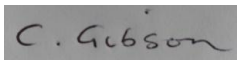
Ryhope Infant School Academy

Acceptable Use Policy

Updated:	**September 2025**
Produced by:	**Mrs T Allen**
	Headteacher
Ratified by:	**Board of Trustees**
Signed:	
	Chair of Trustees
Review Date:	**September 2027**

1. Introduction

1.1. New technologies have become integral to the lives of children and young people in today's society, in schools, and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

1.2. This Acceptable Use Policy (AUP) is intended to ensure:

1.3. that all adults will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

1.4. that school systems and users are protected from accidental or deliberate misuse **and malicious activities, including cyber-attacks**, that could put the security of the systems and users at risk that all adults are protected from potential risk in their use of technology in their everyday work.

1.5. The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

1.6. This school is committed to providing an environment that is at all times conducive to learning. Accordingly, this environment should remain (as far as is practicable) free from disruption or distraction and should allow pupils to concentrate fully on their learning activities.

2. Scope and Purpose

2.1. Where there is reference to adults or staff, this includes all direct employees, supply staff, Trustees, volunteers, college students, trainee teachers, visitors and contractors.

2.2. This policy applies to all adults using our ICT facilities and other communications technologies, ensuring that ICT and other devices are used correctly. Any inappropriate use must be avoided and is the responsibility of every individual. If you are unsure about any matter or issue relating to this policy you should speak to the School Business Manager or Head Teacher.

2.3. The purpose of the policy is to ensure the school network is operated safely and all users of ICT and other communications technologies, are safe. It refers to our school ICT network and to the use of mobile technologies within it and explains the behaviours, which are acceptable and unacceptable within our school.

2.4. Ryhope Infant School Academy has provided laptop computers for use by staff as an important tool for teaching, learning and administration of the school. Use of school computers, by both members of staff and pupils, is governed at all times by the following policy. Please ensure that you understand your responsibilities under this policy, and direct any questions or concerns to the School Business Manager in the first instance.

2.5. School laptops must not be taken offsite without being first encrypted with a secure password. If your laptop is not encrypted, it must not leave the school. Please see the School Business Manager if you require an encrypted laptop.

2.6. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. Our AUP must be fully complied with at all times. All users of the school network should note that it is monitored on a regular basis. Any person who is found to have misused the school system or not followed our AUP could face the following consequences:

- Temporary or permanent withdrawal from the school system
- Suspension or exclusion from the school

- Disciplinary action
- In the most serious cases, legal action may also be taken, **especially in cases involving deliberate attempts to breach network security or conduct cyber-attacks**.

2.7. Whilst our network and systems are organised to maintain the most secure environment possible, it is your responsibility to make sure the children you are directly working with are safe. **You must also remain vigilant against cyber threats such as phishing, ransomware, malware, and other forms of cyber-attacks that could compromise the school's systems.**

2.8. All adults working in school must do so under the guidance of the member of staff to whom they are responsible.

2.9. As an adult working in school you may be the first point of contact in dealing with incidents of misuse or abuse. Every such incident must be reported to the Class Teacher who will then follow the procedures set out in our AUP.

2.10. Your key responsibilities are:

- Maintaining an appropriate level of professional conduct in your own internet use within school.
- Developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children.
- Implementing our school AUP through effective classroom practice.
- Reporting any instances of ICT misuse to the Class Teacher who must report it to the SLT in line with our school AUP. If the Class Teacher is suspected of being involved, report directly to the Head Teacher.
- Supporting pupils who experience problems when using the internet, working with the Class Teacher.
- Using the internet and ICT facilities to ensure that internet safety is not compromised e.g. evaluating websites in advance of classroom use, using child-oriented search engines.
- Embedding internet safety messages.
    - Following the school rules relating to acceptable use of our ICT equipment and other mobile technologies.
    - Reporting any suspicious emails, links, or digital activity immediately to the School Business Manager or Head Teacher, to help prevent potential cyber-attacks.

2.11. Copies of our rules for pupil use of the network are displayed around the school. Please ensure you have read them and make sure the pupils you work with adhere to them.

3. School ICT Network - Managing filtering

3.1. The school Network and associated services may be used for lawful purposes only.

3.2. The school monitoring and filtering system is provided by the school's ICT provider, Omnicom. The school will work with the Omnicom ICT support technicians to ensure systems that protect pupils are reviewed and improved.

3.3. If staff or pupils discover an unsuitable site, it must be reported to the School Business Manager (SBM) and the Designated Safeguarding Lead (DSL).

3.4. The SBM and the DSL will ensure that regular checks are made so that the filtering methods selected are appropriate, effective and reasonable.

3.5. The school will also monitor for and protect against potential cyber-attacks, including attempts to breach the network via phishing, malware, ransomware, or other unauthorised digital intrusions. Any suspicious network activity must be reported immediately to Omnicom and the SBM.

4. Passwords

4.1. Each child and adult working within the school must log on to the computers using the username and password given to them (class account or individual account). Passwords for adults need to be kept a secret. If for any reason an adult needs to leave their computer when it is logged on to their account, they should lock the computer to prevent others from using their account by pressing 'Ctrl, Alt and Delete'. Passwords for adult's accounts will be changed regularly and no less than every 60 days.

4.2. It is forbidden for adults to use other adult's accounts or files. Both adults and children will respect copyright and not copy anyone's work and call it their own.

4.3. For the young children in our school, the adult(s) working with those children will take full responsibility for their safe internet use in school.

4.4. Any supply staff or visitors to the school must see our School Business Manager to obtain a guest account and password. Their password will need to be kept a secret.

4.5. Passwords must be strong and not easily guessable. If a user suspects their password has been compromised through a cyber-attack or phishing attempt, they must report it immediately and change the password without delay.

5. Software and Downloads

5.1. All users are prohibited from installing software onto the network from a CD-ROM, other device or by downloading from the Internet without permission from the SLT. If users need a new program installing onto the computer, our ICT support technicians will be asked to do this if possible.

5.2. Copyright and intellectual property rights must be respected when downloading from the internet.

5.3. Software or downloads from unverified sources can pose a cybersecurity risk. Any attempt to install unauthorised software may result in malware or other cyber threats entering the school network. Staff must remain vigilant and only use software approved and installed by the ICT support team.

6. Personal Use

6.1. The school recognises that occasional personal use of the school's computer is beneficial both to the development of ICT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use:

6.2. Most comply with all other conditions of the AUP as they apply to non-personal use, and all other school policies regarding staff conduct.

6.3. Must not interfere in any way with your other duties or those of any other member of staff.

6.4. Must not have any undue effect on the performance of the computer system; and

6.5. Must not be for any commercial purpose or gain unless explicitly authorised by the school.

6.6. Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

6.7. Staff must ensure that personal use does not expose the network to cyber attacks, including accessing suspicious websites, downloading unsafe files, or opening unverified email attachments.

7. Email

7.1. All members of staff with a computer account in school are provided with a school email address for communication both internally and with other email users outside of school.

7.2. No member of staff (including Trustees) must use non-school email accounts for any school/work related activity – **no exceptions!**

7.3. Users are responsible for e-mail they send and should be aware that these are open to be read and should be treated as public.

7.4. E-mail should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety. Anonymous messages and chain letters must not be sent.

7.5. When writing emails, you should use appropriate language. You should not use language that could be calculated to incite hatred against ethnic, religious or other minority. You need to remember that you are a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.

7.6. All emails both sent and received will be scanned by forensic software.

7.7. E-mail attachments should only be opened if the source is known and trusted.

7.8. Extra caution should be taken when opening email attachments or clicking on links. These are common methods used in cyber-attacks such as phishing. If in doubt, report suspicious emails to the SBM or ICT provider.

7.9. Children are not permitted under any circumstances to e-mail a member of staff using their personal e-mail address. In addition, members of staff should not be emailing children using their personal email address.

7.10. Email is not guaranteed to be private! Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.

7.11. Privacy – personal information should not be revealed to anyone including (e.g. name, address, age, telephone number, social network details) details of other users to any unauthorised person.

7.12. Other users' files or folders should not be accessed without permission.

7.13. Login credentials (including passwords) should not be shared with any other individuals, displayed or used by any individual. If login details are compromised they should be changed immediately and brought to the attention of the Head Teacher.

7.14. After using a computer and before walking away, individuals should log off, if unattended machines are found logged on under another username they should be logged off immediately. (After 2 minutes computers automatically go into hibernation).

7.15. Any unsuitable communications received must be reported to a member of staff immediately.

7.16. All staff are responsible for helping prevent email-based cyber threats by reporting phishing, suspicious messages, or unauthorised access attempts as soon as possible.

8. Images/Videos

8.1 All children need parental permission to have photographs or videos published electronically or in a public area even if they are unidentifiable.

8.2 No photos or videos which include nudity or inappropriate actions are permitted to be taken or downloaded under any circumstance.

8.3 Staff must not upload or share any image or video using external platforms that could compromise school cybersecurity or data protection. Cloud-based services must be approved by the school.

9. Network Protocol

9.1. School computer and Internet use must be appropriate to a pupil's education or to staff professional activity.

9.2. Respect other people's material and do not corrupt, interfere with or destroy them.

9.3. Do not open other people's files without expressed permission.

9.4. When working with personal data ensure that the data is secure.

9.5. All users must take precautions to prevent cyber-attacks such as phishing, ransomware, and malware that can compromise the integrity of the school network. Any suspicious activity or attempted breaches must be reported immediately to the School Business Manager who will contact our ICT support team.

10. Internet Usage

10.1. Pupils must be supervised at all times when using the internet.

10.2. Activities should be planned so 'open searching' is kept to a minimum. The facility for caching sites should be used prior to using the internet with pupils.

10.3. When searching the internet with pupils, adults should encourage the children to use 'child safe' search engines. 'Safe Search' is set on all computers in school as a default on search engines.

10.4. Pupils may not use social networking sites, public chat rooms and messaging systems (e.g. Facebook, Messenger, Twitter). Staff should not access these sites through the school network.

10.5. Use the internet for personal financial gain, gambling, political purposes or advertising is forbidden.

10.6. Visiting websites that may be considered inappropriate or illegal is not allowed. Downloading of some material is illegal and that the police or other authorities may be called to investigate.

10.7. Users must not access suspicious or untrusted websites that could be used to launch cyber-attacks against the school network. All downloads and internet activity should comply with cyber security best practices to protect school data and systems.

11. Use of Social Networking Sites and Online Forums

11.1. Staff must take care when using websites such as Facebook, Twitter, Dating Sites etc, even when such use occurs in their own time and when on their own computer at home. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

11.2. You must not allow any pupil to access personal information you post on a social networking site. In particular:

- **You must** not add a pupil to your 'friends list', nor invite them to be friends with you.
- **You must** ensure that personal information is not accessible via 'Public' setting, but ensure it is to a 'Friends only' level of visibility.
- **You should** avoid contacting any pupil privately via social networking site, even for school-related purposes.
- **You should** take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them to access to your personal information.

11.3. It is advised not to accept invitations from the pupils' parents or carers to add you as a friend to their social networking sites, and you should consider carefully whether to invite them to be your friend, as damage to professional reputations can inadvertently be caused by quite innocent postings or images.

11.4. You will need to ensure that **any** private social networking sites/blogs that you create or actively contribute to are not to be confused with your professional role in anyway.

11.5. Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

11.6. Unless authorised to do so, you must not post comments on websites that may appear as if you are speaking for the school.

11.7. You should not post any material online that can be clearly linked to the school that may damage the school's reputation.

11.8. You should avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass or defame the subject.

11.9. Staff must also be aware that social media platforms can be used as vectors for cyber attacks such as impersonation scams, malicious links, or credential harvesting. Extreme caution must be exercised when interacting with unknown users or suspicious messages.

12. Use of your own Equipment

12.1. Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff, and must not be used until approved. This test must be performed at regular intervals as required by school's normal rules on electrical safety testing.

12.2. You must not connect personal computer equipment to school computer equipment without prior approval, with the exception of storage devices such as USB memory sticks.

12.3. Any personal device connected to the school network must have up-to-date antivirus protection and must not contain any software that could pose a cyber threat to the school system.

12.4. If staff are out on visits or courses, the school mobile phone may be used for contacting school. In emergencies (accidents, bus delays, children ill etc) staff may use their personal mobiles to contact the school or emergency services if the school mobile is not available.

13. Camera Mobile Phones and other Mobile Devices including Smart Watches

13.1. There is significant potential for camera mobile phones to be misused in schools. These can all too easily become an instrument of bullying or harassment directed against pupils and/or staff members.

13.2. Personal mobile phones should not be used in areas of school where pupils are present. During teaching time, mobile phones should be stored in a locker, away from the children.

13.3. Adults are allowed to access their personal phones on breaks, lunch times, PPA and after school BUT only in areas where the children are not present.

13.4. No member of staff should ever use his or her own mobile phone to photograph pupils. School mobile phones may be used for this purpose only in connection with making an official record of a recognised school activity.

13.5. No images of the children should be taken without parental consent. Devices must not be removed from the school premises if they contain images of pupils without permission.

13.6. Staff who choose to wear a smart watch must refrain from using watches for messages, calls and photographs.

13.7. Smart watches can be used to count steps only.

13.8. Smart watches with a camera function must be stored away as per mobile phones and accessed from lockers in the staff room only

13.9. Staff should be aware that mobile devices and smart watches connected to the internet may pose cybersecurity risks. Devices must not be used to access the school network or email without prior authorisation and appropriate security settings.

14. School Mobile Phones

14.1 Mobile phones are supplied to staff for work-related use only. Occasional and low-cost personal use will be tolerated only as and when related to work activity (for example, when working away from the school premises or outside of normal working hours in order to confirm safe arrival or notify delay etc).

14.2 A written record must be maintained of all school mobile phones issued to staff. This record should identify by name the staff member responsible for any individual identifiable device and should specify the time frame within which that individual holds responsibility.

14.3 Any discussions with senior staff in regard to mobile phone use (such as in an emergency) must be documented in writing as soon as possible and must be countersigned by both parties (i.e. the senior staff member and the individual responsible for the mobile phone at the time of the emergency).

14.4 Staff members are responsible at all times for the security of any school mobile phone issued to their care. The PIN code on the school mobile phone must be set on receipt and the device should never be left unattended or (especially in vehicles) on display.

14.5 All staff must be aware of the importance of ensuring appropriate confidentiality and security when using mobile phones in public places.

14.6 Any loss or theft of a school mobile phone must be reported immediately to the school office as the school remains responsible for all call costs until the phone is officially reported lost or stolen.

14.7 School SIM cards must only be used in mobile phones owned by and provided by the school for educational purposes.

14.8 No school mobile phone is permitted to be used to call (or send text messages to) premium rate numbers or numbers outside the UK unless this is in relation to official business (e.g. on a school trip).

14.9 No personal numbers of staff members or students, nor any text or other messaging or photographs are permitted to be stored on school mobiles.

14.10 Necessary contacts, tasks and calendars should be stored using 'exchange server' to ensure back up of all contacts and to maintain security levels for both school and user.

14.11 All users to whom a school mobile phone has been issued must ensure that they have read and understood the school's policy on staff use of mobile phones and must confirm, by signing the acceptance form, their agreement to abide by the terms of this policy.

14.12 Upon leaving the employment of the school, any staff member in possession of a school mobile phone must ensure that this device is returned to their manager.

14.13 All staff must ensure school mobile phones are not used in ways that expose the school to cybersecurity threats. This includes avoiding suspicious links in text messages, ensuring phones are updated with the latest security patches, and reporting any abnormal activity immediately.

15. Mobile phones and driving

15.1. The use of mobile phones (other than hands free) whilst driving a vehicle is illegal. Drivers should find a safe place to stop and turn off the engine before making or answering calls.

15.2. Staff must ensure that no sensitive school information (including emails or Class Dojo data) is accessed while driving, to prevent accidental exposure to cyber threats such as phishing or spoofing during distraction.

16. Accessing School emails and Class Dojo on personal devices (mobile phones)

16.1. At Ryhope Infant School Academy email is the main method of communication used to cascade messages to all staff. Not all staff have access to a laptop/ tablet or other device that is not a mobile phone. Therefore, staff can access their school emails using a personal mobile phone as long as the following is in place prior to setting up school email access on the device:

- The mobile phone has a personal password to be able to gain access and this is not shared with anyone else including those who live in the same household.
- No one other than the member of staff accesses the school mailbox or Dojo via the personal mobile phone.

- No school email is ever shared beyond the school mailbox e.g. forwarding it to a personal email address or discussing the content.
- The contents of an email or information on Dojo is kept completely confidential and remains in email form only, within the school-based mailbox or on the Dojo App.
- If the mobile phone was lost or stolen it is immediately reported to the network provider who will instantly block all access to the device and the sim card.
- Staff must ensure their mobile device has updated antivirus protection, and avoid clicking links or opening attachments from unknown senders, to prevent cyber-attacks such as malware or phishing from compromising school data.
- Any suspected unauthorised access or data breach involving personal devices must be reported immediately to the School Business Manager and Head Teacher.

17. Use of phones by pupils

17.1. There is no reason for children to bring mobile phones to school. If a child does bring a mobile phone to school it will be turned off and kept safe until the end of the day where it will be handed back to parent/carer.

17.2. This policy is also in place to reduce the risk of unauthorised access to the school network or social engineering cyber-attacks that could occur via pupil devices.

18. Use of phones by visitors/ students/ volunteers

18.1. Visitors are allocated a locker upon arrival. The same policy applies as it does to staff.

18.2. Visitors must not connect personal mobile devices to the school's Wi-Fi or systems unless authorised, as this can increase the risk of cyber-attacks or data breaches.

19. Use of phones by parents

19.1. Parents are advised to switch off mobile phones in the vicinity of school.

19.2. During individual class assemblies and year group or whole school performances a reminder of mobile phones to be switched off will be given. Parents are welcome to take a photograph of their own child at the end of the performance.

19.3. Parents must not use mobile devices to access school-related systems or attempt to connect to the school's digital infrastructure, as this could pose a cybersecurity risk.

20. Social Media

20.1. Parents, carers, staff, Trustees, visitors and pupils must all refrain from discussing the Academy, uploading photographs of or related to the Academy on personal social media websites (including Facebook, Instagram Twitter etc.).

20.2. Users must also be aware that malicious links and fake profiles on social media platforms can be used in cyber-attacks to gather sensitive school-related information or impersonate staff members. Any suspicious social media activity relating to the Academy must be reported immediately.

20.3. Supervision of Pupil Use

- Pupils must be supervised at all times when using school computer equipment. When arranging use of computer facilities for pupils, you must ensure adequate supervision is available.
- Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for pupils is enforced.
- Supervising staff must ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by pupils.
- Staff should also be aware of online threats such as cyber-attacks targeting young users, including harmful downloads or malicious pop-ups. Protective measures must be enforced at all times.

21. Reporting Problems with the Computer System

21.1. It is the job of the IT support (Omnicom) and the School Business Manager to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible.

21.2. You should report any problems that need attention to the School Business Manager.

21.3. If you suspect your computer has been affected by a virus or other malware, you must report this immediately.

21.4. If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the less chances of your data being recoverable.

21.5. Any suspected cyber-attacks, including phishing emails, unauthorised access, data breaches or ransomware activity must be reported immediately and will be investigated in collaboration with our ICT provider (Omnicom).

22. Reporting Breaches of this Policy

22.1. All members of staff have a duty to ensure this Acceptable Use Policy is followed. You must immediately inform the Head Teacher, of abuse of any part of the computer system. In particular, you should report:

- Any websites accessible from within school that you feel are unsuitable for staff or pupil consumption.
- Any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc.
- Any breaches, or attempted breaches, of computer security, or
- Any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the school computer system.
- All reports will be treated confidentially.
- Any signs of cyber-attack, including but not limited to unusual system behaviour, phishing attempts, spoofed email addresses, or unauthorised logins, must be reported immediately to IT support and the Head Teacher.

22.2. All staff should be fully aware that failure to comply with this policy is likely to result in disciplinary action. Additionally, in certain circumstances, failure to observe this policy may potentially lead to allegations of inappropriate behaviour likely to generate a child protection investigation. Such enquiries may lead to suspension from work (in accordance with the disciplinary policy) pending police enquiries.

22.3. Any proven incident of this nature involving a student is likely to be viewed as a serious disciplinary offence warranting sanction up to and including dismissal for gross misconduct.

22.4. Accordingly, this guidance should be viewed as a necessary safeguard for both staff and pupils, in addition to maintaining the valued reputation of the academy.

23. Electronic Devices - Searching & Deletion

23.1. In accordance to 'The Education Act 2012' school has the right to search and or delete anything from personal devices if they believe illegal or suspicious activity is taken place.

23.2. This includes instances where a personal device is suspected of being used to initiate or facilitate a cyber-attack on the school's systems.

24. Review and Evaluation

24.1. This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

24.2. Cyber threats are evolving constantly; therefore, the Acceptable Use Policy will be updated regularly to reflect best practice in cyber security and the latest guidance from the Department for Education and cybersecurity authorities.

24.3. Our Acceptable Use Policy (AUP) has been created by our Trustees and Senior Leadership Team in consultation with employees.

25. Other policies and procedures

25.1. This policy will be supported by the following policies and procedures:

- Staff Behaviour (Code of Conduct) Policy
- Disciplinary Policy
- Data Protection Policy
- Cyber Security Attack Policy
- Incident Response Plan (covering procedures for responding to cyber-attacks)

Acceptable Use Policy Agreement

This policy is designed to keep pupils, staff and the school safe when using technology.

The school owns the ICT network and devices. Staff can use them for work tasks like teaching, planning and admin. Occasionally, school mobile phones may be used for short personal calls when related to work.

The school may check or delete files, monitor internet use, and view online activity related to the school.

It may also investigate any suspected or actual cyber attacks on school systems or data.

All staff must follow this policy and sign below to confirm they understand and agree to it.

What I Agree To

1. Using School Systems Safely

- I will use school systems responsibly to keep myself and others safe.
- I know the school can monitor my use of the internet, emails and devices.
- I will not share my login details and will keep passwords secure.
- I will report anything suspicious, including strange emails or system issues, in case it is a cyber attack.
- I understand school technology is mainly for work use.

2. Professional Behaviour Online

- I will be polite and respectful in all digital communication.
- I won't access or change other people's files without permission.
- I won't take or share images of others without following school policy.
- I won't contact pupils or parents using personal accounts.
- I won't post anything online that could damage my reputation or the school's.

3. Personal Devices and Internet Use

- If I use my own phone or laptop for work, it must have a password and antivirus protection.
- I won't open suspicious links or attachments.
- I won't download anything illegal or harmful.
- I won't try to bypass filters or change system settings.
- I will help protect the school from cyber threats by using strong passwords and being careful online.

4. Data Protection

- I will follow data protection rules when handling personal or school information.
- I will only share data when it's allowed, and will keep it secure.
- If I lose data or see a data issue, I will report it straight away.
- I understand cyber attacks can lead to data breaches, and I have a role in preventing them.

5. Legal Use

- I will follow copyright rules.
- I won't download or share anything illegal.

6. Responsibility

- This policy applies both inside and outside of school.
- If I break these rules, I may face disciplinary action, and in serious cases, the police may be involved.

- I understand that being part of a cyber attack—even by accident—could have serious consequences.

Confirmation

I have read and understood this policy. I agree to follow it when using school systems or my own devices for school work.

Name: _____

Signature: _____

Date: _____

The school's Acceptable Usage Policy has been drawn up to protect all parties – the pupils, the staff and the school.

The ICT network and associated devices is owned by the school. It is made available to staff to enhance their professional activities including teaching, research, administration and management.

On occasion, school mobile phones are supplied to staff for work-related use only. Occasional and low-cost personal use will be tolerated only as and when related to work activity (for example, when working away from the school premises or outside of normal working hours in order to confirm safe arrival or notify delay etc).

The school reserves the right to examine or delete any files that may be held on its computer system or any other communication devices, to monitor any internet sites visited and the online public profiles of any staff member.
The school also reserves the right to investigate any suspected or actual cyber-attacks that may compromise the integrity, confidentiality, or availability of school systems, data or services.

It is a requirement of any position held within the school, to adhere to the Acceptable Usage Policy at all times. Staff must sign a copy of this Acceptable Use Agreement and return it to the Headteacher or School Business Manager, to indicate that the policy has been read and understood.

Agreement

I understand that I must use all school systems in a responsible way, to ensure that there is no risk to my safety or to the safety of others whilst also accepting my responsibility for ensuring the security of the systems. I recognise the value of the use of digital technology for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of digital technology. I will, whenever it is appropriate, educate children in the safe use of digital technology and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, internet, mobile phones etc) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my school username or password to anyone else, nor will I try to use any other person's username and password. I will update my password regularly as required by the Academy.
- I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate, or harmful material or incident that I become aware of to the appropriate person.
- I understand that I have a duty to remain vigilant against cyber-attacks such as phishing, spoofing, malware, and ransomware, and will report any suspicious emails, system behaviour, or security alerts immediately.

I will be professional in all my communications and actions when using digital technologies and communications systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will only communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so.
- I will only use social networking sites in school in accordance with the school's policy.
- I will only communicate with pupils, parents and carers using official school systems. Any such communication will be professional in tone and manner.
- I will not allow any current pupil to become a friend on my personal social media accounts.
- I will not give current pupils my personal mobile phone number.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will avoid sharing sensitive school-related information over unsecured platforms or social media, to reduce the risk of social engineering or cyber-based threats

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal devices (laptops / tablets/ mobile phones/ USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are password protected and protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses for correspondence on school matters.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs).
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Data Protection Policy (or other relevant school policy). Where digital personal data is transferred outside the secure school network, it must be securely encrypted or password protected. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that the Data Protection Policy requires that any staff or pupil data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will be proactive in preventing cyber-attacks by following best practices in cyber hygiene, including regular software updates, using strong passwords, and avoiding suspicious links or downloads.
- I understand that cyber-attacks may target both school systems and personal devices used for school business, and I have a responsibility to help prevent the spread of such threats.

When using the internet in my professional capacity or for school-sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, or I am unsure of the copyright status, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment and systems, but also applies to my use of digital technology equipment systems out of school that might affect my professional position and my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Trustees and in the event of illegal activities the involvement of the police.
- I understand that any involvement—intentional or accidental—in a cyber-attack or data breach could lead to investigation and, if necessary, disciplinary or legal action.

I have read and understand the above and agree to use school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Full Name: _____ Role: _____

Signed: _____ Date: _____

Access Approved: _____ Date: _____