must advise the IT Team immediately to ensure access to the Trust’s network is deactivated. Immediate notification is imperative so that the Trust may assess the risk of a loss of personal data as defined in the General Data Protection Regulation and the current Data Protection Act.
* Staff who work from using their own device should complete a Display Screen Equipment Assessment of their workstation and make adjustments where necessary. If home working is a routine element of their work then the Working From Home Risk Assessment should be completed (**Working From Home Policy – Appendix 1**).

**Devices and Security**

Any personal device used for work purposes must contain a level of security in line with our existing IT infrastructure, this will include passcode protection and automatic locking when idle. Access to the Trust’s infrastructure will be in line with current security levels and user profiles. The Trust will not allow any device to connect to the network which has been jailbroken (e.g. where officially released software restrictions placed by the manufacturer are removed to circumvent security breach prevention) altered or tampered with in any way. It is the individual’s responsibility to ensure this is adhered to and that any device that subsequently becomes jailbroken, altered or tampered with will have all access to the network revoked.

Any Trust data and confidential information available on a personal device must be accessed by the authorised user only and this should be in line with the existing Information Security and Data Protection Policies. No access to the device or Trust’s network will be permitted for third party users.

Personal devices will be remotely wiped of Trust installed software by the IT Team in cases of a suspected confidentiality breach, lost or stolen device or termination of employment. The Trust holds no responsibility with regard to any loss of personal photos and/or applications as a result of this action. The responsibility for the upkeep of the device and any liability or risks associated with the use of the device for business purposes remain with the employee. The personal device should be made available for monitoring upon request by the Trust IT Team. Every effort will be taken to ensure that personal data is not accessed on the device, however in the event that this is not possible no records of the information will be stored and that data will not be used unless required by Law.

The Trust may need to apply security policies to your device which will protect the Trust’s information held on your device. We expect you to accept any updates pushed to your device by the Trust. The employee assumes full liability for risks including, but not limited to, the partial or complete loss of Trust and personal data due to operating system crashes, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

**General**

The following general points apply to usage of your own device for business purposes:

* If the school or normal place of work remains a frequent work base for a member of staff and equipment is retained on the premises, the school / Trust will not usually provide staff members with additional equipment to use at home. Only staff who are required to work across multiple sites will be considered for additional equipment to use at home.
* The use of personal devices is entirely at the risk of the owner.
* Personal devices remain the responsibility of the employee and all associated costs for the device and the running of the device shall remain with the employee.
* The Trust accepts no responsibility for any loss or damage to personal devices that are the result of employee failure to observe rules, procedures or instruction, or, as a result of your negligent behaviour.
* The Trust accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.
* Misuse of Trust information, data and/or software provided by the Trust will be investigated and may be dealt with under the Trust’s Disciplinary Policy.
* Upon termination of employment you must ensure that all Trust data and software is removed from your device on your last day of work at the latest. Evidence of this must be presented upon request to the IT Team, who may require you to submit your device to them for inspection and removal of Trust data and software if necessary.
* Any breach of this policy will be investigated and may be dealt with under the Trust’s Disciplinary Policy.

Staff must adhere to the following good practice:

**Do's**

* Ensure your device operating system is kept up to date and patched with the latest security updates.
* Ensure your software applications or apps are up to date with the latest versions.
* Ensure your device has anti-virus software / malware protection installed.
* Keep your personal and work files and activities separate and organised.
* Use Muti-Factor Authentication (MFA) and use strong passwords to access your work account.
* If possible, encrypt your device to prevent access if your device is stolen.
* If anything is suspicious, let the IT team know immediately.

**Don’ts**

* Allow any other person to access work related data.
* Save or keep work related data on personal devices.
* Do not disable anti-virus software.
* Do not connect to untrusted computer networks.
* Do not share passwords, Multi-Factor Authentication requests / codes, or access credentials.