Pate's ICT and Internet

Acceptable Use Policy

Approved by:	Full Governing Board	**Date:** March 2023
Last reviewed on:	Jan 2022	
Next review due by:	March 2026	

Contents

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the everyday life of our school, and is a critical resource for pupils, staff, 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, 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 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 pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors. Breaches of this policy will be dealt with under our Promoting positive behaviour Policy.

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 2022
- 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
- UKCIS 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 which 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, pupils, 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

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.

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 pupils, 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
- Causing 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

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Assistant Headteacher for Technology and Innovation, Head of Computing, Network Manager, or any other relevant member of staff, 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 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on behaviour.

The Schools policies can be found here.

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 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 an email address. This email account should be used for work purposes only. Staff will need to use multi-factor authentication on their email account.

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 that contains the personal information of another person, they must inform the network manager immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents or pupils. Staff must 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 ICT acceptable use.

5.1.2 Connecting devices to our systems

Connectivity of all devices is centrally managed by the Network Manager, who must approve a device before it can be connected to our systems. We reserve the right to refuse or remove permission for your device to connect with our systems.

In order to access our systems it may be necessary for the IT Department to install software applications on your device. If you remove any such software, your access to our systems will be disabled.

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 Headteacher, Network Manager or Assistant Headteacher for Innovation and Technology and may withdraw or restrict this permission at any time and at their discretion.

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 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. 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) for school work.

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 pupils and parents could see them.

Staff should take care to follow the school's guidelines on use of social media 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 always appropriate. Professionality is upmost at all times. Please see the Staff Handbook for more details.

5.3 School social media accounts

If your school has official social media accounts, adapt this section. Otherwise, delete it and renumber the subsections below.

The school has an official account for several online platforms including Facebook, Twitter, etc. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, these accounts.

The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

Some departments have their own social media accounts. There must adhere to the above rules and must re-notify the Assistant Headteacher for Innovation and Technology each September. These can be removed or deleted if used inappropriately.

5.4 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 effectiveness of any filtering and monitoring will be regularly reviewed.

Where appropriate, authorised personnel may raise concerns about monitored activity with the school's designated safeguarding lead (DSL) and Network Manager, as appropriate.

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.

5.5 Responsibilities

All staff have a responsibility for:

- Ensuring responsible ICT use amongst student users.
- Demonstrating best practice.
- Dealing with incidents of breaches in this Policy.
- Reporting incidents of breaches in the Acceptable Use Policy within the school.
- Educating students about the responsible use of ICT.
- Engaging in training events on responsible use of ICT.
- Recording any serious incident in the E-Safety Incident Book, held with the Head's PA

5.6 Data and Communications

All communications and information stored on the ICT systems should be assumed to be property of Pate's Grammar School. Any items stored in your user area or folders within your user area maybe subject to deletion. No member of Pate's Grammar School including the Head Master or the governors can be held responsible for any loss of data.

All portable storage media must be checked for viruses prior to use. Suitable encryption should be used to ensure compliance with the Data Protection Policy. See the Network Manager for guidance.

6. Pupils

6.1 Access to ICT facilities

Computers and equipment in the school's ICT suite are available to pupils. Specialist ICT equipment, such as that used for music, or computer science, must only be used under the supervision of staff.

Pupils will be provided with a Microsoft 365 account which is linked to the SharePoint site for the school, which they can access from any device by using the following: https://patesgs.sharepoint.com/sites/PGS-Home

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 pupils and confiscate their mobile phones, computers, or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out (please see the Promoting Positive Behaviour Policy here), **and/or**

- Is evidence in relation to an offence.

This includes, but is not limited to:

- Pornography.
- Abusive messages, images, or videos.
- Indecent images of children.
- Evidence of suspected criminal behaviour (such as threats of violence or assault).

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the designated safeguarding lead.
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's co-operation.

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk.

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, 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 the Network Manager in conjunction with the DSL / headteacher / other member of the senior leadership team] 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 if there is a good reason to erase data or files from a device, staff members will consider if 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 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 pupil 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) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Promoting Positive Behaviour Policy here.

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

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the Our Promoting Positive Behaviour Policy here, if a pupil 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 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 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 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

7.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT 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.

7.2 Communicating with or about the school online

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

7.3 Communicating with parents about pupil 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. When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents in the same way that information about homework tasks is shared.

In particular, staff will let parents know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction. Parents may seek any support and advice from the school to ensure a safe online environment is established for their child.

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, pupils, parents, 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 pupils 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.

If Teachers need to generate passwords for pupil's accounts, they will keep these in a secure location in case pupils lose or forget their passwords.

All users will be subject to password changes over time as determined by the Network Manager

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 here.

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 a member of SLT or 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.

9. Protection from cyber attacks

Please see the glossary (appendix 1) 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
- Put controls in place that are:
  - **Proportionate**: the school will continue to take external advice from industry experts
  - **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.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT department.
- Make sure that staff:
  - Enforce multi-factor authentication on school Microsoft 365 accounts.
  - Store passwords securely using a password manager.
- 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 and updated to the latest security patches
- 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. This plan will be reviewed and evaluated annually.

10. Internet access

The school's wireless internet connection is secure. It is filtered using a proxy that is maintained monitored by Exa Networks our Internet Service Provider

10.1 Pupils

Wi-Fi is available to students. Instructions on how to do this are found on SharePoint. All student access is filtered by our Proxy. The Wi-Fi will only allow access to content that is appropriate for students.

10.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's Wi-Fi 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 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)

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Online Learning

There may be times, during which the school will deliver online lessons. Please read the guidance below:

- Staff and students must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral background.
- The live class will be recorded, so that if any issues were to arise, the video can be reviewed.
- Language must be professional and appropriate, including any family members in the background.

We as a school are committed to the following and expect you to reciprocate:

- Be positive, responsible, ambitious, and proactive.
- Demonstrate resilience and emotional awareness.
- Be kind, compassionate and listen to others.
- Respond to challenges and make the best of our learning opportunities.
- Ensure we have consistently high levels of respect for each other.
- Have consistently high expectations of behaviour online as we would in the classroom.

Expectations of Students

- Be kind.

- Arrive to lessons on time.
- Be fully equipped for the lesson.
- Follow staff instruction immediately.
- Do not disturb the learning of others.
- Show cooperation and respect at all times.
- To meet deadlines
- Recognise the impact of our behaviour on other people's learning.

12. Monitoring and review

The headteacher, Assistant Headteacher for Innovation and Technology and Network Manager 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 3 years. The Full Governing Board is responsible for reviewing and approving this policy.

13. Related policies

Adapt this list as required.

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

- Online safety
- Safeguarding and Child Protection
- Promoting Positive Behaviour
- Data Protection

Appendix 1: 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 are 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.

Term	Definition
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 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 two 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.

Appendix 2 General Advice

- Be careful with your personal details on the Internet especially on social networking sites such as Facebook and chat rooms.
- Backup your work, the school cannot be held responsible for any loss of data.
- Please report all damage and/or faults of school owned ICT to the ICT Department
- Please report anything that you think maybe in breach of this policy to the ICT Services Team
- Printing is a costly process and has environmental impact – please think before you print.
- You MUST keep your password a secret, and immediately change it if you feel it has become known
- Do not logon with another person's details.
- If you have a social networking profile, you should:
  - Ensure your profile is private.
  - Consider what photos are accessible on your profile and how this may reflect on you in school.
  - Consider what you write on your profile and how this may reflect on you in school.

Appendix 3 Parental Consent and Student User Agreement

Please note that Internet access will not be permitted unless both the Parental Consent and Student Agreements have been signed.

Parental Consent

As a parent or guardian of a student at School, I have carefully read the above information about the appropriate use of ICT facilities and Internet access at the school, and I understand that this agreement will be kept on file.

My child may use the school network in accordance with the ICT Acceptable Use policy ☐

I would prefer that my child is not given access to the school network ☐

Parent Name (print): **Parent Signature:**

Date:

Student Agreement

When using the school'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.
- 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 inappropriate images, videos, or livestreams.
- Share my password with others or log in to the school's network using someone else's details.

I understand that the school will monitor the websites I visit and my use of the school'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 me or others. I will always use the school's ICT systems and internet responsibly.

I understand that any violation of the Acceptable Use Policy will result in the withdrawal of the privilege of Internet access and that I may also be subject to disciplinary action in line with existing policy regarding school behaviour. Temporary or permanent exclusion may be imposed for serious violations and police may be involved or other legal action taken where appropriate.

Student Name (print): **Student Signature:**

Student Tutor Group:

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

Name:

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 pupils without checking with teachers first
- Share confidential information about the school, its pupils 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) and Network Manager know if a pupil 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 pupils in my care do so too.

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