THE RADCLIFFE SCHOOL
INSPIRE AND ACHIEVE

E-Safety and Acceptable Use of IT Policy

Headteacher:	P Lawson	Review frequency:	Five yearly
Chair of Governors:	P Critchley	Date reviewed:	July 2022

Contents

E-Safety

Introduction ……..……..……. 4

Managing Access and Security ……..……..…….. 4

Internet Use ……. ……..……... 4

E-Mail ……..……..…….. 4

Published Content ……..……. 5

Publishing Students' Images and Work ……..……. 5

Use of Social Media and Communication……..…….. 5

Instant Messaging ……..……..……. 5

Use of Personal Devices ……..……..…….. 5

Authorising Access ……..……..……. 6

Assessing Risks and Reporting ……..…… 6

Handling E-Safety Complaints ……..…….. 6

Acceptable Use Policy……..…. 6

Acceptable Use of ICT

Introduction ……..…… 7

Acceptable Use Policy Agreement …… 8

School Internet and E-mail Systems …… 9

Data Encryption, Data Security and Data Storage …… 11

Appropriate use of Social Networking/Media Sites and Online Safety …….. 13

Students …… 13

Staff …….. 14

Examining Electronic Devices …… 15

Appendix 1 – Acceptable Use Agreement Staff …… 16

Appendix 2 – Acceptable Use Agreement Students …… 18

Introduction

The e-safety policy covers the use of all technology which can access the school network and the internet, which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets, and one-to-one devices (school iPads).

The e-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff or student.

Managing Access and Security

The school will provide managed internet access to its staff and students in order to help students to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.

The school will ensure that its equipment has security software and virus protection. Access to school networks will be controlled by passwords.

Systems are in place to ensure that internet use can be monitored and logged so if there are any incidents the school can identify patterns of behaviour and to inform e-safety policy.

All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.

Internet Use

The school will provide an age-appropriate e-safety curriculum that teaches students how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.

All communication between staff and students or families will take place using school equipment and/or school accounts.

Students will be advised not to give out personal details or information which may identify them or their location.

E-Mail

Students and staff may only use approved email accounts on the school IT systems. Staff to student or staff to parent email communication must only take place via a school email

address. Group emails sent to parents must be sent using the school's email groups provided for this purpose.

Incoming email should be treated as suspicious and attachments not opened unless the author is known. Even if the author is known, any email attachments still may potentially be suspicious if its receipt was not expected. If in any doubt contact the IT department.

Published Content

The contact details for published content e.g. school web-site, or other internet presence will always be the school address, email and telephone number. Staff or students' personal information will never be published.

Publishing Students' Images and Work

Written permission will be obtained from parents or carers before photographs or names of students are published on the school web-site or any school run social media.

Use of Social Media and Communication

All communication must meet the expectations laid out within the school behaviour policy (Students and Parents) and the Staff Ethos Policy (Staff).

Staff and students should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.

School devices do not permit access to social networking sites.

Parents and carers should not allow access to social media sites to students which are not age appropriate e.g. below 13 (Facebook, Instagram, Snapchat) or 16 (Whatsapp).

Private instant messaging services must not be used. Only school approved platforms can be used and must be used for school work/business.

Only school conference video messaging services (such as Teams) can be used. In the event of the need to hold a one-to-one video call this must be approved by a member of the Senior Leadership Team and a risk assessment conducted.

Use of Personal Devices

Staff must not store images of students or student personal data on personal devices. The school cannot be held responsible for the loss or damage of any personal devices used in school.

Authorising Access

Students can only access the school network using a school device. The school have the right to withdraw access to the network as a result of breaches to the school behaviour policy or the E-Safety and Acceptable Use of IT Policy.

Assessing Risks and Reporting

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer or school device. The school cannot accept liability for any material accessed, or any consequences of internet access.

Staff, students and parents/carers have a responsibility to report any incidents of on-line abuse, harassment, bullying or cyber-crime.

Any such incident must be reported to their Safeguarding Leads for further action, and followed up by IT Support to ensure the risk is mitigated. Furthermore, all staff must contact their Safeguarding Leads where information from a child indicates the use of technology inappropriately, ie grooming, accessing age-inappropriate materials, or involved in possible radicalisation activities falling under our Prevent Duty. In all cases or if in any doubt, please contact the Designated Safeguarding Lead.

Handling E-Safety Complaints

Complaints of internet misuse will be dealt according to the school's Behaviour for Learning policy and Safeguarding Policies.

Complaints of a Safeguarding nature must be dealt with in accordance with the schools safeguarding and child protection procedures. In the first instance the Safeguarding Leads must be contacted.

Students and parents will be informed of consequences and sanctions for students misusing IT and this will be in line with the schools' behaviour policy.

Acceptable Use Policy

This E-Safety policy should be treated in conjunction with the Acceptable Use Policy and where applicable iPad User Agreement.

Students need to agree to comply with the student Acceptable Use Policies in order to maintain access to the school IT systems and to the internet. Students will be reminded about the contents of the Acceptable Use Policies as part of their e-safety education.

All school staff must sign and agree to comply with the staff Acceptable Use Policies in order to maintain access to the school IT systems and to the internet.

Acceptable Use of ICT

Introduction

Information and Communications Technology (ICT) plays a critical role in everyday life in the 21st century and is a powerful tool for enhancing teaching and learning. ICT related technologies detailed below are an expected part of our daily working life in school. The aim of this policy is to create an environment where all users have safe internet access and an awareness of how to keep safe when online and to explain how to report inappropriate use and content.

The school has developed a digital strategy that has five pillars:

Creativity:
Using technology to enhance the learning experience by providing memorable experiences that are exciting and engaging.

Collaboration:
Developing critical thinkers who are able to work efficiently together, receiving and acting on feedback any time or anywhere.

Communication:
Providing new avenues of communication inside and outside of the classroom, expanding horizons for all within a global economy.

Aspiration:
Promoting confident, aspirational learners with ambition and drive, future proofing their digital literacy.

Equity:
Ensuring access for all by meeting the needs of individual learners to address the demands for future employability.

The Radcliffe is aware of its responsibility to educate our students on E-Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

This policy is intended to address both school owned computer hardware in addition to the use of non-school owned electronic devices by students, staff, volunteers, governors and other visitors/guests at The Radcliffe School.

This Acceptable Use Policy is intended to ensure that:

- Any student, staff, volunteer, governor and visitor/guest user will be responsible users and stay safe while using the Internet, school network and other communication technologies for educational, personal and recreational use.
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and other users at risk.
- Users are protected from potential risk in the use of ICT in their everyday work.
- Clear guidance on how to minimise risks and how to deal with any infringements are provided.

Device Types: For the purpose of this acceptance policy, the word 'device' means a school-owned electronic piece of equipment that includes laptops, notebooks. and tablets. The word 'user' refers to any individual either connecting to the school hard wired network or wireless networks.

Both this policy and the Acceptable Use Agreement (for all staff and students) are inclusive of both fixed and mobile technologies provided by the school (such as PCs, laptops, tablets, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, tablets, mobile phones and other mobile devices).
.
The policy also links to the E-Safety, Data Protection, Anti-Bullying Policy, Disciplinary, Managing Underperformance, Student Behaviour for Learning Policy and the Staff Ethos Policy.

Acceptable Use Policy Agreement

All users should familiarise themselves and follow the guidance as outlined in the linked policies. All parts of this ICT Acceptable Use Policy and associated policies should be understood fully prior to acceptance and any questions that arise should be directed to the Designated Safeguarding Lead and IT Manager.

Students, staff and guest users should understand that they must use school ICT systems in a responsible way, to ensure that there is no risk to their safety or to the safety and security of the ICT systems and other users. They should recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. Staff will, where possible and if appropriate, educate the young people in their care in the safe use of ICT and embed online safety in their work with young people.

Whilst exciting and beneficial both in and beyond the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these technologies and that some have

minimum age requirements eg. Thirteen years for some social media platforms. All users are must read and sign this ICT Acceptable Use Policy.
.

In school, devices will gain access through the school's firewall, which is maintained by IT Support. Outside of school devices will be manged via a locally installed filtering solution. No firewall or internet filter is impenetrable, so all school users are expected to maintain a level of personal responsibility when using our system and any mobile technologies.

All users should be aware that compliance with this policy is mandatory.

School Internet and E-mail Systems

The Radcliffe School will provide a filtered educational internet and email service which is monitored and logged in school to reduce the risk of access to inappropriate material.

The School is not responsible for any content accessed by a user using their own devices through non-school controlled wireless or network systems, such as personal networks, 'Hotspots', Proxy or VPN bypass Systems.

Whilst the school takes reasonable and necessary precautions, including filtering and other security measures to help ensure a safe computing environment for students, staff or visitor/guest users, all users must be aware that some services available on the Internet may be offensive. Should access be gained to any inappropriate content all users must report this immediately to the IT department so that it can be blocked as soon as possible.

The Radcliffe School's e-mail and Internet facilities are provided to its users for school related teaching and learning or business purposes only. Any use of the systems for personal purposes is discouraged and must be limited ie. Use of the Internet must not interfere with a user's work commitments (or those of others). If it is discovered that personal usage has been excessive, disciplinary action may be taken and access to the facilities may be withdrawn without notice.

The following principles must be adhered to when representing the school either online or when using a school email account:

- Users are not permitted to enter into any contract or subscription on the internet on behalf of the school, without specific permission to do so.
- E-mail should be treated in the same way as any other form of written communication. Users should not include anything in an e-mail which is not appropriate to be published generally. They should exercise care when copying or forwarding e-mails as this may disclose sensitive or confidential information to the wrong person.
- Users should be aware that e-mails are disclosable as evidence in court proceedings and, even if they are deleted, a copy may exist on a back-up system or other storage area.
- An email message which is abusive, discriminatory on the grounds of sex, marital or civil partnership status, age, race, disability, sexual orientation including being or

becoming a transsexual person, pregnancy and maternity or religious belief (or otherwise contrary to our Equal Opportunities policy) or defamatory is not permitted.
- Statements criticising competitors, staff, students or parents and those stating problems with services, suppliers or customers should be avoided.
- Staff should also refer to guidance set out within Staff Ethos Policy and E-Safety Policy.
- The school can monitor users' Internet, email and network activity without consent.

Care should be taken when opening files or e-mail attachments received via the Internet or web-based email providers. If there is any doubt or concerns regarding the contents, then please delete the files. If you have any concerns, you should contact the IT Support as soon as possible. Information received from the Internet should not be uncompressed or executed unless the source is trusted. Under no circumstances should unsolicited data or files be opened, uncompressed or executed.

A school email address must not be used for any non-work/school related purpose or Personal Websites. School email addresses are issued to staff and students for school work/business only.

Set out below are examples of inappropriate use of the school's Internet and e-mail facilities, which are by no means exhaustive:

- Users must not use any software that supports the illegal or legal download of materials using the school's Internet
- Users should not try (unless they have permission) to make large downloads or uploads that might consume internet capacity and prevent other users from being able to carry out their work.
- The use of any 'Proxy' or 'VPN' avoidance/bypass sites/software/systems used to gain access to restricted sites
- The creation, downloading, storage, processing or transmission of any message, picture, video or graphical content that might constitute bullying
- The creation, downloading, storage, processing or transmission of any form of obscene, indecent or offensive material in any form.
- The unauthorised accessing, downloading or distribution of confidential information about other students, the school, its staff or their families.
- The accessing, downloading or distribution of copyright information and/or software including; illegal downloading and copying of games, music, movies and other protected works, in breach of the Copyright, Designs and Patents Act 1988.
- The use of the e-mail system for the purpose of 'spamming' (e.g. large scale distribution of unsolicited e-mail to other users, both internally or externally, sending or copying of chain letters, jokes, gossip, movies or cartoons).
- To intercept or view an e-mail message or attachments that was originally destined for someone else.
- The use of another e-mail account other than your own to impersonate another person in a malicious context irrespective of how the logon details to that account were obtained.
- If users open inappropriate material this must be reported immediately to the school's IT Support.

- Should users receive an e-mail that has been wrongly delivered to their e-mail address, they must notify the sender by re-directing the message to that person and then delete the original email.
- All access to the network in school will be supervised and available only to those who possess a valid network username and password. Users should be reminded of the need for password security and must use a strong password. Passwords will be reset every month.

It is recommended that users do not use their school network password for any external websites and services that are not synced and managed by IT support.

The following requirements must be adhered to at all times by all users:

- Never share or disclose details of the School's network or technical information including login information with any other person, either directly or indirectly. No user should impersonate another user by using their login information.
- Not write down or store a password where it is possible that someone may steal it.
- Personal devices must not be plugged into the school's local area wired network via an Ethernet cable.
- Resourced networked printers are in use at the school and printing is controlled, therefore users should only print materials they require in order to minimise waste.
- Physical vandalism is prohibited.
- Electronic vandalism is prohibited.

Licensing of software is for The Radcliffe School use only; and not the individual user (unless specifically instructed).

Users should not attempt to compromise the security of the school's network. Examples of this include, but are not limited to:

- Unauthorised access (hacking) into school technical hardware, ie. servers, network switches, printers.
- No staff or student should log onto the e-mail, Internet or school network systems and knowingly or negligently leave the workstation unattended for use by another person.

All users' network and school IT access will cease upon them leaving The Radcliffe School.

The Radcliffe School monitors with specialist software, user's network activity to reduce the risk of access to inappropriate material. Access to inappropriate material and non-compliance with this policy may result to further action in accordance with the school's Disciplinary and Managing Underperformance Policy for staff or the school's Behaviour for Learning Policy for students.

Data Encryption, Data Security and Data Storage

Staff and students are permitted and encouraged to store or save their data onto the school's secure central server, shared cloud storage area eg. Google drive, Office 365 or, where available, within their school provided cloud account.

Portable storage devices should be avoided. Personal or sensitive data should not be stored on these devices and should only be accessed via the school network.

All users must take all sensible measures to protect information including but not limited to the use of authenticated access to their own device (i.e. requiring a PIN, pattern or password to be entered to unlock the device).

Users should also ensure their device auto-locks if inactive for a period of time. The school reserves the right to remotely wipe school email stored on a device in the event of loss or theft.

Personal or sensitive information must not be downloaded or saved on a personal device unless approved by the Headteacher.

Any sensitive or personal data must be securely deleted when it is no longer required in accordance with the retention periods set out in the school's Data Protection Policy.

Users will not publish any documents containing personal data or critical information on externally accessible websites, unless remote (Internet) access to this data is configured to require user authentication.

The School takes its compliance with the General Data Protection Regulation (GDPR) seriously and aims at all times to keep personal data secure. It takes suitable measures to prevent unauthorised or unlawful processing of personal data and accidental loss or destruction of or damage to personal data.

All members of school staff are required to undertake GDPR training prior to accessing information and data stored on the school's systems and networks The training provided is designed to help staff understand key areas of compliance and also to provide evidence that staff have read and understood relevant policies and documents.

Regular monitoring checks will be undertaken to ensure compliance with the criteria set out above. All incidents resulting in a breach of these guidelines must be reported to the school's Data Protection Officer.

Staff will only transport, hold, disclose or share personal information about themselves or others, as outlined in the school's Data Protection Policy. Staff will not be permitted to remove or copy sensitive or personal digital data from school network unless the data storage device is encrypted and is transported securely for storage in a secure location.

Paper based protected and restricted data must be held in lockable storage. Staff must make sure they have a valid purpose to have any data in print and if data has been printed off it needs to be securely disposed of once it is no longer required. Staff must not leave personal data unattended.

Before taking any personal data (excluding student work) off-site staff must obtain permission from the Business Manager or Data Protection Officer and ensure that this has been recorded.

Wherever possible staff should use school-based programs to access and store information they need and should always ensure the ongoing confidentiality and integrity of any administrative and/or teaching and learning Management Information System and/or services that they use. Staff should not export any sensitive or confidential student/parent/ staff data into an Excel spreadsheet from any system and store this data on their home/public computer or device.

Staff should understand that General Data Protection Regulation Policy requires that any staff or student data to which they have access, will be kept private and confidential, except when it is deemed necessary that they are required by law or by school policy to disclose such information to an appropriate authority. Therefore staff should not send personal data unless legally required to do so. If unsure staff must seek further advice from the Business Manager or Data Protection Officer.

Any user that sends email attachments containing private, personal or sensitive data in accordance with a legal requirement must encrypt this via secure email or equivalent.
If staff are planning to purchase or use any online IT systems or services that store or process student or parent personal data they should in the first instance liaise with the Data Protection Officer so that a Data Protection Impact Assessment can be undertaken.

The IT Manager is responsible for ensuring that personal data stored on school systems regarding staff, students and parents is appropriately restricted and only accessible to designated individuals. Staff are strictly prohibited from storing student or parent data on their own personal devices. Staff are therefore expected to act responsibly if using their personal mobile device for school business.

Appropriate use of Social Networking/Media Sites and Online Safety

Social media is a fun part of everyday life, but it can carry risks. The following guidance is intended to ensure students and staff stay safe while still making best use of social media for teaching/learning and research as well as social purposes.

A social networking site is any website which enables its users to create profiles, form relationships and share information with other users. It also includes sites which have online discussion forums, chat-rooms, media posting sites, blogs and any other social space online. They include, but is not limited to sites such as Facebook, Instagram, Pinterest, Snapchat etc.

Students

- In line with the E-Safety policy students should not be using age-inappropriate Social Media sites or Apps.
- Students should familiarise themselves and follow the guidance as outlined in the E-Safety Policy.

- Students must not use any social network site to attack, abuse or bully any school staff, other students or any other members of the school community or the public.
- The privacy and the feelings of others should be respected at all times.
- Students may be required to remove posts which are deemed to constitute a breach of this policy.
- Students must not include personal information or contact details of other students or staff.
- Pictures must only be posted with consent of the subject(s) or parents/carers of minors. For the purposes of this agreement minors are any student under the age of 18.
- Any content that students post about themselves or others could be brought to the attention of the school, future employers or professional bodies and may be detrimental to your studies and/or future career.
- Students should never reveal confidential information about the school or its staff or students. This might include aspects of school policy or details of either internal or private discussions. Please consult with your Form Tutor if you are unclear about what might be confidential.
- Students should take effective precautions when using social networking sites to ensure their own personal safety and to protect against identity theft.
- Students need to be aware that most students are minors (under the age of 18 years of age) and that any interactions with them should not only be approached with some caution, but also that the content of conversations/responses is suitable for members of this age group.
- Students need to consider intellectual property rights, copyright and ownership of data when using social media.
- Individuals should exercise caution when interacting with, and responding to, potentially contentious posts on social media sites. Any interacting, such as sharing, liking or commenting may be subject to the school's Behaviour Policy.
- Students are strongly advised to follow Childnet's SMART rules when using Social media sites:
  - Safe. Keep safe by being careful not to give out personal information - such as your name, email, phone number, home address, or school name - to people who you don't know or trust online.
  - Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.
  - Accepting emails, instant messages, opening files, pictures or texts from people you don't know or trust can lead to problems - they may contain viruses or nasty messages.
  - Reliable. Someone online may be lying about who they are, and information you find on the Internet may not be reliable.
  - Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried.

Staff

- Staff should familiarise themselves and follow the guidance as outlined in the staff Code of Conduct and E-Safety Policy.

• Staff must communicate with others in a professional manner, and not use aggressive or inappropriate language appreciating that others may have different opinions. Staff will only communicate with staff, students and parents/carers using official school systems.
• Staff will not use their personal equipment to record and upload images of students or other members of staff without consent of the Headteacher.
• Where these images are published it will not be possible to identify by name, or other personal information, those who are featured, unless in agreement with the subject and parent/carer (where applicable).
• Staff must only use chat and social networking sites in school in accordance with the school's policies.
• Staff must not engage in any on-line activity that may compromise their professional responsibilities.

Examining Electronic Devices

School staff have the specific power to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

• Cause harm, and/or
• Disrupt teaching, and/or
• Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

• Delete that material, or
• Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
• Report it to the Police

Any searching of students will be carried out in line with the Department for Education's latest guidance on screening, searching and confiscation.

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

Appendix 1
Acceptable Use Agreement Staff

This agreement has been written in line with guidance and is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are required to agree to abide by this agreement and the Acceptable use of ICT. Staff must sign a copy of this agreement. Any concerns or questions arising from the policy should be addressed to the school's Online Safety Lead.

Safeguarding the facilities and supporting student behaviour

I am aware that:

- When unattended all computers including desktops, laptops, tablets etc must be logged off or screen locked. This is equally applicable in classrooms, curriculum areas and offices.
- All computers and other associated equipment should be shut down at the end of the school day.
- Upon discovery, all damage must be reported immediately to IT Support.
- Students must always be supervised in ICT suites and in classrooms where computers are in use.
- Seating plans must be used to ensure that any subsequent damage can be tracked to individual students.
- Ceiling projectors or displays must be turned off by remote control when they are not in use.
- Food and drink should not be consumed in ICT suites or classrooms where IT is in use.

Staff Responsibilities and Expectations

I appreciate that ICT includes a wide range of systems including mobile phones, tablets, digital cameras, e-mail, social networking sites. I understand that I should only use my school email address for school business. School email addresses should not be used to 'sign-up' or 'register' any services not relating to school. I will comply with the ICT system security and will not disclose any passwords provided to me by the school or other related authorities. Passwords can however, be given to IT staff if requested, but it is advised to reset them afterwards. Passwords should not be written down. I understand that I am responsible for all activity carried out under my username. I will ensure that school data including data relating to students and staff, for example data from SIMS, is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.

- I will not install any hardware or software without the permission of the IT Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. I am aware that the school's system will detect any foul language, inappropriate phrases or indecent images.
- I understand that all my use of the Internet, including email and other related technologies, can be monitored and logged and a record can be made available on request to the Headteacher.
- I will respect copyright and intellectual property rights.

• I understand that images of students will only be taken with school cameras and other devices, stored safely on the school's network and only used in external publications with the permission of parents/carers.
• I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
• I understand that I am required to make any social networking sites e.g. Facebook non-public. As 'profile' pictures are also public, I am aware that I must maintain an image that is suitable for students to see or hide them completely.
• I understand that I must not communicate with students on social networking sites unless it is an authorised and permitted platform designated by the school. No 'friending', 'linking', 'liking', 'joining' or 'following' must take place until a student is over 18 and no longer on roll as a student. To maintain a professional boundary, it is strongly advised that staff should not 'friend', 'link', 'like', 'join' or 'follow' students or ex students until they are over 21. Until this point any communication should be through your school email account.
• I will ensure that all of my privacy settings are such that students and other users cannot access my personal information and posts.
• I will ensure that all electronic communications with parents, students and staff, are compatible with my professional role and in line with the Staff Ethos policy.

Safeguarding the welfare of students

• I will support the school's Child Protection and E Safety policies and help students to be safe and responsible in their use of ICT and related technologies.
• I will report any incidents of concern to the Online Safety Lead and Designated Safeguarding Lead or, in their absence, to the Headteacher.

Handling complaints

• I understand that staff misuse will be referred to the Headteacher and will be managed through the school's Disciplinary policies.

Activity which might be deemed to be criminal may be referred to the Local Authority Designated Officer (LADO) or the Police.

I understand the expectations and responsibilities as described in the Acceptable Use of ICT policy (Staff).

I agree to comply with these expectations and support the safe use of ICT throughout the school.

Full Name: ……
(Printed)

Job Title: ……..

Signature: …… Date: ……

Appendix 2
Acceptable Use Agreement Students

Supervision

The school reserves the right to monitor the use of its devices, systems, communications and all material held on the school network including e-mails at any time.

Using Devices

▪ You must abide by the E-safety policy at all times.
• You may only use school devices for educational purposes and not for personal use e.g. social media, internet browsing.
▪ You must be supervised at all times when using school devices, including outside of lesson times when a member of staff must be in the room with you.
▪ Do not change any settings on the computers, devices, systems and services, move cables or attempt to fix hardware.
▪ You must not access, remove, distribute or copy others' work, property or files without the owner's knowledge and permission and must only do so in accordance with school policies, eg. You must not copy and submit another student's homework or coursework.

Using your own Device

▪ You must not connect any devices to any school device or system.

Passwords

▪ Make sure your password is not easy to guess (eg. use a mixture of numbers and upper and lower case) and never reveal it to anyone.
▪ Keep your password safe and do not write it down or store it where someone can steal it. If you think someone else has been using your password, report it to a member of staff immediately.
▪ You must never use someone else's user name and password.

Using the Internet and E-mail

▪ Never reveal your name or any personal information about yourself or others, including students and staff when online. This includes names, address, email addresses, telephone numbers, age, gender, educational details, financial details etc.
▪ If a stranger contacts you when online, or you receive any inappropriate material or messages that make you feel uncomfortable tell a member of staff immediately. DO NOT REPLY.
▪ You must not open any hyperlinks in emails or email attachments unless you trust the person or organisation that sent it and they are known to you.
▪ Always be polite and responsible when communicating with others. Do not use offensive language in emails or write about other people.
▪ Do not download files unless approved by a member of staff.

Links to Behaviour Policy

▪ Failing to comply with the rules set out in this policy will be dealt with in accordance with the school's behaviour policy and serious incidents will be reported to the police.

Amendments

Date	Page	Item	Detail
July 2022			Amended to account for one-to-one devices (I Pads). All amendments highlighted.