Watford Grammar School for Girls

Information Technology Policy

This policy adopted by Curriculum Committee	November 2020
Next review date	November 2022
Committee Responsible	Curriculum
Template	WGGS
Category	Non-Statutory

Contents

Page

IT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.
However, the IT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.
This policy aims to:

- Set guidelines and rules on the use of school IT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of IT systems
- Support the school in teaching pupils safe and effective internet and IT use

This policy covers all users of our school's IT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our behaviour policy.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2018
- Searching, screening and confiscation: advice for schools

3. Related policies

This policy should be read alongside the school's policies on:

- Esafety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection

4. Definitions

"IT facilities": includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the IT service

- "Users": anyone authorised by the school to use the IT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- "Personal use": any use or activity not directly related to the users' employment, study or purpose
- "Authorised personnel": employees authorised by the school to perform systems administration and/or monitoring of the IT facilities
- "Materials": files and data created using the IT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

5. Unacceptable use

The following is considered unacceptable use of the school's IT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).
Unacceptable use of the school's IT facilities includes:

- Using the school's IT facilities to breach intellectual property rights or copyright
- Using the school's IT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's IT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the IT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's IT facilities
- Causing intentional damage to IT facilities
- Removing, deleting or disposing of IT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's IT facilities.

5.1 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action. For staff, this will be in line with the school Disciplinary policy. For students, the protocols in the 'Unacceptable use of IT' document (appendix three) will be used.

6. Staff (including governors, volunteers, and contractors)

6.1 Access to school IT facilities and materials

The IT Strategic Lead manages access to the school's IT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's IT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT Team.

6.2 Use of phones and email

The school provides each member of staff with an email address.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the IT team immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff should, whenever possible, use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for IT acceptable use as set out in section 4.

6.3 Personal use

Staff are permitted to use school IT facilities occasionally for personal use subject to certain conditions set out below. Personal use of IT facilities must not be overused or abused.

Personal use is permitted provided that such use:

- Does not take place during contact time.
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's IT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's IT facilities for personal use may put personal communications within the scope of the school's IT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of IT (even when not using school IT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

6.4 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

6.5 Remote access

We allow staff to access the school's IT facilities and materials remotely via the LARA system. This is managed by the IT team. All staff are able to access the network remotely using their network log ins. Staff accessing the school's IT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's IT facilities outside the school and take such precautions as the IT team may require, from time-to-time, against importing viruses or compromising system security.

Our IT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

6.6 School social media accounts

Detail about the school social media accounts, and how the guidelines within which they are managed, is given in the ESafety policy.

6.7 Monitoring of school network and use of IT facilities

The school reserves the right to monitor the use of its IT facilities and network. This includes, but is not

limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised IT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.
The school monitors IT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and IT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

7. Pupils

7.1 Access to IT facilities

Computers and equipment in the school's IT suite are available on an open-access basis to pupils at break and lunch time. Specialist IT equipment, such as that used for music or design and technology must only be used under the supervision of staff.

7.2 Have your own device

Students in all years may bring a laptop or tablet device to school so that it may be used for educational purposes.

Any device brought into school remains the responsibility of the student. The school is not liable for any loss of, or damage to a device. Parents are advised of this and encouraged to consider appropriate insurance.

A student bringing a laptop or tablet to school must:

- Connect to the student wifi network. It is not permitted to access the internet via 3G, 4G or 5G.
- Use it only with the permission of a class teacher.
- Ensure that their use of the device is in accordance with the student Acceptable Use Policy (see appendix)

Students who bring mobile phones to school must then follow the guidance in the school rules about their use during the day.

7.3 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

7.4 Unacceptable use of IT and the internet outside of school

The school may sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following at any time (even if they are not on school premises):

- Using IT or the internet to breach intellectual property rights or copyright
- Using IT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restrITed areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's IT facilities
- Causing intentional damage to IT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

8. Parents

8.1 Access to IT facilities and materials

Parents do not have access to the school's IT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

9. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's IT facilities should use safe computing practices at all times.

9.1 Passwords

All users of the school's IT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

9.2 Software updates, firewalls, and anti-virus software

All of the school's IT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's IT facilities.

Any personal devices using the school's network must all be configured in this way.

9.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

9.4 Access to facilities and materials

All users of the school's IT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the IT team.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the IT team immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

10. Internet access

The school wireless internet connection is secured. Appropriate filtering is in place, as is explained in the ESafety policy.

10.1 Pupils

Students bringing their own devices to school must connect to the student wifi network. They may not access the internet using 3G, 4G or 5G technology. This is to ensure that their access to the internet is filtered.

10.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)

- Visitors need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)
- Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The Headteacher and Assistant Head with responsibility for IT will monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.
This policy will be reviewed every 2 years.

Appendix one
ACCEPTABLE USE AGREEMENT: STUDENTS

I understand that IT systems in school - including the internet, email, digital video and mobile technologies - are provided for educational purposes.

Learning effectively

- I will use the school IT systems to support my learning.
- I will listen carefully to the advice I am given by my teachers, and use IT as they show me in order to help me learn.

Keeping safe

- I will choose a strong password. I will not reveal it to anyone. I will only log on to the school network/learning platform with my own user name and password.
- If I discover an unsuitable site, I will switch the screen off and immediately tell a teacher.
- I will not bypass or attempt to bypass any of the security features provided at the school.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately
- If I feel bullied online then I will tell my parent/ carer or a teacher.
- For school-related activities, I will only use my school email address.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone via the internet.

Showing respect for others

- I will make sure that all digital communication with students, teachers or others is responsible, appropriate, inoffensive and sensible. This is both inside and outside of school, and includes use of social media.
- I will not use IT systems to bully or harass someone else.
- I will respect the privacy and ownership of others' work on-line at all times. I will not bring into school any illegal content, including pirated songs, movies, software, offensive material and will not try and share or distribute it further.
- I will seek permission from my teacher before I take, store and distribute images, audio or videos of students and/ or staff. These digital recordings must never be of an inappropriate or offensive nature. If asked to delete any digital recordings I will do so from all media (i.e. USB, home computer etc)
- I will ensure that my digital activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring it into disrepute.

Taking care of our resources

- I will not download or install software on school technologies.
- I will log off when I have finished using a computer to allow others to use the machine.
- I will not deliberately damage computer, systems or networks and will report any incidents of damage I see to staff.
- I will not consume food or drink in the IT rooms.

My own device

I understand I may bring a device to school.

- I understand that I may use my own device for educational purposes only.
- I may use my device in lessons only if the teacher has given me permission.
- If I am using my device in class, I must keep my device in full view of the member of staff throughout the lesson.
- I understand that all incoming messages must be ignored completely until after a lesson. Audible alerts that a message has arrived must be turned off.
- I will not use my device to access text messages, personal emails, social media or other communications during lesson time.
- I must access the internet via the school wifi system. I may not connect to the internet via 3G, 4G or 5G.
- I am entirely responsible for the security and maintenance of any device and understand that school is under no obligation to investigate or compensate me or my parents for any loss or damage to devices whilst they are in school.
- I am responsible for charging my device and may not charge it during the day in school. The only exception to this is for sixth formers, who may charge devices in the Tennet Centre.
- I will not use my device at lunchtime. The only exceptions to this are if a member of staff has given permission and for sixth formers in the Tennet Centre.
- I understand that if I do not use my device in line with these rules, I may be told that I cannot bring it to school.

I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer or even the police may be contacted.

I understand the school has the right to monitor my use of the school network to ensure that this Acceptable Use Agreement is being followed.

Appendix two: Acceptable use, staff

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed reasonable by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, social networking username, twitter account and personal email address, to students unless sanctioned by the Head. I will not use any personal account for communication with students unless sanctioned by the Head.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any hardware of software without permission of the Network Manager or e-Safety Co-ordinator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/ or staff will only be taken, stored and used for professional purposes In line with school data protection policy.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head.
- I will respect copyright and intellectual property rights.
- I will not bring into school any illegal content, including pirated songs, movies, software, offensive material and will not try and share or distribute it further.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. This will include for example, posts on social networking sites, video and photo publishing and sharing sites.
- I will support and promote the school e-Safety policy and help students to be safe and responsible in their use of ICT and related technologies.
- By logging into this PC or Laptop I agree to abide with the terms of the school IT policy and school Esfaety policy. Every login is captured and can be used in evidence if a policy breach occurs.

<u>Bringing My Own Device to use in school (Laptop, tablet, kindle, mobile phone etc)</u>

- Staff are allowed to access the school network using their own devices. They may use their own devices only when connected to the 41075_staff network.
- I understand my device must be on silent when outside the staff areas.
- All incoming messages will be ignored completely when in a classroom. Audible alerts that a message has arrived must be turned off.
- I will not use my device to access text messages, personal emails, social media or other communications during lesson time.

*Asterix denotes that the term "staff" includes individuals on the Schools Direct scheme and PGCE candidates.

Please note - on the last day of service your account will be deleted, email address and O365 accounts will be closed due to Microsoft Licencing compliance terms and conditions. Please ensure that you handover any relevant data to your successor. By signing this agreement that you understand that removing data from the school that contains sensitive information, that you are breaching the GDPR.

Appendix three: Unacceptable use of devices

Occasions will arise when students misuse devices. This may involve:

- Using devices at lunchtime when this is not permitted.
- Using devices during a lesson time for non-work purposes.
- Using devices to access inappropriate material.
- Using devices to cyber-bully.

Any staff member who encounters a student using a device deliberately to access inappropriate material or to cyber-bully should treat this as a serious incident.
The student should be told to turn off the device, and the member of staff should then immediately report the incident to the on-call member of SLT. It should be recorded on CPOMS as soon as possible.
Students misusing devices in these ways will receive sanctions designed to acknowledge the severity of the issue and to educate the student about safe behaviour. The exact sanctions remain at the discretion of the school, and will be applied after careful consideration of the details of the incident and also with an awareness of the context of the student. Examples of sanctions which may be applied include:

- Informing parents
- Requiring the student to attend an after-school safety class.
- A detention (if longer than 15 minutes, 24 hours notice will be given).
- Requiring the student to engage in restorative justice by apologising to students who have been hurt.
- Denying the student permission to bring a device to school, either permanently or for a fixed period of time.
- Fixed term or permanent exclusion.

A student using a device at lunchtime or for non-work purposes should be warned and told to stop their behaviour.
The misuse of the device should then be recorded using the 'device misuse' form.
The Assistant Head with responsibility for IT will monitor this form weekly and share reports with Heads of Year. If a student is reported three times, the Assistant Head will send a letter to the student's family, warning them that if a further breach is reported, the student will lose the right to bring a device to school. If a further breach is reported, the student will be prohibited from bringing a device to school for a fortnight.
The school reserves the right to apply this policy with discretion and an awareness of the content of individual students. It may be necessary, on occasion, to prohibit a student from bringing a device to school after only one or two reports of misuse. It may also be appropriate to apply a sanction from the list above as an alternative to prohibiting the student bringing the device to school.