



LORD
WANDSWORTH
COLLEGE

BRING YOUR OWN DEVICE (BYOD) POLICY

Staff Member responsible	Revision Date	Approved By	Approval Date	Reason
JJD	December 2016	SLT	17/1/17	New policy
JJD	November 2017	Governors	6/12/17	Reviewed
SLB/DGM	October 2018	SLT	15/11/18	Reviewed and updated
SLB/DGM	November 2021	Governors	1/12/21	Reviewed and updated
CJA	April 2024	Governors	02/05/2024	Reviewed and updated in line with ISBA framework

Bring Your Own Device

Introduction

We recognise that many of our staff and visitors have personal mobile devices (such as tablets, smartphones and handheld computers), which they could bring to the College and, in the case of staff, use these devices for work purposes. However, the use of personal mobile devices within the College 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 College data (including personal data), as further defined below; and
- set out how we will manage and monitor your access to our systems.

Staff covered by this policy may use a personal mobile device for work purposes, subject to adherence to the terms of this policy.

This policy is also intended to address the use by pupils of non-College owned electronic devices to access the internet via the College's internet connection, to access or store College information, or to make photographs, video, or audio recordings at College.

Devices include smart phones, tablets, laptops, wearable technology and any similar devices. If you are unsure whether your device is captured by this policy please check with the College's Director of IT Services. These devices are referred to as 'mobile devices' in this policy.

This policy is supported by the IT Acceptable Use Policy and the Safeguarding Policy.

The College reserves the right to prohibit bringing personal devices into the College and using them for work purposes. The College also reserves the right to require personal devices to be switched off at certain times or within certain areas of the College.

This policy supplements and should be read in conjunction with our other policies and procedures in force from time to time, including without limitation our College's Safeguarding and Child Protection Policy and the Anti-Bullying Policy, Data Protection Policy, Data Retention Policy, Artificial Intelligence Policy and the Taking, Storing and Use of Images Policy and IT Acceptable Use Policy, all of which are available on the school website and on the Staff and Student Hub.

Scope and purpose of the policy

This policy applies to staff, pupils and visitors who use a personal mobile device including any accompanying software or hardware (referred to as a device in this policy) within the College and/or for work purposes. Note that it applies to use of the device for work purposes both during and outside College hours and whether or not use of the device takes place at College.

For staff, this policy applies to all devices used to access our IT resources and communication systems (collectively referred to as **systems** in this policy), which may include (but are not limited to) smartphones, mobile or cellular phones, PDAs, tablets, and laptop or notebook computers.

Bring Your Own Device

When you access our systems, you may be able to access data about the College, including information which is confidential, proprietary or private (collectively referred to as **College data** in this policy).

As part of granting your personal device access, the College will take steps to keep your personal device's wider data and systems separate from our systems and College data which you access from that device.

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 College 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.

Staff, pupils and visitors to the College may use their own mobile devices in the following locations:

- In the classroom only with the permission of the teacher
- In some College areas at certain times of the day – e.g. library, common rooms, boarding houses (see the IT Acceptable Use Policy)

Staff, pupils and visitors to the College are responsible for their mobile device at all times. The College is not responsible for the loss or theft of or damage to the mobile device. The IT Department must be notified immediately of any damage, loss, or theft of a mobile device, and these incidents will be logged.

Mobile devices must be turned 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.

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 College hours and/or whether or not use of the device takes place at College. 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.

This policy also applies to staff, pupils and visitors who access our wireless networks on their own devices for personal use (see further below).

Access to our wireless internet networks

We provide a wireless network that you may use to connect your device to the internet. Access to the wireless network is at the discretion of the College. It should under no circumstances be used to access or distribute content that is unlawful, harmful, explicit, offensive or otherwise inappropriate. We may withdraw access from anyone we consider is using the network inappropriately.

We cannot guarantee that the wireless network is secure, and you use it at your own risk. In particular, you are advised not to use the wireless network for online banking or shopping.

In order to access the Internet, all Pupils and Staff must enrol their device by connecting to the LWCBYOD network and accepting or installing our certificate before any access is given. The only exemption to this is Visitors, who temporarily join our Guest WiFi.

Bring Your Own Device

By enrolling devices, our Firewall software can monitor all traffic and apply restrictions based on the sites visited. This method offers the safest way for all pupils and staff to access the Internet and prevents any attempted misuse at source.

The College 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 College's wireless network. This activity is taken at the owner's own risk and is discouraged by the College. The College will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the College's wireless network.

The information that we 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 (including passwords), information uploaded to or downloaded from websites, and peer-to-peer traffic transmitted via the network. All aspects of enrolled devices except internet traffic provided by LWC will remain absolutely private and cannot be seen by anyone other than the owner. Visitor devices on the LWC Guest network have less monitoring, however basic application, URL logs and filtering is still active on this network.

Staff should also refer to the Monitoring section below for further information.

Student BYOD network and social media times

Network internet access times to BYOD

Form	Start Time	End Time	Weekends
1 st	07:00	20:15	Sat 07:00 – Sun 20:15
2 nd	07:00	20:15	Sat 07:00 – Sun 20:15
3 rd	07:00	21:30	Sat 07:00 – Sun 21:15
4 th	07:00	21:45	Sat 07:00 – Sun 21:30
5 th	07:00	22:00	Sat 07:00 – Sun 22:00
6 th	06:00	23:00	Sat 07:00 – Sun 23:00

Social media access times, Monday – Friday

Form	Start Time	End Time	Start Time	End Time	Prep	Start Time	End Time
1 st	-	-	-	-		-	-
2 nd	-	-	-	-		-	-
3 rd	-	-	17:00	19:00		20:30*	21:30
4 th	-	-	17:00	19:00		21:00*	21:45
5 th	-	-	16:00	19:00		21:00*	22:00
6 th	12:50	13:40	16:00	19:00		20:00 *	23:00

*On Friday evenings social media to be accessible from 20:15

Bring Your Own Device

Social media access times, weekends

Form	Start Time	End Time
1 st	_*	_*
2 nd	_*	_*
3 rd	Sat 07:00	Sun 21:30
4 th	Sat 07:00	Sun 21:45
5 th	Sat 07:00	Sun 22:00
6 th	Sat 07:00	Sun 23:00

*Allow for some age-appropriate games to be unblocked for Junior pupils for shortened windows – requests should be made to Junior Houseparent.

Images and recordings (staff and visitors)

You are not permitted under any circumstances to use your personal devices when taking images, videos or other recording of any pupil nor to have any images, videos or other recording of any pupil on your personal devices. The Taking, Storing and Using Images of Children Policy lays out in detail our approach to this, including the approach parents and close family members to taking photographs of their children. Please read this in conjunction with the Safeguarding and Child Protection Policy and the IT Acceptable Use Policy.

Connecting devices to our systems (staff and students)

Connectivity of all devices to the College's systems is centrally managed by the Director of IT Services. We reserve the right to refuse or remove permission for your device to connect with our systems.

Before using your device to connect to our systems, it may be necessary for the IT Department to ensure that a relevant certificate is running on your device to ensure the security of our systems.

Monitoring (staff using systems)

The contents of our systems and College data are our property. All materials, data, communications and information, including but not limited to e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device (collectively referred to as content in this policy) during the course of business or on our behalf is our property, regardless of who owns the device.

We reserve the right to monitor, intercept, review and erase, without further notice, all content on the device that has been created for us or on our behalf. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, logins, recordings and other uses of the device, whether or not the device is in your possession.

It is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. You should have no expectation of privacy in any data on the device. Staff are advised not to use our systems for any matter intended to be kept private or confidential and

Bring Your Own Device

to avoid processing any personal data relating to non-College related third parties (for example, your family and friends) on our systems.

Monitoring, intercepting, reviewing or erasing of content will only be carried out to the extent permitted by law in order for us to comply with a legal obligation or for our legitimate College purposes, including, without limitation, in order to:

- prevent misuse of the device and protect College data.
- ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy).
- monitor performance at work; and
- ensure that staff members do not use our facilities or systems for any unlawful purposes or activities that may damage the College, its systems or reputation.

We may also store copies of any content for a period of time after they are created and may delete such copies from time to time without notice. We may obtain and disclose copies of such content or of the entire device (including personal content) for litigation or investigations.

You acknowledge that the College is entitled to conduct such monitoring where it has a legal obligation or legitimate basis to do so, and that (without further notice or permission) we have the right to copy, erase or remotely wipe the entire device (including any personal data stored on the device).

Whenever we monitor personal data it will be carried out in line with the Data Protection Policy, Data Retention Policy and Privacy Notice and government guidance such as KCSIE, GDPR and Subject Access Requests.

You acknowledge that you use the device at your own risk and that we will not be responsible for any losses, damages or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of any device, its software or its functionality.

Security requirements (staff)

You must comply with the IT Acceptable Use and Safeguarding policy when using your device to connect to our systems.

In addition to the requirements set out in the above-mentioned policies and set out above in this policy, you must also:

- in no circumstances use your personal email or other personal messaging account to transfer, attach, discuss, or otherwise use College data or any other information which may be contained in our systems. To the greatest extent technically possible, our systems and our data must be kept separate from the rest of your personal device.
- install any anti-virus or anti-malware software at our request before connecting to our systems and consent to our efforts to manage the device and secure our systems and College data.

Bring Your Own Device

- protect the device with a PIN or strong password and keep that PIN or password secure at all times. The PIN or password should be every six months. If the confidentiality of a PIN or password is compromised, you must change it immediately.
- not download or transfer any College data or correspondence to the device, for example via e-mail attachments, unless specifically authorised to do so. Staff must immediately erase any such information that is inadvertently downloaded to the device.

We reserve the right, without further notice or permission, to inspect your device and access data and applications on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the College data on it for legitimate business purposes.

You must co-operate with us to enable such inspection, access and review, including providing any passwords or PINs necessary to access the device or relevant applications.

If we discover or reasonably suspect that there has been a breach of this policy, including any of the security requirements listed above, we shall immediately remove access to our systems and, where appropriate, remove any College data from the device. Although we do not intend to wipe other data that is personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from College data in all circumstances. You should regularly backup any personal data contained on the device.

You acknowledge that, without further notice or permission, we may need to inspect a device and applications used on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the data on or from a device for legitimate purposes.

Lost or stolen devices and unauthorised access (staff)

In the event of a lost or stolen device, or where a staff member believes that a device may have been accessed by an unauthorised person or otherwise compromised, the staff member must report the incident to the Director of IT Services immediately.

Appropriate steps will be taken to ensure that College data on or accessible from the device is secured, including remote wiping of the device where appropriate. The remote wipe will destroy all College data on the device (including information contained in a work e-mail account, even if such e-mails are personal in nature). As noted above, although we do not intend to wipe other data that is strictly personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from College data in all circumstances. You should regularly backup all personal data stored on the device.

The College takes any security incident involving a staff member or pupil's device very seriously and will always investigate a reported incident. Loss or theft of the mobile device should be reported to the IT Department in the first instance. Data protection incidents should be reported immediately to datacompliance@lordwandsworth.org.

Procedure on termination of employment (staff)

On your last day of work, all College data (including work e-mails), and any software applications provided by us for work purposes, will be removed from the device. If this cannot be achieved remotely, the device must be submitted to the Director of IT Services for wiping

Bring Your Own Device

and software removal. You must provide all necessary co-operation and assistance in relation to this process.

Personal use (staff)

We have a legitimate basis or legal obligation to access and protect College data stored or processed on your device, including the content of any communications sent or received from the device. Where we are relying on our legitimate interests, we recognise the need to balance our need to process data for legitimate purposes, with your expectations of privacy in respect of your personal data. Therefore, when taking (or considering taking) action to access your device or delete data on your device (remotely or otherwise) in accordance with this policy, we will, where practicable:

- consider whether the action is proportionate in light of the potential damage to the College, its pupils or other people impacted by College data.
- consider if there is an alternative method of dealing with the potential risks to the College's interests (recognising that such decisions often require urgent action).
- take reasonable steps to minimise loss of your personal data on your device, although we shall not be responsible for any such loss that may occur; and
- delete any such personal data that has been copied as soon as it comes to our attention (provided it is not personal data, which is also College data, including all personal emails sent or received using our email system).

As noted above, it is important to separate your personal data from College data. To reduce the likelihood of the College inadvertently accessing your personal data, or the personal data of third parties, you must comply with the following steps to separate College data from your personal data on the device:

- Only access the College's data using the specific and relevant application that contains that data, for instance Microsoft 365, and not download this data onto your device.
- do not use work e-mail for personal purposes.
- regularly backup all personal data stored on the device.
- ensure that multi factor authentication is set up on your device.

Appropriate use (staff)

You should never access or use our systems or College data through a device in a way that breaches any of our other policies, in particular our IT Acceptable Use Policy, Data Protection Policy, Data Retention Policy, The Taking, Storing and Use of Images Policy, Antibullying policy and the Safeguarding and Child Protection Policy. If you breach any of the above policies, you may be subject to disciplinary action up to and including dismissal.

You should also minimise the amount of College 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.

Bring Your Own Device

You must not talk, text, e-mail or otherwise use a device while operating a College vehicle or while operating a personal vehicle for College purposes. You must comply with any applicable law concerning the use of devices in vehicles.

Support

The College takes no responsibility for supporting staff's and pupil's own devices. However, the College does require electrical items to be PAT tested. It is the owner's responsibility to make sure that a request for a PAT test is logged via the LWC Helpdesk. The Maintenance Department will make arrangements for the item to be PAT tested.

Compliance, Sanctions and Disciplinary Matters for staff

Non-compliance of this policy exposes staff, pupils, visitors and the College to risks. If a breach of this policy occurs the College will respond immediately by issuing a verbal, then written warning to the staff member or pupil. Guidance will also be offered. If steps are not taken by the individual to rectify the situation and adhere to the policy, permission to use the device on College premises will be temporarily withdrawn.

Who is responsible for this policy?

The Headmaster in conjunction with the Director of IT Services shall have overall responsibility for the effective operation of this policy and shall be responsible for reviewing this policy to ensure that it meets legal requirements and reflects best practice. If you have any questions about this policy or other queries related to use of your own device for work purposes please contact the Director of IT Services.