



LORD
WANDSWORTH
COLLEGE

IT Acceptable Use Policy

<i>Staff Member responsible</i>	<i>Revision Date</i>	<i>Approved By</i>	<i>Approval Date</i>	<i>Reason</i>
CJA	April 2024	Governors	2 May 2024	New/reinstated policy
CJA	September 2024	Governors	3 Sep 2024	Amended mobile phone policy
CJA/COO	August 2025	Governors	3 Sep 2025	Amended mobile phone policy

IT Acceptable Use Policy

Introduction

The IT Acceptable Use Policy was formerly incorporated into College Rules and is now a standalone policy to cover the use of devices and the College hardware and infrastructure, ensuring that every user accesses our systems in a safe and secure manner.

This policy applies to all members of the College community (staff or pupils) who use College IT systems, as a condition of access. Access to College systems is not intended to confer any status of employment on any contractors.

Online behaviour

As a member of the college community you should follow these principles in all of your online activities:

- The college cannot guarantee the confidentiality of content created, shared and exchanged via College systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the College community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the College community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Accessing the Internet at Lord Wandsworth College

In order to access the Internet, all Pupils and Staff must ensure that our certificate is installed on their device. This can be done by either enrolling their device through Company Portal, via Intune, or installed directly via the browser or when logging a phone onto the BYOD network. The only exemption to this is Visitors, who temporarily join our Guest WiFi.

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.

IT Acceptable Use Policy

All aspects of enrolled devices except internet traffic provided by LWC, device make/model and MAC address will remain absolutely private and cannot be seen by anyone other than the owner. Anyone who leaves will automatically have their device removed from our Company Portal if the device is connected to that service.

Using the College's IT Systems

Whenever you use the College's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access College IT systems using your own username and password. Do not share your username or password with **anyone** else.
- Do not attempt to circumvent the content filters or other security measures installed on the College's IT systems, and do not attempt to access parts of the system that you do not have permission to access. This includes the use of VPNs on personal devices.
- Do not attempt to install software on, or otherwise alter, College IT systems without the express permission of the IT department.
- Do not use the College's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the College monitors use of the College's IT systems, and that the College can view content accessed or sent via its systems.

Breaches of this Policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the College's usual procedures. In addition, a deliberate breach may result in the College restricting your access to College IT systems.

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the College community is being harassed or harmed online you should report it to the DSL. Reports will be treated in confidence.

Passwords

Passwords protect the College's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

You will be required to change your password every regularly to mitigate the risk of any unknown password and the IT department will monitor password strength or shared passwords and request password changes where necessary. If a password is deemed not

IT Acceptable Use Policy

complex enough and the staff member of student does not ensure that their account is secure the IT department may reduce or restrict access to our systems.

Our minimum password complexity requires your password to be at least 8 characters long, contain at least one upper-case, one lower-case and one number. It cannot include your name or be a recently used password.

When you receive your login for the first time you will receive a password that the IT staff will have seen. You are strongly advised to change this password at the first opportunity. On a College owned device this can be done from within the 'change a password' dialog box in Windows. If you have forgotten your password then please visit the IT Services department who will be able to assist you.

Multi Factor Authentication

All staff have access to a vast amount of data on a variety of different subjects, such as students, parents and the general running of the college. To ensure that our data is secure we enforce multi factor authentication on all staff that are attempting to access school data via their Microsoft storage, or our MIS systems.

The methods of authentication we use are:

- Passwords (as above)
- Biometrics
- Authenticator apps
- IP based authentication
- Trusted devices

Use of Property

Any property belonging to the college should be treated with respect and care and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the IT Services department.

Use of College systems

The provision of College email accounts, Wi-Fi and internet access is for official College business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their College IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the College's right to monitor and access web history and email use.

Use of personal devices or accounts and working remotely

All official College business of staff and governors must be conducted on College systems, and it is not permissible to use personal email accounts for College business. Any use of personal devices for College purposes, and any removal of personal data or confidential information from College systems – by any means including email, printing, file transfer,

IT Acceptable Use Policy

cloud or (encrypted) memory stick – must be registered and approved by the IT Services department.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the College's policies, including two factor authentication when off site.

Monitoring and access

Staff, parents and pupils should be aware that College email and internet usage (including through College Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and College email accounts may be accessed by the College where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Any personal devices used by pupils, whether or not such devices are permitted, may be confiscated and examined under such circumstances in conjunction with the Arrangements for Searching Pupils Policy.

Tracking Devices and Technology

The College is not responsible for individual settings on personal devices, nor for the use of tracking apps / devices for purely personal and domestic purposes.

Use of this technology in the context of College activities is not specifically encouraged but if parents do plan to use it then they should be aware of potential third-party privacy considerations and only use it for domestic / personal purposes in respect of their own child and/or their or their child's belongings.

Compliance with related College policies

To the extent they are applicable to you, you will ensure that you comply with the sections regarding online safety in the 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.

Retention of digital data

Staff and pupils must be aware that all emails sent or received on College systems will be routinely deleted after 3 years and email accounts will generally be closed within 1 year of that person leaving the College.

Any information from email folders that is necessary for the College to keep for longer, including personal information, should be held on the relevant personnel or pupil file. Important records should not be kept in personal email folders, archives or inboxes, nor in local files. Hence it is the responsibility of each account user to ensure that information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the College's email deletion protocol.

IT Acceptable Use Policy

If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact itsupport@lordwandsworth.org. Further information regarding this can be found in the Data Retention Policy.

Data Breach reporting

The law requires the College to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the College regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data.
- any external hacking of the College's systems, e.g. through the use of malware.
- application of the wrong privacy settings to online systems.
- misdirected post, fax or email.
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The College must generally report personal data breaches to the ICO without undue delay if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the College must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or pupils become aware of a suspected breach, directly contact the Director of IT services and email datacompliance@lordwandsworth.org.

Data breaches will happen to all organisations, but the College must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The College's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

Artificial Intelligence

Artificial Intelligence is changing the way that we all interact with technology. As a college we embrace the opportunities that AI and LLM's provide for us, whilst being considered about the possibilities for bias and inaccurate data that may be produced.

IT Acceptable Use Policy

For further information on the College's work with AI and LLMs please refer to the Artificial Intelligence policy.

Breaches of this Policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the College's usual procedures. In addition, a deliberate breach may result in the College restricting your access to College IT systems.

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the College community is being harassed or harmed online you should report it to the DSL. Reports will be treated in confidence.

Misuse: Statement of Policy

Lord Wandsworth College will not tolerate any illegal material and will always report illegal activity to the police and/or the LSCB. If the College discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). The College will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy.

Safe Use of Personal Electronic Equipment

- The College's guidance is that pupils and staff should always think carefully before they post any information online. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.
- The College offers guidance on the safe use of social networking sites and cyberbullying through assemblies, talks and PSHEE lessons. The guidance covers blocking and removing contacts from 'friend lists'.
- The College provides guidance on what to do if being stalked or harassed online.
- The College offers guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential in the e-world.
- The College gives guidance on how to keep safe at home e.g. not opening unknown attachments and reporting any illegal content.
- Similarly, the College covers how a mobile phone filter can be activated and how to block nuisance callers.
- The College advises on the responsible use of webcams. It appreciates that free video calls can provide boarders, particularly overseas boarders, with an invaluable means of maintaining contact with their families and friends.

Further information regarding eSafety issues and safe use of electronic equipment can be found in the College's Safeguarding and Child Protection Policy.

IT Acceptable Use Policy

Use of Mobile Phones and other devices

There are guidelines in place to ensure that staff and pupils are responsible in their use of mobile phones and devices both during the working day and during their free time and to enable them to benefit from the advantages of mobile technology during the working day.

Appropriate use of mobile phones and devices during the school day

1st – 5th form pupils are not permitted to have mobile phones/devices on their person during the school day. 3rd -5th form students are required to hand in their mobile phones at the boarding house during the day where it will be securely stored. Mobile phones should be handed in by 8:30am each morning, Monday to Friday, and can be collected any time after 6pm or when the student is leaving for the day. Your laptops provide all the digital access that is needed during the day, so you do not need to carry your phone.

- Phones may not be taken on day trips out of school. They should be handed in at the boarding house as normal before the trip and collected after the trip.
- Students may keep their mobile phones with them on Saturday, but they must be not seen and not heard on campus from 8:30 until 11:30am.
- Students attending an away fixture may collect their phone to take with them, but the phone must only be used on transport and must not be seen or heard at the fixture. This applies to fixtures on any day of the week
- Students who are overseas boarders may access their phones as required for communication with their family. If this is during time when phone access is restricted, the phone should be collected from matron, used in house and then be returned to matron.
- Sixth Formers can use their mobile phones in the Sixth Form Centre, but they must be not seen and not heard anywhere else on campus between 8:30am and 6pm Monday to Friday and Saturday morning. This includes outdoor spaces.
- For all students, phones that are seen when students are not supposed to be carrying them or using them will be confiscated and passed on to your Houseparent.

Appropriate use of mobile phones and devices during boarding time in Houses

The House Handbooks state the rules regarding the use of mobile phones in Houses. These are also displayed on House noticeboards.

In the boarding house, mobiles and other devices should not be used after 'lights out'. 3rd, 4th and 5th Form students need to hand in all devices to the staff member on duty before lights out.

Lord Wandsworth College expects all pupils and staff to adhere to this policy. The College may impose sanctions for the misuse, or attempted misuse of the internet, mobile phones and other electronic devices.