Watford Grammar School for Girls

Information Technology Policy

This policy adopted by Curriculum Committee	November 2023
Next review date	November 2024
Committee Responsible	Curriculum
Template	WGGS
Category	Non-Statutory

Table of Contents

1. Introduction and aims

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 or staff Code of Conduct.

2. Relevant legislation and guidance

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

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- 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
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

- Meeting digital and technology standards in schools and colleges

3. Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff Code of Conduct
- 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.

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
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):
    - During assessments, including internal and external assessments, and coursework
    - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

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.

6. 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 staff Code of Conduct. For students, the Behaviour Policy will guide any action taken.

7. Staff use (including governors, volunteers, and contractors)

7.1. Access to school IT facilities and materials for staff

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.

Teaching staff are provided with school laptops, and non-teaching staff an appropriate desktop or laptop.. These should be the only devices used for work purposes in school. It should normally be the case that staff with laptops use these, rather than personal devices, if working off-site.

If a member of staff uses a personal device for work purposes off-site then they must use school-approved remote solutions.

7.2. 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.

7.3. 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. 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.

7.4. 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. Details are given in the Code of Conduct.

7.5. 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.

8. School social media accounts

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

9. 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

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

Further details about internet filtering and monitoring are given in the Online Safety Policy.

10. Pupils

10.1. 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.

10.2. 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 Online Safety Policy).

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

10.3. Examining content on student devices.

Whilst investigating incidents of behavior, or supporting a student with a safeguarding concern, it is sometimes the case that a member of staff will find it helpful to see content on a student device. For example, it may be helpful for a member of staff to see screenshots linked to an issue of cyber-bullying. Details of the process to be followed are to be found in the Online Safety Policy.

10.4. 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 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 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

11. Parents

11.1. 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.

12. 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.

12.1. 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.

12.2. 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.

12.3. Data protection

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

12.4. 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.

12.5. Internet access

The school wireless internet connection is secured. Appropriate filtering and monitoring is in place, as is explained in the Online Safety policy.

12.6. 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.

12.7. 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.

13. 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.

Copies of the Acceptable Use Policies were previously included as appendices, but have been removed from this policy as they are now in the Online Safety Policy.