Walthamstow School For Girls

"Neglect not the gift that is in thee"

Policy Document

ICT and Online Acceptable Use Policy

Author(s):	**Dave Shackson**
Ratification Date:	**December 2023**
Next Review Date:	**December 2024**
Reference:	**_POLICY_V2.0**

CONTENTS PAGE

1. INTRODUCTION AND AIMS

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for students, staff (including the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, students, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching students safe and effective internet and ICT use
- This policy covers all users of our school's ICT facilities, including governors, staff, students, volunteers, contractors and visitors.
- Breaches of this policy may be dealt with under our Capability Policy, Behaviour for Learning Policy or the Parent and Carer 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. DEFINITIONS

- **ICT facilities:** 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 that may become available in the future which is provided as part of the school's ICT service

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

See appendix 4 for a glossary of cyber security terminology.

4. UNACCEPTABLE USE

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

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT 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
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its students, or other members of the school community
- Connecting any device to the school's ICT 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 programme, tool or item of software designed to interfere with the functioning of the school's ICT 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 ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel 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 or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

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
- To create fake images, video and or audio of members of the school community

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

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion. For example a lesson in ICT may involve testing AI tools in a way that might otherwise be unacceptable use.

4.2 Sanctions

Students and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's relevant policies listed in 1.
Ultimately the school reserves the right to withdraw ICT access from anyone in breach of this policy.

5. STAFF (INCLUDING GOVERNORS, VOLUNTEERS AND CONTRACTORS)

5.1 Access to school ICT facilities and materials

The school's Network Manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

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

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

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

5.1.1 Use of phones and email

The school provides each member of staff with a Microsoft 365 account that includes an email address and access to the school's TEAMs file storage.
This email account should be used for work purposes only.
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/carers and students, 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 stored in the appropriate Microsoft TEAMs folder so that the information is only accessible by the intended recipient and others authorised to view those attachments.

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 that contains the personal information of another person, they must inform the SLT Member in charge of Data Protection or the Data Manager immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or students. Staff must use phones provided by the school to conduct all work-related business. In circumstances where staff have no choice but to use a personal phone (on a school trip dealing with an emergency or working from home) they should dial the appropriate code to anonymise their number.

School mobile phones should 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 ICT acceptable use as set out in section 4.

The school can record incoming and outgoing phone conversations as well as meetings conducted on TEAMs but participants must be informed.

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The network manager as directed by the Headtacher may withdraw or restrict this permission.

Personal use is permitted provided that such use:

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

Staff may not use the school’s ICT 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 ICT facilities for personal use may put personal communications within the scope of the school’s ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the these same restrictions

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

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

5.2.1 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times. Teaching staff should be aware that aspects of the Teaching Standards do apply to personal conduct outside of school which includes conduct on social media.

Staff should not share information about the school, students and other staff on their open social media accounts other than information that is already in the public domain.

Under no circumstances should staff follow students on social media nor should they communicate with students through private social media. If a student contacts a staff member through public social media they should direct them to use school email and make no further contact.

If a staff member is concerned that they are being contacted or “followed” by students on social media they should bring that to the attention of a member of the SLT or, where there is a safeguarding concern, the DSL.

Staff should not have contact with former students through private email or social media until the year they turn 19.

5.3 Remote access

We allow staff to access the school’s ICT facilities and materials remotely.

This includes

- Access to Microsoft Office 365 Accounts
- In some cases, direct access to the school network

Staff accessing the school's ICT 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 ICT facilities outside the school and must take such precautions as the against importing viruses or compromising system security.

Our ICT 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.

Remote access to the school's ICT network should only be done on secure networks and within the UK or European Union.

5.4 School social media accounts

The school has social media accounts using X (formally known as Twitter) and Instagram. Guidelines and information on how these are managed can be found in Appendix 1.

5.5 Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

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

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The school uses a filtering system as provided through London grid for Learning.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT 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

Our governing board is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
  - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
  - It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

6. STUDENTS

6.1 Access to ICT facilities

All students are given access to the school ICT network through a login and school Microsoft Office 365 account:

- Computers are available for use in ICT rooms. There are also a supply of iPads and laptops that may be used by students in some lessons or circumstances
- In lessons the use of ICT equipment is directly supervised by staff but students are able to access ICT facilities at other unsupervised permissible times for work and study (for example in the LRC or ICT suites at lunchtimes.)
- Students can also access their Microsoft Office 365 accounts outside of school.

6.2 Search and deletion

Under the Education Act 2011, the headteacher, and any member of staff authorised to do so by the headteacher, can search students and confiscate their mobile phones, computers or other devices.

More information on the circumstances in which searchers can be conducted and the processes involved can be found in the school's Searching Students Policy.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The student and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for, or deleting, inappropriate images or files on students' devices will be dealt with through the school complaints procedure.

6.3 Unacceptable use of ICT and the internet inside and outside of school

The school will sanction students, in line with the Behaviour for Learning Policy if a student engages in any of the following **at any time** (even if they are not on school premises but using school ICT facilities):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT 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 making 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
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other students, 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 ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. PARENTS/CARERS

7.1 Access to ICT facilities and materials

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

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

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

Parents are provided with access to a school financial transaction account (SQuid) and a school data and reporting account (Go4Schools). We ask that parents make sure they access these accounts in a secure way and carefully manage password security.

On some occasions school events such as Parents' and Carers' Evenings will be conducted online using School Cloud. Other events may also be hosted on TEAMs. When involved with such events we ask that parents and carers abide by our Parent and Carers' Code of Conduct. We also ask that:

- Participants abide by any camera on/off protocol as set out before the event
- Do not record the meeting unless that has been agreed to
- Ensure the meeting is taking place in an appropriate setting
- Participants may blur a background in the interests of privacy.

7.2 Communicating with or about the school online

We believe it is important to model for students, and help them learn, how to communicate respectfully with, and about, others online.

Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with the school online.
If using email, we ask that parents use the info@wsfg.waltham.sch.uk email to contact any school staff, indicating in the header which staff member they wish to contact
We ask parents/carers to abide by the Parent and Carer Code of Conduct when communicating with the school online.

7.3 Communicating with parents/carers about student activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out that involves communicating with an external organization.
Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

7.4 Use of ICT in school by parents and carers

When attending a school event or meeting there must be no audio or visual recording by any party unless a prior arrangement has been made. For school events like concerts the school will communicate the rules regarding recording or taking photographs in advance of the event if it is to be allowed.
In all circumstances the default position is that no recording is allowed.
Images and recordings made in the school should not be placed online by parents and carers without prior permission.

8. DATA SECURITY

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.
Staff, students, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

All users of the school's ICT 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 students who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and 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 ICT facilities.
Any personal devices using the school's network must all be configured in this way.

8.3 Data protection

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

8.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices. These access rights are managed by the network manager.
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 network manager 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 shut down completely at the end of each working day. In cases where staff need to leave a PC on for remote access, they should always lock the system.

8.5 Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.
School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as student information) out of school if they have been specifically authorised to do so by the headteacher.
Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Network Manager.

9. PROTECTION FROM CYBER ATTACKS

Please see the glossary (appendix 4) to help you understand cyber security terminology.
The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure

Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:

- Check the sender address in an email
- Respond to a request for bank details, personal information or login details
- Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data

Put controls in place that are:

- **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
- **Up to date:** with a system in place to monitor when the school needs to update its software
- **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical each day and store these backups on drives not connected to the school network.
- Delegate specific responsibility for maintaining the security of our Office 365 system to the Data Manager and ICT Technicians.
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification

- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident
- Work with our Local Authority to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. INTERNET ACCESS

The school's wireless internet connection is secure.

- A separate guest account is provided for visitors to the school requiring WiFi access.

10.1 Students

Access to the school WiFi by students is only allowed for students in years issued with iPads

10.2 Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the headteacher or Network Manager.

The headteacher or Network Manager will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer)
- 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 SLT member in charge of ICT will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year.

The governing board is responsible for reviewing and approving this policy.

12. RELATED POLICIES

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

- Online Safety Policy
- Business Continuity and Critical incident Plan
- Safeguarding Policy
- Positive Behaviour for Learning Policy
- Staff Code of Conduct
- Data Protection Policy
- Searching Students Policy

Appendix I

Social Media Protocols at Walthamstow School for Girls

Principles

Social media is used by Walthamstow School for Girls to publicise the school, its achievements and activities and to engage with the community as widely as possible.

However in doing so it is very important, in terms of observing online safety, that we do so in a manner that protects the students, staff and wider community and also protects the reputation and public perception of the school.

Social Media Accounts

1. Currently Walthamstow School for Girls will only operate a single X (formally known as Twitter) and Instagram account.

2. Walthamstow School for Girls will only operate central accounts.

3. Our accounts are identified by the tag @WalthamstoWSFG and our nickname is WSFG.

4. The accounts will be run the Support Admin assigned to Website & Social Media.

5. On most occasions the social media accounts are monitored on a weekly basis during working hours.

6. The School issued mobile phones are linked with a Whatsapp account. Staff using these phones will use this feature to share photographs of the trip that can then posted by the Website and Social Media team.

7. Photograph permissions should be checked before taking photographs but where this has not occurred, this must always be highlighted by the person sharing the photograph for possible publication.

8. While the school's data protection policy does normally allow the use of first names on publicity, they are not used on Twitter or Instagram. While our feeds are regularly checked, the possibility of "trolling" comments naming a student and commenting in a cruel manner can still occur and remain unblocked, especially on weekends and during holiday periods. In addition, the terms and conditions of both social media platforms means that they have been given ownership of the images and we cannot control their further use or impose our copyright.

Twitter

9. Twitter is used as the main social media for publicity and communication. It is recognised that this is currently the most useful social media platform to communicate a public face in an open and transparent manner.

10. The account is public and, as a rule, will not block any followers or individuals wishing to make a comment that will then appear on our feed.

11. In order that their comments do not appear on the school's public feed, Walthamstow School for Girls will block users who:

- Engage in deliberate harassment or "trolling" whereby the purpose is to deliberately create a conflict rather than contribute positively to a discussion.
- Make offensive comments especially those that are racist, sexist, homophobic or generally violate the principles of our Equal Opportunities Policy.
- Are students who are clearly making comments that identify information about themselves or others that could be deemed sensitive information including special characteristics data.
- Are parents or carers who are clearly making comments that identify information about their children or others that could be deemed sensitive information including special characteristics data.

- Are staff who are clearly making comments that identify information about themselves, their students or others that could be deemed sensitive information including special characteristics data. Staff can also be referred to the headteacher for disciplinary action in circumstances where this is a breach of the school's GDPR compliant policies.
- Make unfounded accusations that bring the school into disrepute.
- Are individuals who have significant public notoriety because they have been convicted of a crime or are well known for expressing publically, views or values that are not consistent with the views and values that underpin the school's commitment to equal opportunities and British values.
- Are individuals who express views that are not supportive of girls' education and women's rights.
- Make posts that the school decides will have a negative impact on the safety or wellbeing of students or staff.

12. In cases where a user makes a post that meets the criteria of any of the above, but is not done with malicious attempt, the school will attempt to contact them through direct messaging and attempt to have the relevant post deleted or modified.

Instagram

13. Instagram is used as a secondary form of social media. It is recognised that this is very popular with students and is used to share photographs of events in school and others which the school is involved with.

Students as followers

14. The school does not proactively monitor its followers and seek to identify students. However, if it becomes apparent that the account of a follower is clearly set up in such a way that it puts a student at risk because it clearly identifies them and sensitive information pertaining to them, the school will contact the family of that student to suggest changes.

15. The school does not take responsibility for enforcing the terms and conditions of Twitter or Instagram amongst its followers.

Following

16. The school does follow:

- Organisations and individuals that are associated with the school or are linked with the school in some capacity but are not employees of the school.
- Organisations and individuals that promote values shared by the school, especially in empowering girls and young women.
- Other schools in the Local Authority
- Sixth Forms and Colleges.
- Universities and institutions offering further education and training.
- Organisations that offer careers and further education opportunities available to our students.
- Members of local and national government (e.g. the sitting MP) directly linked to the school and its community but only in their executive or official capacity. The school does not follow party political groups or individuals seeking elected office.
- Community, social, spiritual and sporting organisations that offer opportunities for our students in the local community.

17. Unless they fall under the above criteria the school does not normally follow former members of staff or former students.

18. The school does not take action against accounts that link themselves with the school or identify closely with the school unless those accounts fraudulently suggest they have official status or there is a possibility that a reasonable person would misinterpret them as having official status.

Appendix 2: Acceptable use agreement (students and parents/carers)

ACCEPTABLE USE OF THE SCHOOL’S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS

Name of student:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school’s ICT systems (like computers) and get onto the internet in school I will:

- Always use the school’s ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a permission at times where use is allowed
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher or other staff member immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I’ve finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school’s network using someone else’s details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

I agree that the school will monitor the websites I visit and that there will be consequences if I don’t follow the rules.

Signed (student):	**Date:**

Parent/carer’s agreement: I agree that my child can use the school’s ICT systems and internet. I agree to the conditions set out above for students using the school’s ICT systems and internet, and for using electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of students unless authorised to do so
- Share confidential information about the school, its students or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that students in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website

TERM	DEFINITION
	address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it’s from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim’s computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user’s identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.