Our vision

Challenging expectations and sharing success

Waverley School

Bring your own device (BYOD) Policy

CONTENTS

1.

Policy Summary

This policy covers any person wishing to use a device owned by someone other than the School (e.g. personal devices) to access School data – commonly known as Bring Your Own Device (BYOD). You must comply with the whole policy, but in summary:

- If you have accepted certain policies and your device meets certain criteria, you may access School data from a personal device.
- **The School retains control of the data**, and as part of this agreement you accept the installation of software that can erase data from your device and adds certain management facilities for School use which include being able to record use of facilities.
- **You must tell the School** if your device is lost, stolen, infected with malware or the security of the device is otherwise compromised.
- **The School does not support use of personal devices** although FAQs and installation instructions are maintained for your use. The School will accept comments and issues around BYOD but does not commit to respond to them. Issues with connectivity will be investigated, but if they cannot be reproduced you will have to find solutions in conjunction with your personal providers.
- **Some types of data CANNOT be stored or accessed on BYOD devices.** If you are using as part of your role data from certain partners, you cannot use BYOD devices.
- Compliance with this policy is part of your employment contract.

2. Introduction

The School has a responsibility to safeguard the information that has been provided to it by people and various government and statutory organisations to carry out its business. In order to do this we need to make sure that:

- the requirements of UK law on personal data management are being met.
- the School's own Data Privacy and Information Security policies are being followed.
- where third party data is being used, the requirements of the data owners are being followed.

The School recognises that users may wish to use their own mobile devices to access School data and use School applications as part of flexible working arrangements. This policy outlines the responsibilities of both the device owner and the School.

3. Who does the Policy apply to?

This policy applies to all persons who connect or intend to connect a device not owned by the School to use School data. (SUGGESTION) Note that if you have a school-provided mobile phone, you cannot additionally have a personal mobile phone connected due to technical limitations.

4. School's Responsibilities

As the data controller, the School is responsible for ensuring that all processing of personal data which is under its control remains in compliance with UK law. Additionally, the School receives data from partners which may be restricted by their security policies with which we have to comply.

The School must also remain mindful of the personal usage of such devices and the privacy of the individual. Technical and organisational measures used to protect School owned data must remain proportionate to the risks and consider your rights as an individual to privacy. Decisions on these matters will be made via the School's internal governance routes.

5. Rights, Privileges and Responsibilities

The use of a personally-owned device in connection with school business is a privilege granted to device owners. The School reserves the right to revoke these privileges without notice.

You must read and understand this policy before configuring your device to access School information.

(SUGGESTION) You must also complete the School's online eLearning courses on Data Protection, Freedom of Information and Information Security prior to being provided access to information from your personal device.

There are additional requirements for certain persons e.g. contractor staff who may need to sign additional agreements; please consult if you are in this group.

The School remains the data controller for all data held on BYODs.

Disciplinary and / or criminal action may be taken if a breach of policy or law occurs. Compliance with this policy is part of your employment contract.

As the device owner, you carry specific responsibilities, as listed below:

- You will not lend anyone your device to access school information or use school infrastructure.
- Should you decide to sell, recycle, give away or change your device, you will inform the School. **Do not allow the device to leave your possession until you have been informed School data has been wiped.**

- (SUGGESTION)The policy will require a minimum a four-digit pin or a passcode to access your device.
- In order to access your e-mail and calendar, you will need to enter your network account password.
- You must ensure that your device is compliant, and that security software is kept up-to-date. (SUGGESTED) The system will check whether your device meets compliance criteria and if not, will automatically stop syncing and potentially be wiped of School data.
- (SUGGESTED) The School data will be automatically wiped without notice if:
    1) you lose the device;
    2) the device is stolen;
    3) you terminate employment with the School;
    4) IT detects a data or policy breach or virus/malware infection;
    5) Your device becomes jailbroken or rooted (either intentionally or through the installation of software or an application that makes the modification to add additional functionality);
- (SUGGESTED) You are responsible for the safekeeping of your own personal data. We recommend that you secure and encrypt your phone appropriately using the facilities on the device, and that you have an up-to-date malware scanning solution installed (anti-virus).
- You must conform strictly to the School's Data Protection Policy-and use of information.

All users are expected to use their device in an ethical manner. Using your device in ways not designed or intended by the manufacturer is not allowed. This includes, but is not limited to, "jailbreaking" your iPhone or "rooting" your android device even if this adds additional functionality.

6. Which devices are covered?

(SUGGESTED) Current devices approved for Bring Your Own Device use are listed below along with the minimum system requirements:

- Android 5 ("Lollipop") or higher Smart Phones and Tablets
- iOS 9.3 or higher iPhones and iPad
- Windows 10 Mobile or higher
- MacOS devices with TPM 2.0 and MacOS version 10.11 or higher
- Windows 10 devices with TPM 2.0 running the Professional edition or higher (Home edition is not supported)

(SUGGESTED) Devices below these specifications will not comply with our policies and therefore will not be allowed to be used as BYOD.

It should be noted that as technology improves and newer versions of operating system are introduced by vendors or vulnerabilities are discovered in existing operating systems this list is subject to immediate change and access maybe revoked (in some instances this may be without notice).

7. Which IT Services Are Available?

(SUGGESTED) IT Services available and covered by policy are:

- E-mail. Note that the amount of email allowed on the phone is fixed by the School and cannot be changed.
- Calendar
- Contacts
- Tasks
- Telephony, Meetings and Instant Messaging via Skype for Business
- File access and editing via SharePoint and OneDrive for Business (using the Microsoft Office suite for the mobile device).
- Multi-factor authentication via Microsoft Authenticator
- Collaboration and group discussion via Yammer / Teams
- School building Wi-Fi

Note that some file types cannot be securely opened, and hence you may find you cannot open certain attachments etc. Additionally, mobile software may have different and more limited functionality from desktop versions.

(SUGGESTED) A minimum four-digit passcode will be required to access devices containing School data; you will also initially need to set up the device using your School username/email and password. You will need to update these as per School policy and **MUST NOT** share these with any other person.

(STRONGLY RECOMMENDED – IF YOU DO NOT DO THIS YOU WILL NOT BE COMPLIANT WITH THE DATA PROTECTION LAW) School data is stored encrypted to protect it and is subject to restrictions on copying and where it can be saved.

8. Who Manages this Facility?

IT will manage the BYOD facility, as described within this document, on behalf of the School. Human Resources will advise managers if corporate policies have not been followed.

9. What Support will IT provide?

(SUGGESTED) IT will not support or maintain any personal device. Furthermore, the School will not cover any damage to the device or any loss of personal data that may occur as a result of installing any mobile device management solution or when data is removed as part of the data wiping ability of the solution. The School makes reasonable endeavours to ensure that your device is not affected and that only School data is erased, but this cannot be fully guaranteed and the School accepts no liability for issues resulting from use.

(SUGGESTED) It is recommended that device owners insure their device as part of their home contents insurance or via a specific mobile device insurance scheme and advise their insurer that the device will be used for work purposes at home and at work locations.

Upon installation of the mobile device management software, the device owner can connect to the School infrastructure to access their School accessible data. However, the device owner is personally liable for the device and carrier service costs. They will not be reimbursed by the School for the acquisition of a mobile device, its use, maintenance or replacement or any carrier service charges incurred. The device owner must agree to all terms and conditions in this policy to be allowed access to School services listed in this document.

10. If a Security incident should occur

A Security incident is defined as **any** event that could compromise information security. Some examples: your device is lost or stolen, someone else gains access to your password/passcode, your device becomes infected with malware.

If a security incident should occur, you are required to inform IT **immediately** with details.

The School reserves the right to wipe either School data and applications or the whole device if it is deemed necessary. This may impact other personal applications and data, such as the native Address Book data and any personal files on your device. We recommend that you investigate backup solutions for your personal files available for your operating system.

The School has developed and implemented a Breach Management Process, you should ensure that you read and understand both the policy and your responsibilities under the reporting process.

The School also needs to take action where potential incidents are identified. Where ‘near misses’ occur, these should be reported to the School Business Manager a local decision taken as to whether the cause of the ‘near miss’ is one which could involve the enhancement of the policy or the process
Note that not reporting security incidents is a breach of the Acceptable Use Policy.

11. Guidelines for Acceptable Behaviour

Device owners are expected to behave in accordance with the School’s behaviours framework at all times whilst undertaking work for the School. Further information can be obtained by contacting a member of the HR team.

Be aware that any personal device used at work may be subject to discovery in litigation. This means that it could be used as evidence in a lawsuit against the School. Your data could be examined not only by the School but also by other parties in any legal action.

12. Allowed Countries

The UK law on data protection only permits export of personal data to certain countries. Because of this, we cannot permit BYODs with School data to be taken to countries in the following classes:

- Countries in the European Economic Area
- Countries with an "assessment of adequacy of data protection (see http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm)

For countries outside this list, the School may choose to perform an assessment of risk of its own, but it has not so far done so. Any such decisions will be added to the list above

13. If You Leave the Employment of the School

As part of the leaver's process, your access to the School infrastructure and applications will cease and your device will be de-provisioned and ensure access to School data is ceased and School data is wiped.

14. School Release of Liability and Disclaimer Statement

School hereby acknowledges that the use of a personal device in connection with School business carries specific risks for which you, as the device owner and user, assume full liability. These risks include, but are not limited to, the partial or complete loss of data as a result of a crash of the OS, errors, bugs, viruses, and/or other software or hardware failures, or programming errors which could render a device inoperable.

The School hereby disclaims liability for the loss of any such data and/or for service interruptions. The School expressly reserves the right to wipe the device management application (or similar applications) at any time as deemed necessary for purposes of protecting or maintaining School infrastructure and services.
The School also disclaims liability for device owner injuries such as repetitive stress injuries developed. The School provides IT equipment that is suitable for long-term office use.

Device owners bring their devices to use at the School as their own risk. Device owners are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

School is in no way responsible for:

- Personal devices that are broken while at work or during work-sponsored activities
- Personal devices that are lost or stolen at work or whilst undertaking work-related activities
- Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues)
- The management or creation of users own ‘cloud’ based user accounts, which are required for purchasing software, or backing up data

School does not guarantee that Service will be compatible with your equipment, or warrant that the Service will be available at all times, uninterrupted, error-free, or free of viruses or other harmful components, although it shall take reasonable steps to provide the best Service it can.

Furthermore, depending on the applicable data plan, the software may increase applicable rates. You are responsible for confirming any impact on rates as a result of the use of School supplied applications as you will not be reimbursed by the School.

Finally, the School reserves the right, at its own discretion, to remove any School supplied applications from your personal device as a result of an actual or deemed violation of the School’s BYOD Policy.