Wakefield Grammar School Foundation

Document Reference	**WGSF Bring Your Own Device Policy**
Version Number	V1.03
Author/Lead **Job Title**	John Lister, ICT Technical Director
Checker Person Name **Quality Assurance**	Jenny Cocker, Director of Finance and Operations
Consultation	Vicky Weeks, Compliance Manager
Name of Ratifying Committee **Date Ratified**	Governing Board **28.08.2024**
Date of Next Review (2 yearly)	**August 2026**

VALIDITY – Policies should be accessed via Firefly to ensure the current version is used.

CHANGE RECORD - REVIEW PERIOD 2 YEARS

Version	Date	Change details
V1.00	Oct 2015	Reviewed
V1.01	July 2017	Updated, J Lister
V1.02	Dec 2020	Updated, J Lister
V1.03	Aug 2024	Updated, J Lister

To be published on the following:

Staff shared	**X**	**School website**	**X**

WGSF Bring Your Own Device (BYOD) Policy

1. Introduction

The Foundation is committed to providing a technology based learning environment that creates opportunities to support and extend learning and teaching in all of its schools and beyond. As part of this commitment we offer staff, governors, Sixth Form pupils and approved visitors the ability to access the respective school wireless network using their own technology (laptop, smart phone, tablet). This element of the Foundation's ICT provision is a privilege and as such there are rules associated with this 'Bring Your Own Device' (BYOD) initiative that, if broken or abused, will result in that privilege being taken away and sanctions being applied.

This is a voluntary scheme and a particular note should be made of the fact that the Foundation accepts no responsibility for the loss, theft or damage of any phone, laptop, tablet or other device brought into school.

This BYOD Policy compliments the rules laid down in the WGSF ICT Acceptable Use Policy with particular reference to Annex 1: Online Safety.

We encourage Students and Staff to use the Foundation issued Chromebook or other Foundation devices for school or Foundation work, including those in the Sixth Form, but we do understand that some courses can be augmented by the use of an individual's own device.

The Foundation reserves the right to prohibit bringing personal devices into the school and/or using them for work purposes (as applicable). The Foundation also reserves the right to require personal devices to be switched off at certain times and/or within certain areas of the school.

The use of personal mobile devices within the school introduces increased risks in terms of the security of our IT resources and communication systems, the protection of confidential and proprietary information, and compliance with legal obligations (including child safeguarding).

This policy sets out rules on the use of personal devices in order to:

- Protect our systems, as further defined below;
- Protect Foundation data (including personal data), as further defined below; and
- Set out how we will manage and monitor your access to our systems.

2. Implementation

2.1 Currently there are no plans to offer BYOD access via their own device to pupils below Sixth Form, as they are all allocated Chromebooks.

2.2 Digital Services will enable access unique to each individual. This may be used on up to two devices per individual.

2.3 The level of access when individuals are logged onto the internet via their device may be different according to year group or role within the Foundation. This filtering will be subject to review.

2.4 Parents will be required to sign a BYOD Acceptable Use Agreement form before their child will be given access for their device. The form for this is on Firefly. All users are required to sign up to the ICT Acceptable Use Policy when they join the Foundation and also periodically to reaffirm their acceptance of the policy.

2.5 For access to be granted to the Foundation network via your own device the Foundation may require the installation of software or a certificate to aid monitoring of that device or its traffic on the Foundation network.

2.6 Visitors must request access via their Foundation Link to Digital Services or other nominated staff member.

3. Terms and Conditions

3.1 The Foundation provides wireless connectivity as a guest service and offers no guarantees that any use of the wireless connection is in any way secure or that any privacy can be protected when using this wireless connection. All Foundation internet activity is monitored, filtered and logged.

3.2 Use of the Foundation Schools' wireless network is entirely at the risk of the user and the Foundation is not responsible for any loss of any information that may arise from the use of the wireless connection, or from any loss, injury or damage resulting from use of the wireless connection.

3.3 All Individuals accessing the Foundation Schools' networks are bound by the ICT Acceptable Use Policy. In using the Foundation WiFi you agree to the BYOD policy. You are also agreeing to all of the above cautions and policies as they pertain to non-school devices.

3.4 Any individuals who do not accept the terms of service will not be able to access the school's network.

3.5 The Foundation may use technology that detects and monitors the use of mobile and other electronic or communication devices which are connected to or logged on to our network or services. By using a mobile device on the Foundation network, you agree to such detection and monitoring.

3.6 The use of a device in lesson time is entirely at the discretion of the teacher. If the teacher asks you not to use your device then you must follow those instructions.

3.7 The use of a personal ICT device is not to be a distraction in any way to teachers or pupils. Personal devices must not disrupt class or Private Study areas in any way. Playing games or other non-school work related activities are not permitted.

3.8 All individuals shall make no attempts to circumvent the Foundation's network security. This includes setting up proxies and downloading programs to bypass security.

3.9 The Foundation has the right to take action against anyone involved in incidents of inappropriate behaviour, that are covered in the BYOD Acceptable Use Agreement or the schools' Behaviour Policies, whether in school or out of school (examples would be cyber-bullying, use of images or personal information).

3.10 All individuals using their own devices on site must check their device daily for basic Health and Safety compliance to ensure it is free from defects. Any personal ICT device that has obvious Health and Safety defects should not be brought into school.

3.11 Any failure to comply with this BYOD Acceptable Use Policy will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities, involvement of the police.

3.12 The Foundation reserves the right to search the content of any mobile or handheld device on the school premises where there is a reasonable suspicion that it may contain inappropriate material or is being used for an inappropriate activity, including, but not limited to, those which promote pornography, gambling, violence, bullying or discrimination of any form.

3.13 Individuals are not to access websites that promote extremism, radicalisation or terrorism using their device on the Foundation's premises.

3.14 Individuals must not submit or publish personal information about themselves or others (including 'selfies') unless part of an approved educational activity. This includes using apps, micro-blogging sites such as blogging, social networking, personal web pages, VLE, e-mail systems, SMS, online forums and chat or any other web based public information and collaboration systems and any app service using their device while on Foundation premises.

3.15 Individuals must not access, store or share 'unsuitable' or illegal material on any Foundation IT system or their own tablet or personal device. Unsuitable material includes (but is not restricted to) gambling, pornography, promotion of bullying, sexual exploitation, extreme violence or sites inciting hatred of a particular group. Where internet access is gained outside of the school network, e.g. via Mobile 3G/4G/5G, the same rules apply in terms of not accessing 'unsuitable' material.

3.16 All devices connected to the BYOD network or used for Foundation activities must be of a minimum standard which includes on device encryption. Devices should be running an operating system supported by the operating system manufacturer. Software on the devices should also be maintained and supported.

3.17 All device accounts on personal devices should only be used by those with Foundation access and access to Foundation services should not be shared with others, even if those others have a role within the Foundation.

3.18 Files not related to Foundation activities should not be stored on Foundation Storage. Please be aware that files stored on Foundation Storage (Google Drive, One Drive, Sharepoint, Gmail and other systems) are subject to access from other members of the Foundation and delegated support providers for regulation, antivirus, antimalware, disciplinary, investigation, subject access request or Foundation business continuity purposes.

3.19 When you access our systems using a device, we are exposed to several risks, including from the loss or theft of the device, the threat of malware and the loss or unauthorised alteration of school data. Such risks could expose us to the risk of non-compliance with legal obligations of confidentiality, data protection and privacy. This could also result in damage to our systems, our business and our reputation.

3.20 Breach of this policy may lead to us revoking your access to our systems, whether through a device or otherwise. It may also result in disciplinary action up to and including dismissal. Disciplinary action may be taken whether the breach is committed during or outside Foundation hours and/or whether or not use of the device takes place within the Foundation premises. You are required to co-operate with any investigation into a suspected breach, which may involve providing us with access to the device and any relevant passwords and login details.

3.21 You should also minimise the amount of school data you retain on the device by accessing information remotely where possible, and deleting any data saved locally on your device as soon as it is no longer required. Any data pertaining to individuals should be encrypted on that device.

3.22 Once the right to use the Foundation BYOD is removed. (e.g. you have left the Foundation, or it has been removed for other reasons) you MUST remove all content or software provided by the Foundation. All Foundation data should be removed from any personal devices.

3.23 All BYOD use is subject to minimum standards of device and/or device update level to allow the use of newer security technologies as they develop. This is subject to regular review.

See Appendix 1 for Frequently Asked Questions.

Appendix 1: Frequently Asked Questions - All

What personal ICT devices can I use in school?

You may use either a laptop, Chromebook, smartphone or tablet computer. For lesson use we recommend a device with a keyboard.

Can I transfer work from school computers to my personal ICT device?

We would prefer this did not happen, but individuals may transfer files from the Foundation / School network to their devices via the school Portal/Google Drive to work on individual files using compatible software. This should be kept to a minimum and must be encrypted if containing information about an individual. Please be aware that downloading any information about an individual to your device outside of opening files inside your google workspace account and applications may lead to it being considered for search if a subject access request is received.

Can I physically plug my device into the School Network using a network cable?

Individuals must not plug into the school network using a network cable unless they have written permission from the Foundation Technical Director.

Can I physically plug my device into a screen to present to others?

Connections to screens and projectors via HDMI and USB-C are appropriate where preconfigured and presented by digital services in classrooms and meeting rooms. Pupils should seek advice from their teacher before connecting. Advice should be sought from Digital Services if you are changing the configuration of any Foundation devices.

Can I use my device as a personal WiFi hotspot or broadcast my own wireless network to allow others to access the internet?

Individuals are **not permitted to use their device to broadcast their own SSID or use it as a hotspot so that it can allow others to access the internet by by-passing the Foundation's wireless network** while in school (this can also cause interference with other individuals' devices and other Foundation services) without the written consent of the Foundation Technical Director. The Foundation cannot permit access to non-filtered services for safety reasons and this includes all wireless services. Any individuals enabling such a network would be committing a gross breach of trust and would no longer be able to use a personal ICT device in school. Additional sanctions for breaching school rules would also apply.

How do I charge my ICT device at school?

Devices should be charged at home. All electrical devices used in school need to be PAT tested so, for Health and Safety reasons, personal devices cannot be charged in school. Some low voltage USB ports are available for charging. Though the Foundation does maintain them, they can accept no responsibility if damage were to result from using one of these ports.

Why am I filtered and monitored on my own device? Shouldn't I be able to see what I want to on my own device?

The Foundation is providing you with a service that it is committed to making you and our schools as safe and secure as possible. This is part of our wider duty of care to which all who work in schools are bound to follow. Your device is using the Foundation's wireless network which is filtered and secured according to our specifications. Please note, the BYOD WiFi network is there to help support teaching and learning and not as a recreational tool.

Does the Foundation track all the use of my personal device if I use the WiFi or Foundation Google / Microsoft or Apps?

No. The Foundation only has access to the information on website activity when using the Foundation WiFi. The Foundation also has access to information shared by the particular application provider when signed in on a Foundation account and using Foundation resources and applications on your device. Please make sure that you are signed in as a personal user into Google Search for example when making personal searches or using other google applications such as Maps.

How do I remove Foundation access to my device when I leave / do not wish to use this service?

Please sign out of any Foundation Google / Microsoft apps / other applications or websites on your device. Also please delete any files downloaded separately from these apps.

Please note: *It is important to understand that the Foundation has the right to make any necessary changes to how the wireless access works for the best interest and security of pupils and staff in the Foundation.*

Appendix 1.1: Frequently Asked Questions - Pupils

How do I get permission to use a personal ICT device on the school WiFi?

Parents must complete the BYOD Agreement on Firefly. Your agreement will be recorded on SIMS and Digital Services will subsequently contact you, allowing you to use a personal ICT device in school.

Does this mean I can use my mobile phone anytime I would like now that I have connected it to the school WiFi?

No. Mobile phone use by pupils is controlled by the Schools' Behaviour Policies.

Can I use my personal ICT device in class?

Devices may only be used in class with the approval of the class teacher.

Appendix 1.2: Frequently Asked Questions - Staff and Governors

How do I get access to use a personal ICT device on the in school WiFi?

Please contact Digital Services who will advise you on setup procedures.

Can I use my own device for regular teaching at the front of class?

No, the Foundation provides resources for each department and member of staff which should cover day to day teaching needs as discussed with Heads of School, Faculty and Department. BYOD is provided as an additional resource for lesson preparation and administration convenience.

Can I connect Outlook or another Web / Email client to my school account?

No all access to Google Workspace products should be through the authorised Google Tools. Gmail and Google Calendar Apps are available for this purpose through your app store on your device.