TOLWORTH GIRLS' SCHOOL & SIXTH FORM
ICT ACCEPTABLE USAGE POLICY

Governing Body Committee: Finance, Assets & Audit (F, A & A)
Date approved: January 2023
Next review: January 2025

Contents

1. Introduction and aims

The Governors of Tolworth Girls' School & Sixth Form, the Headteacher and staff wish to encourage students to use the ICT facilities at school for educational purposes. The responsible use of these facilities contributes significantly to the rich academic and personal experience of the students.

The guiding principle that underpins this policy is that ICT should be used responsibly at all times. This applies to all members of the school community.

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

However, the ICT resources and facilities our academy uses 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 academy's policy on data protection, online safety and safeguarding.

- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems.
- Support the academy in teaching students' safe and effective internet and ICT use.

This policy covers all users of our academy's ICT facilities, including governors, staff, students, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our Behaviour/Staff Disciplinary/Staff Code of Conduct policies.

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 2022
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

3. Definitions

"ICT 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 ICT service

"Users": anyone authorised by the school to use the 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

"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 ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See **appendix 6** for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the academy's ICT 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 academy's ICT facilities includes:

- Using the academy's ICT facilities to breach intellectual property rights or copyright
- Using the academy's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the academy'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 (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the academy, or risks bringing the academy into disrepute
- Sharing confidential information about the school, its students, or other members of the school community
- Connecting any device to the academy's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the academy'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 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 academy's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT 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 academy
- Using websites or mechanisms to bypass the academy's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

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

In order to carry out **essential** aspects of their professional role within school, staff in **specific and unusual** circumstances and with the consent of their line manager may have to act differently to the stated practice. Staff will be assumed to be acting in good faith at all times and to safeguard themselves and the academy, these instances should be recorded in writing.

4.2 Sanctions

Students and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the School Behaviour, Staff Disciplinary and Staff Code of Conduct policies.

Dependant on the severity of the breach sanctions may consist of the following:

- Blocked access to ICT facilities
- Restricted access to some systems
- Disciplinary Action – Staff

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

5.1 Access to school ICT facilities and materials

The academy's Network Manager manages access to the academy's ICT facilities and materials for academy 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 log-in/account information and passwords that they must use when accessing the academy's ICT 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 Network Manager.

If access is required to files, this can be arranged in the first instance by contacting the IT Department.

5.1.1 Use of phones and email

- The academy provides each member of staff with an email address.
- 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 encrypted so that the information is only accessible by the intended recipient. Staff should contact the Data Protection Officer (DPO) or IT Support for assistance in this.
- 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 DPO and IT Department immediately.
- Staff must not give their personal phone numbers to parents/carers or students. Staff must use phones provided by the academy 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 ICT acceptable use as set out in section 4.

The academy can record in-coming and out-going phone conversations.

If you record calls, callers **must** be made aware that the conversation is being recorded and the reasons for doing so. For instance:

- "All calls to the school office are recorded to aid administrators"
- "Calls are recorded for use in staff training"

Staff who would like to record a phone conversation should speak to the Network Manager for further assistance in this.

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

Requests to record conversations are normally sanctioned if the following conditions occur:

- Discussing a complaint raised by a parent/carer or member of the public
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Headteacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching hours and/or non-break time.
- 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 academy'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 academy's ICT facilities for personal use may put personal communications within the scope of the academy'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 academy's BYOD policy.

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 academy'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.

5.2.1 Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.
The academy has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.3 Remote access

We allow staff and students to access the academy's ICT facilities and materials remotely this is provided by way of Remote Access.

- The IT Department manages this facility.
- It utilises a secure https connection to our IT System.
- Instructions on how to use are provided at Staff Induction and for students during ICT lessons.

Staff accessing the academy'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 academy's ICT facilities outside the school and take such precautions not to use this facility in an Internet Café.

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.

The academy's Privacy Notice policy can be found on our School Website.

5.4 School social media accounts

The academy has an official Facebook, Instagram, Twitter and YouTube page, managed by the Marketing, Website and Media Co-ordinator. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The academy has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.5 Monitoring of school network and use of ICT facilities

The academy reserves the right to monitor the use of its ICT 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 ICT use in order to:
- Obtain information related to school business
- Investigate compliance with academy 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

6. Students

6.1 Access to ICT facilities

- Computers and equipment in the academy's ICT suite are available to students only under the supervision of staff.
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff.
- Students will be provided with an account linked to the academy's Microsoft 365 environment, which they can access from any device by using the following URL https://www.office.com/
- Sixth Form students can use the computers in the 6th form study room and snack bar area independently for educational purposes only.

6.2 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 students' phones,

computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The academy 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.

Staff members may also confiscate devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse contains an online element.

6.3 Unacceptable use of ICT and the internet outside of school

The academy will sanction students, in line with the Behaviour policy, if a student engages in any of the following **at any time** (even if they are not on school premises):

- 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 academy'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.
- Consensual and 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 academy, or risks bringing the academy into disrepute.
- Sharing confidential information about the academy, 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 academy's ICT facilities.
- Causing intentional damage to ICT 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.

7. Parents/carers

7.1 Access to ICT facilities and materials

Parents/carers do not have access to the academy'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 the PTA) may be granted an appropriate level of access, or be permitted to use the academy'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.

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 through our website and social media channels.

We ask parents/carers to sign the agreement in appendix 2.

8. Data security

The academy is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the academy cannot guarantee security. Staff, students, parents/carers and others who use the academy's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the academy'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/carers or volunteers who disclose account or password information may have their access rights revoked.

All staff are encouraged to use a password manager to help them store their passwords securely.

The IT Department allocates initial password for new users. Staff are required to change their password every 3 months. Students can request a password reset from either the IT Department or the ICT Teachers.

8.2 Software updates, firewalls and anti-virus software

All of the academy's ICT 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 academy's ICT facilities.

Any personal devices using the academy's network are governed by the Bring Your Own Device (BYOD) Policy.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the academy's data protection policy. (***Refer to the academy's Privacy policy***)

8.4 Access to facilities and materials

All users of the academy's ICT facilities will have clearly defined access rights to school systems, files and devices. These access rights are managed by Network Manager.

Users should not access, or attempt to access, systems, files or devices where 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 Department 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.

8.5 Encryption

The academy ensures that its devices and systems have an appropriate level of encryption. Academy staff may only use personal devices upon signing of the BYOD policy.

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.
The academy will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the academy secure.
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the academy'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:
    - **'Proportionate'**: the academy will verify this using a third-party audit (such as this one annually, to objectively test that what it has in place is up to scratch.
    - **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 academy needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be

The back-up of critical data is carried out daily on the premises and replicated to an off site server. We delegate specific responsibility for maintaining the security of our management information system (MIS) to Arbor.

We will ensure staff:

- Use Remote Access when working from home
- Enable multi-factor authentication where they can, on things like CPOMS
- Store passwords securely using a password manager

We will ensure IT staff:

- conduct regular access reviews to make sure each user in the academy 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 seeing if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department, for example:

    - including how the academy will communicate with everyone if communications go down
    - who will be contacted when, and
    - who will notify Action Fraud of the incident. This will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

10. Internet access

The school wireless internet connection is secured. Our Wi-Fi access is subject to the same filtering on our wired network.

We offer a secure wireless connection that only the school supplied wireless devices can use and a BYOD Wi-Fi network that is only available for Staff and Students. We do not offer Wi-Fi access for parents/carers or members of the public.

Our filtering system is not 100% foolproof. If you feel a website has been incorrectly filtered or should be filtered in the first instance, you should contact IT Support Department.

10.2 Parents/carers and visitors

Parents/carers and visitors to the academy will not be permitted to use the academy's Wi-Fi unless specific authorisation is granted by the Network Manager.

The Network Manager will only grant authorisation if:

- Parents/carers are working with the academy in an official capacity (e.g. as a volunteer or as a member of the PTA).
- Visitors need to access the academy's Wi-Fi 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) In this case, a user specific account is created for the visitor e.g. generic accounts are not permitted.

Staff must not give their user account credentials to anyone to access the school Wi-Fi. Doing so could result in disciplinary action.

11. Monitoring and review

The Headteacher and Network Manager monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the academy.

12. Related policies

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

- Bring Your Own Device
- Safeguarding and Child Protection
- Behaviour
- Staff Code of Conduct
- Data Protection

This policy will be reviewed every 2 years.

The F, A & A committee is responsible for approving this policy.

Appendix 1: Facebook cheat sheet for staff

Don't accept friend requests from students on social media

10 rules for academy staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your students
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our academy or your students online – once it's out there, it's out there
8. Don't associate yourself with the academy on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents/carers or students)

Check your privacy settings

- Facebook - Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, students and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list – please review your settings by clicking here
- Facebook - Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- Facebook - The public may still be able to see your profile picture and cover photo, even if your profile settings are private, please make sure they're appropriate
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- Personal Instagram, TikTok accounts should be private, to avoid sharing personal information with students or parents. This should be done by clicking on your profile settings > Privacy and Security > click on Private account.
- In case you have a public professional account (ex. photography, cooking blog), please contact the HR and/or Marketing coordinator to assess the case and note it down
- In case you're not sure of any of the above settings, please email the IT and Marketing team to assist you
- **Google your name** to see what information about you is visible to the public

- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if…

A student attempts to add you on social media

- Do not accept the friend request, take a screenshot and send a report of the request to the Designated Safeguarding lead.
- Check your privacy settings again, and consider changing your display name or profile picture
- If the student asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students and that if they persist, you'll have to notify senior leadership and/or their parents. If the student persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the Headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the academy
    - Students may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current student or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The academy uses the following official channels: • Facebook page, Instagram page,Twitter Page, LinkedIn profile, YouTube page and Our website • Email/text groups for parents (for school announcements and information) • Our remote learning platform Microsoft Teams Parents/carers also set up independent channels to help them stay on top of what is happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the academy via official communication channels, or using private/independent channels to talk about the academy, I will: • Be respectful towards members of staff, and the academy, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the academy's official channels, so they can be dealt with in line with the academy's complaints procedure I will not: • Use private groups, the academy's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the academy can't improve or address issues if they aren't raised in an appropriate way • Use private groups, the academy's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other students. I will contact the academy and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for older students

Acceptable use of the academy's ICT facilities and internet: agreement for students and parents/carers	
Name of student:	
When using the academy's ICT facilities and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Use them to break school rules • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • 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 • Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo • Share my password with others or log in to the academy's network using someone else's details • Bully other people I understand that the academy will monitor the websites I visit and my use of the academy's ICT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material, which might upset, distress or harm others or me. I will always use the academy's ICT systems and internet responsibly. I understand that the academy can discipline me if I do certain unacceptable things online, even if I am not in school when I do them.	
Signed (student):	**Date:**
Parent/carer agreement: I agree that my child can use the academy's ICT systems and internet when appropriately supervised by a member of academy staff. I agree to the conditions set out above for students using the academy's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the academy's ICT facilities and accessing the internet in school, or outside school on a work device, 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 academy'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 academy's network
- Share my password with others or log in to the academy's network using someone else's details
- Share confidential information about the academy, 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 academy

I understand that the academy will monitor the websites I visit and my use of the academy'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 academy's Data Protection policy.

I will let the Designated Safeguarding Lead (DSL) and IT Manager 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 academy's ICT systems and internet responsibly, and ensure that students in my care do so too.

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

Appendix 5: Glossary of cyber security terminology

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

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
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.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like 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.

TERM	DEFINITION
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	Programs 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 executives.