Barnwell School
ICT Acceptable Use Policy

Reviewed – May 2024

To be reviewed – May 2026

ICT ACCEPTABLE USE POLICY

1. Policy statement and objectives

1.1 Information and communications technology (ICT) is an integral part of the way Barnwell School works, and is a critical resource for students, staff (including senior leadership teams), governors, volunteers, and visitors. ICT supports teaching and learning, pastoral, and administrative functions of the school.

1.2 However, the ICT resources and facilities we use in school and remotely can also pose risks to data protection, online safety and safeguarding. This policy aims to:

1.2.1 Set guidelines and rules on the use of school ICT resources for staff, students, parents, and governors

1.2.2 Establish clear expectations for the way all members of the school community engage with each other online

1.2.3 Support the school's policy on data protection, online safety, and safeguarding

1.2.4 Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems

1.2.5 Support the school in teaching students safe and effective internet and ICT use

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

1.4 This ICT Acceptable Use Policy should be read in conjunction with Barnwell School's Data Security Policy and Data Protection Policy.

1.5 Breaches of this policy may be dealt with under our school's disciplinary policy, climate for learning policy and staff code of conduct.

2. Relevant legislation and guidance

2.1 This policy refers to, and complies with, the following legislation and guidance:

Data Protection Act 2018

The General Data Protection Regulation

Computer Misuse Act 1990

Human Rights Act 1998

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Education Act 2011

Freedom of Information Act 2000

The Education and Inspections Act 2006

Keeping Children safe in education 2024

Searching, screening and confiscation: advice for schools

National Cyber Security Centre (NCSC)

Education and Training (Welfare of Children Act) 2021

3. Definitions

3.1 **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service

3.2 **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors

3.3 **"Personal use":** any use or activity not directly related to the users' employment, study or purpose

3.4 **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities

3.5 **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

4. Unacceptable use

4.1 The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings.

4.2 Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination

- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its students, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications, or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting, or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school

- Using websites or mechanisms to bypass the school's filtering mechanisms

- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic, or discriminatory in any other way

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

4.4 Exceptions from unacceptable use: Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion. Contact the school's Network Support in the first instance who will seek approval from the Headteacher.

4.5 Sanctions: Students or staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's disciplinary policy, behaviour policies and staff code of conduct.

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

5.1 Access to school ICT facilities and materials

5.1.1 The school's Network Manager manages access to the school's ICT facilities and materials for school staff. These include, but are not limited to:

- Computers, tablets, mobile phones and other devices

- Access permissions for certain programmes or files

5.1.2 Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

5.1.3 Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Network Support who will adhere to the network policies or seek approval as required.

5.2 Use of email

5.2.1 The school provides each member of staff with an email address. This email account should be used for work purposes only and users must adhere to the school's Data Security Policy.

5.2.2 If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential

information, the user must not make use of that information or disclose that information.

5.2.3 If staff send an email in error that contains the personal or sensitive information of another person, they must inform the Network Manager immediately and follow our data breach procedure.

5.3 Use of phones services

5.3.1 Staff must not give their personal phone numbers to parents or students. Staff should use phones provided by the school to conduct all work-related business.

5.3.2 You may make or receive personal telephone calls provided:

- They are infrequent, kept as brief as possible and do not cause annoyance to others
- They are not for profit or to premium rate services
- They conform to this and other relevant HCC and school policies.

5.3.3 School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused.

5.3.4 Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.

5.4 Use of Mobile phones

5.4.1 Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

5.4.2 There is a school mobile phone for the purposes of school trips only. The trip organizer or other appropriate adult is responsible for the security of the school mobile phone. Do not leave it unattended and on display (especially in vehicles).

5.4.3 Report the loss or theft of any school mobile phone equipment immediately.

5.4.4 The school remains responsible for all call costs until the phone is reported lost or stolen.

5.4.5 You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it.

5.4.6 School SIM cards must only be used in school provided mobile phones.

5.4.7 All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default.

5.4.8 Staff must not send text messages to premium rate services.

5.4.9 Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so.

5.5 Personal devices in school

5.5.1 The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school.

5.5.2 Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

5.6 Social Media, including Facebook and Twitter

5.6.1 Barnwell School uses Facebook and Twitter to communicate with parents and carers. The school manages postings on these technologies and closely monitors responses and postings from others.

5.6.2 Staff are not permitted to access their personal social media accounts using school ICT. Social media accounts can be accessed on a member of staffs own personal device and only if not interfering with their work and as an exception rather than the norm.

5.6.3 Staff are able to setup Social Learning Platform accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of Social Media.

5.6.4 Students are not permitted to access their social media accounts whilst at school.

5.6.5 Staff, governors, students, parents, and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.

5.6.6 Staff, governors, students, parents, and carers are aware that the information, comments, images and videos they post online can be viewed by others, copied and stay online forever.

5.6.7 Staff, governors, students, parents, and carers are aware that their online behaviour should at all times be compatible with UK law.

5.6.8 Staff should take care to follow the school's guidelines on social media contained in the Staff Code of Conduct and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.7 Personal social media accounts

5.7.1 Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times. Please refer to the schools policy on Code of Conduct for Employees.

5.8 Remote access and Cloud Services

5.8.1 Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the Network Manager may require from time to time against importing viruses or compromising system security.

5.8.2 Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy and Data Security Policy.

5.9 Monitoring of school network and use of ICT facilities

5.9.1 The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

5.9.2 Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The school monitors ICT use in order to:

- Ensure e-Safety and Safeguarding.
- Ensure Data Protection and Data Security
- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation

- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

Staff will be expected to sign an ICT Acceptable Use Agreement. Please see appendix one.

6. Students

Student access to ICT facilities:

- Computers and equipment in the school's ICT suite are available to students only under the supervision of staff.
- Laptops/Tablets and equipment in classes, and using the school's WIFI, are available to students only under the supervision of staff.
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff.
- Students will be provided 0365 account and other Cloud Apps accounts that the school subscribes to, which they can access from any device at school or on own device at home.

6.1 Search and deletion

6.1.1 Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search students' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

6.1.2 The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

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

6.2 Unacceptable use of ICT and the internet outside of school

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

- Using ICT or the internet to breach intellectual property rights or copyright

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation

6.3 Use of mobile phones and own devices

6.3.1 Mobile phones/devices are banned items. If pupils choose to bring their mobile phone to school, it must be turned off and handed in to their form tutor at the start of the day. Under no circumstance should students use their personal mobile devices/phones to take images or make recordings of any other student or any member of staff.

6.3.2 The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school and devices should have suitable insurance in place.

6.3.3 Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

7. Parents

7.1 Access to ICT facilities and materials

7.1.1 Parents do not have access to the school's ICT facilities as a matter of course.

7.1.2 However, parents working for, or with the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access or be permitted to use the school's facilities at the headteacher's discretion. Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the school online

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

7.2.2 Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to discuss and sign the Student ICT Acceptable Use Agreement, along with their child. Please see appendix one.

8. Data security

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

8.2 Passwords: All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Please refer to the schools Data Protection and security policies on Passwords.

8.3 Software updates, firewalls and anti-virus software: All of the school's ICT devices that support software updates, security updates and anti-virus products will be configured to perform such updates regularly or automatically. Users must not circumvent or make any attempt to circumvent the administrative, physical, and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities. Any personal devices using the school's network must all be configured in this way.

9. Data protection

All personal data must be processed and stored in line with data protection regulations and the school's Data Protection and Security policies.

9.1 Access to facilities and materials

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

9.1.2 Users should not access, or attempt to access, systems, files, or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert Network immediately.

9.1.3 Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out at the end of each working day.

9.2 Encryption

The school ensures that its devices and systems have an appropriate level of encryption. Refer to the Data Protection and Security policies on Encryption.

9.3 Protection from cyber attacks

For protection refer to the Data Protection and Data Security policies. Be suspicious of e-mails, especially from unknown senders and with email attachments. Do not open any suspicious e-mail attachments and report to Network Support to investigate.

10. Internet access

10.1 The school internet connection is secured both for a pc LAN connection and the school's WIFI connection.

10.2 User based filtering is set at different levels for students and staff, whereby students have more restricted access. These filters are based on the recommendations of our broadband supplier for schools that meet government guidelines.

10.3 Filters are not fool prove so staff should report inappropriate sites that haven't been picked up to Network Support who will add to the list of banned items.

10.4 Staff, and 6th form students can have access to the school WIFI using their own devices and all other pupils, using school set devices only.

10.5 Parents and visitors to the school will not be permitted to use the school's WIFI unless authorisation is granted by the Headteacher. Requests to access the WIFI can be made to Network Support.

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

11. Storage of Images

11.1 Photographs and videos provide valuable evidence of students' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

11.2 Photographs and images of students are only stored on the school's agreed secure networks which include some cloud-based services. Rights of access to stored images are restricted to approved staff as determined by Headteacher. Staff and students may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

11.3 Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

11.4 Staff and other professionals working with students, must only use school equipment to record images of students whether on or off site. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

12. E-Safety

12.1 Responsibilities

The headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety leads in this school are Assistant Head Teachers responsible for e-Safety – Martyn Patching and Cary Francis .

All breaches of this policy must be reported to Assistant Headteacher and will be investigated, where appropriate, in liaison with the police.

All breaches of this policy that may have put a child at risk must also be reported to a DSP.

Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when students are on site in the care of the school, then the safeguarding of students is paramount, and

the organisation must adhere to the school's online safety procedures and acceptable use agreements.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by Headteacher.

The school also works with partners and other providers to ensure that students who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following school policies and documents: safeguarding, Keeping Children Safe in Education, GDPR, Health and Safety, Home–School agreement, home learning, behaviour, anti-bullying and PSHCE/RSE policies.

12.2 Curriculum

Online safety is fully embedded within our curriculum. The school provides a comprehensive age-appropriate curriculum for online safety which enables students to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHE curriculum, Relationships and Health Curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for students to develop skills of critical awareness, digital resilience, and good online citizenship to enable them to use the internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic, and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g., regulated screen time and diverse online activity.

- Learning how to develop a positive online reputation and enhance future opportunities e.g., in relationships and employment.

- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content, e.g.,

recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online, (i.e. users may not be who they say they are and may have ulterior motives). Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online.

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others.

- Understanding the permanency of all online postings and conversations

- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.

- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

- How the law can help protect against online risks and abuse.

Appendix 1: Acceptable Use Agreements

Acceptable Use Agreement: Students – Secondary

Student Acceptable Use Agreement / e-Safety Rules

- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc, for school purposes.
- I will not download or install software on school technologies.
- I will only log onto the school network with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school email address whilst in school for school purposes.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the school network/internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher.
- I will ensure that any removable media I use at school will not contain any material that could be considered offensive or illegal and I understand the media can be subject to school security checks.
- I will not give out any personal information such as name, phone number, address, interests, schools or clubs or any personal image. I will not arrange to meet someone unless this is part of a school project approved by my teacher or if outside school, parent/carer.
- Images of students and/or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring into disrepute.
- I will support the school approach to online safety and not deliberately upload or add images, video, sounds or text that could upset or offend any member of the school community.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I will only store files on the school network that are for my studies/subjects at school
- I will use the school network responsibility as instructed by my teachers
- I understand that everything I search for, access, post or receive online can be traced now and in the future. My activity can be monitored and logged and if necessary shared with teachers, parents/carers and then police if necessary. I know it is essential that I build a good online reputation.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.
- I should never post photographs, videos or livestream without permission of all parties involved.
- I will not upload images, videos, sounds or words that could upset, now or in the future, any member of the school community, as this is cyberbullying.
- I will be respectful to everyone online and will not cause distress to anyone in the school community or bring the school into disrepute.
- I will report hurtful behaviour online and have the right to block and say no to any inappropriate or upsetting request.

- I will not lie about my agree in order to sign up for age-inappropriate games, apps or social networks.
- I understand that not everything I see or hear online is true, accurate and genuine and that some people of the internet and not who they say they are. I will gain permission from parents/carers before arranging to meet someone I only know on the internet.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied, and my parent/carer may be contacted. If I break the law the police may be informed.

Dear Parent/Carer

ICT including the internet, email and mobile technologies have become an important part of learning in our school. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of e-Safety and know how to stay safe when using any ICT.

Students are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or the school e-Safety coordinator.

Please return the bottom section of this form to school for inclusion in your child's records.

Student and Parent/Carer Acceptable Use Agreement and eSafety Rules

We have discussed this document and …… (student

name) agrees to follow the e-Safety rules and to support the safe and

responsible use of ICT at Barnwell School.

Parent/carer signature…….

Student signature……

Form…….. Date……..

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. The policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with school e-Safety coordinator.

- I will only use the school's email/Internet/Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address to students.
- I will only use the approved, secure email system for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without permission of the Network Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will ensure that any removable media I use at school will not contain any material that could be considered offensive or illegal and I understand the media can be subject to school security checks.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help students to be safe and responsible in their use of ICT and related technologies.
- I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers of pupils on social networks. I will also ensure my private account will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privilege information must remain confidential. I will not upload any material about or reference the school or its community on my personal social network.
- I will follow the data protection outlined in GDPR policy. These include photographs, personal data and personal and sensitive data.
- I understand that as a member of staff I should at no time put myself in a position where safeguarding allegations can be made against me as a result of my personal device or personal

accounts. I understand that the use oof personal devices in school is at the discretion of the headteacher.
- I understand that this forms part of the terms and conditions set out in my contract of employment.

User signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature……. Date……..

Third Party IT Acceptable Use Agreement / Code of Conduct

There are times when third parties (e.g., lettings, visitors) request the use of a limit user network account to access the internet only or the use of the school's Guest WIFI.

When such an account has been granted the following policy is applied:

- The account's permitted use is for a limited period only.
- The school's internet and related technologies are for professional purposes only and agreed in advance with the Network Manager before the account is assigned.
- The account cannot be used for the conduct of any personal business.
- The account and password cannot be passed on.
- It is prohibited to install any hardware or software on any school device.
- It is prohibited to browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory and subject to the computer misuse act and data protection act.
- Be aware that the use of the internet and other related technologies are monitored and logged and will be made available to relevant personal within the school and to the guest's own organisation they are representing.

User signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature……. Date……..