RYHOPE INFANT SCHOOL ACADEMY

Learn to live

AGE 3-7

Care & Education

WORKING TOGETHER

Ryhope Infant School Academy

Acceptable Use Policy

Updated:	**February 2022**
Produced by:	**Mrs T Allen**
	Headteacher
Ratified by:	**Governing Body**
Signed:	S. Brown
	Chair of Governors
Review Date:	**February 2023**

Technology is key to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet is a powerful tools, which opens 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. Therefore all users have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That all adults will be responsible users and stay safe while using the internet and other electronic communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.
- That staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students' learning and will, in return, expect all adults to agree to be responsible users.

The purpose of the policy is to ensure the school network is operated safely and all users of ICT 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.

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.

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.

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

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

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.
- 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.

School ICT Network - Managing filtering

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

- The school monitoring and filtering system is provided by Omnicom
- The school will work with the Omnicom ICT support technicians to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the School Business Manager (SBM) and the Designated Safeguarding Lead (DSL).
- The SBM and the DSL will ensure that regular checks are made so that the filtering methods selected are appropriate, effective and reasonable.

Passwords

- 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.
- 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.
- **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.**
- 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.

Software and Downloads

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

Personal Use

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:

- Most comply with all other conditions of the AUP as they apply to non-personal use, and all other school policies regarding staff conduct.
- Must not interfere in any way with your other duties or those of any other member of staff.
- Must not have any undue effect on the performance of the computer system; and
- Must not be for any commercial purpose or gain unless explicitly authorised by the school.

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

Email

- 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.
- No member of staff (including governors) must use non-school email accounts for any school/work related activity – **no exceptions!**
- 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.
- 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.
- 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.
- All emails both sent and received will be scanned by forensic software.
- E-mail attachments should only be opened if the source is known and trusted.
- 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.
- 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.
- 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.
- Other users' files or folders should not be accessed without permission.

- 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 HT.
- 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).
- Any unsuitable communications received must be reported to a member of staff immediately.

Images/Videos

- All children need parental permission to have photographs or videos published electronically or in a public area even if they are unidentifiable.
- No photos or videos which include nudity or inappropriate actions are permitted to be taken or downloaded under any circumstance.

Network Protocol

- School computer and Internet use must be appropriate to a pupil's education or to staff professional activity.
- Respect other people’s material and do not corrupt, interfere with or destroy them.
- Do not open other people’s files without expressed permission.
- When working with personal data ensure that the data is secure.

Internet Usage

- Pupils **must be supervised at all times** when using the internet.
- 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.
- 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.
- 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.
- Use the internet for personal financial gain, gambling, political purposes or advertising is forbidden.
- 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.

Use of Social Networking Sites and Online Forums

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.

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.

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. 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.

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.

- Unless authorised to do so, you must not post comments on websites that may appear as if you are speaking for the school.
- You should not post any material online that can be clearly linked to the school that may damage the school’s reputation.
- 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.

Use of your own Equipment

- 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.
- 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.
- 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.

Mobile Devices including Smart Watches

- 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.
- 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.
- It is forbidden for photographs/videos of the children to be stored on personal mobile phones.
- No images of the children should be taken without parental consent and permission from a member of staff using any mobile device e.g. phones, school cameras. These devices must not be removed from the school premises if they contain images of pupils and without permission from a member of staff.
- Staff who choose to wear a smart watch must refrain from using watches for messages, calls and photographs.
- Smart watches can be used to count steps only.
- Smart watches with a camera function must be stored away as per mobile phones and accessed from lockers in the staff room only.

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

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.

Use of phones by pupils

- 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.

Use of phones by visitors/ students/ volunteers

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

Use of phones by parents

- Parents are advised to switch off mobiles phones in the vicinity of school.
- 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.

Social Media

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

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.

Reporting Problems with the Computer System

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.

- You should report any problems that need attention to the School Business Manager.
- If you suspect your computer has been affected by a virus or other malware, you must report this immediately.
- 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.

Reporting Breaches of this Policy

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.

Electronic Devices - Searching & Deletion

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.

Review and Evaluation

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.

Our Acceptable Use Policy (AUP) has been created by our school governors and senior managers and approved by the whole school community.

Acceptable Use Policy Agreement

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management.
The school's Acceptable Usage Policy has been drawn up to protect all parties – the pupils' the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited and the online public profiles of any staff member.

Staff should sign a copy of this Acceptable Use Agreement and return it to the Headteacher/School Business Manager for approval.

I understand that I must use all electronic communication systems in a responsible way, to ensure that there is no risk to my safety or to the safety of others. I also accept responsibility for the security of the school ICT systems. I recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will, whenever it is appropriate, educate children in the safe use of ICT 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 ICT systems (eg laptops, email, internet etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use.
- 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 will immediately report any illegal, inappropriate, or harmful material or incident that I become aware of to the appropriate person.

I will be professional in all my communications and actions when using electronic 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 avoid use of chat and social networking sites in school time.
- I will not allow any current pupil to become a friend on my personal Facebook account, or any similar social networking site.
- I will not give current pupils my personal mobile phone number.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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 hand held/external devices (PDAs/laptops/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.

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programs.
- 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 School Personal Data Policy (or other relevant school policy). Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student/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.

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 ICT equipment in school, but also applies to my use of ICT systems and equipment 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 Governors and in the event of illegal activities the involvement of the police.

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

Full Name: ________________________ Role: ____________________

Signed ___________________________ Date_____________________

Access Approved __________________ Date_____________________