Use of technology: Acceptable Use (staff & students), Computer Security, Cyberbullying and Code of Practice Policy.

The King's School
Cadhay Lane
Ottery-St-Mary
Devon
EX11 1RA

Policy Change Control

Policy Owner	DHT Curriculum
Approved By	Resources Committee
Date of Last Approval	17/06/2021
Next Revision Due	June 2024

Date	Version	Person	Change / Action
30/01/2014	1.0	Trustees	Adoption of Policy
02/05/2017	1.1	LOE	Update to Template and Format
19/09/2017	1.2	DGW	No changes
26/09/2017	1.2	Trustees	Presented to Trustees for Approval
03/03/2021	2.0	DGW	Policy rewritten & name change to reflect new focus.
17/06/2021	2.1	Trustees	Approval

1.0 Policies

This policy should be read in conjunction with the following:

- Data Protection Policy.
- Privacy Notice Policy.
- Curriculum, Assessment and Reporting, Homework, Literacy and Numeracy Policy.
- Safeguarding and child protection policy.

2.0 Use of new technology

2.1 Introduction

New technology, whether hardware or software, can play a key role in ensuring effectiveness and efficiency across the organisation be it teaching or non-teaching.

When used correctly it can have a transformative effect in improving efficiency, reducing workload and improving the core business of the organisation: teaching and learning. This can help engage students and parents and provide support for staff in delivering highly effective lessons.

The effective use of new technologies will be driven by teaching and learning and our whole school curriculum intent rather than a specific technology: the technology is not an end in itself. Any use of new technology therefore needs a clear analysis of how it will improve teaching and learning interactions.

Both teaching and non-teaching staff need time to learn to use new technology effectively. This involves more than just learning how to use the hardware and software; training should also support teachers to understand how it can be used for learning.

Students' motivation to use technology does not always translate into more effective learning, particularly if the use of the technology and the desired learning outcomes are not closely aligned.

2.2 Criteria

The King's School will apply the following criteria when analysing the possible procurement of new technology. This includes, but is not limited to the following:

- To deliver the curriculum effectively and efficiently.
- To ensure teaching and learning is delivered effectively.
- To improve student attainment and progress.
- To deliver personalised education and support.
- To promote independent learning and research skills amongst students.
- To ensure value for money.
- To ensure compliance with the School IT network and infrastructure.
- To support Schools and staff diagnose their development needs and to support more flexible CPD.
- To ensure compliance with GDPR, safeguarding, data protection and key statutory legislation.
- To support and improve communication.
- To improve parental and student engagement.
- To reduce workload.

3.0 Computer Security/SIMS User Policy

3.1 Introduction

The School has a one network system meaning all staff have access to the SIMS data base. Some staff will be familiar with SIMS and some will need training to access the information they need. The School Network and SIMS hold a substantial amount of confidential and, sometimes, sensitive data about students and, in some programmes, staff information (access to SIMS is not open access).

3.2 Objective

To keep this information secure and confidential and to maintain our legal obligations under the Data Protection Act, we must have in place a clear policy to which all staff users must sign. The security of The School Network and SIMS relies on three main aspects: "clear desks", passwords and public\shared folders.

3.3 Policy

The purpose of this policy is to ensure access to the School's confidential information is limited only to those who need it.

Clear Desks

- If a computer is to be left unattended especially when SIMS is not closed, then it **MUST** be left locked.
- Computers must never be open with SIMS running in a place where students can view the screen.

Passwords

- Passwords **MUST** be at least 8 characters long.
- Users **MUST** change their password in the first week of every half term.
- Password should follow the three of four rule: lowercase; caps; numbers; special characters.

Public/Shared folders

- Files which students must not access must not be placed in the U:\ Drive (this includes student photos).
- Files which are inappropriate for all staff must only be stored in the in the H:\ drive or an access restricted folder/drive.
- Files which are not suitable to be viewed by students must not be kept on any computers C:\ drive.

3.4 Supporting framework

In order to achieve this, every member of staff must read and agree to the Computer Security/SIMS User Policy: Staff (see Appendix 3). The network is set up to enforce a password reset every three months.

3.5 Responsibilities

The School's Head Teacher has direct responsibility for maintaining this policy and providing advice and guidance on its implementation.

All staff are responsible for policy implementation and for ensuring that the staff they manage also adhere to the standards.

3.6 Implementation

This policy will be made available to all students, parents, carers, staff (whether permanent or temporary) and Trustees.

4.0 Cyber Bullying

4.1 What is cyberbullying?

"Cyberbullying is an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly over time against a victim who cannot easily defend him or herself."
Seven categories of cyberbullying have been identified:

- Text message bullying involves sending unwelcome texts that are threatening or cause discomfort.
- Picture/video-clip bullying via mobile phone cameras is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people.
- Phone call bullying via mobile phone uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified.
- Email bullying uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
- Chat room bullying involves sending menacing or upsetting responses to children or young people when they are in a web-based chat room.
- Bullying through instant messaging (IM) is an Internet-based form of bullying where children and young people are sent unpleasant messages as they conduct real-time conversations online.
- Bullying via websites includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyberbullying.

4.2 What can Schools do about it?

While other forms of bullying remain prevalent, cyberbullying is already a significant issue for many young people. The King's School recognise that staff, parents and young people need to work together to prevent this and to tackle it whenever it occurs.

School Trustees, Head teachers and schools have a duty to ensure that: bullying via mobile phone or the internet is included in their mandatory anti-bullying policies, that these policies are regularly updated, and that teachers have sufficient knowledge to deal with cyberbullying in School.

The King's School ensures that:

- the curriculum teaches students about the risks of new communications technologies, the consequences of their misuse, and how to use them safely including personal rights.
- all e-communications used on the School site or as part of School activities off-site are monitored.
- clear policies are set about the use of mobile phones at School and at other times when young people are under the School's authority. No mobile phones with cameras will be seen or heard on the School site. If a phone is seen or heard it will be confiscated and locked in the School safe until parents are able to collect it.
- Internet blocking technologies are continually updated and harmful sites blocked.
- students and parents are kept informed so as to ensure that new communications technologies are used safely, taking account of local and national guidance and good practice.
- security systems are in place to prevent images and information about students and staff being accessed improperly from outside School.
- other partners (police etc.) are involved in managing cyberbullying.

- a record of the incident will be kept.

4.3 ICT and Mobile Phone Policy

If a cyberbullying incident directed at a child occurs using e-mail or mobile phone technology, either inside or outside School time, The King's School will take the following steps:

- Advise the child not to respond to the message.
- Refer to relevant policies, e.g. e-safety/student acceptable use, anti-bullying and PSHE and apply appropriate sanctions.
- Secure and preserve any evidence.
- Inform the sender's e-mail service provider.
- Notify parents of the children involved.
- Consider delivering a parent workshop for the School community.
- Consider informing the police depending on the severity or repetitious nature of the offence. The School recognises that some cyberbullying activities could be a criminal offence under a range of different laws including: the Protection from Harassment Act 1997; the Malicious Communication Act 1988; section 127 of the Communications Act 2003 and the Public Order Act 1986.

If malicious or threatening comments are posted on an Internet site or Social Networking Site about a student or member of staff, The King's School will also:

- Inform and request that the comments be removed if the site is administered externally.
- Secure and preserve any evidence.
- Send all the evidence to www.ceop.gov.uk/contact_us.html.
- Endeavour to trace the origin and inform the police as appropriate.

4.4 Working with Parents

The King's School has developed a home-School agreement that includes clear statements about e-communications. The School seeks to regularly update parents on:

- What to do if problems arise.
- E-communication standards and practices in School.
- What's being taught in the curriculum.
- Supporting parents and students if cyberbullying occurs by:
    - Assessing the harm done.
    - Identifying those involved.
    - Taking steps to repair harm and to prevent recurrence.

4.5 Code of Conduct

The King's School has developed a code of conduct with our students. This is available in all IT classrooms:

CODE OF CONDUCT

- Always respect others - be careful what you say online and what images you send
- THINK before you send. Whatever you send could be made public very quickly and could stay online forever
- Treat your password like your toothbrush – keep it to yourself. Only give your mobile phone number or personal website address to trusted friends
- Serious bullying should be reported to the police – for example threats of a physical or sexual nature

- If you can, make a note of the time and date bullying messages or images were sent and note any details about the sender
- Don't retaliate or reply
- Keep and save any offending emails, text messages, images or online conversations

Make sure you tell:

- An adult you trust or call a helpline like Childline on 0800 1111 in confidence or CEOPS www.ceop.gov.uk/reportabuse/index.asp

- The service provider. Check the mobile phone company or internet provider. They may be able to track the bully down

- Your School. Your tutor, Head of House or Student Support can help you.

4.6 CYBERBULLYING RESOURCES FOR SCHOOLS

www.childnet-int.org has a DVD for secondary Schools about keeping safe in online chat rooms.. Order at www.childnet-int.org/order.
Childnet International also advises on Internet safety and has a range of leaflets for children and parents in a number of languages, including Hindi, Punjabi and Maltese.

www.wiredsafety.org has some useful tips.

Stop receiving text messages for a while by turning off incoming messages for a couple of days. This might stop the person texting by making them believe the number's changed. To find out how to do this, visit www.wiredsafety.org.
If the bullying persists, you can change your phone number. Ask your mobile service provider (such as Orange, O2, Vodafone or T-Mobile).

Child Exploitation and Online Protection Centre (CEOP)

Set up by the Government, the CEOP website helps adults get to grips with new and emerging technologies popular with young people. It includes advice on how to report cyberbullying, sexual abuse on line and the dangers of viruses

Thinkuknow.co.uk
Information from the Child Exploitation and Online Protection Centre on how to stay safe online. It includes details of the CEOP training courses. It provides interactive resources for KS1-KS4, teachers and parents

Virtual Global Taskforce (VGT)

Made up of police forces around the world, working together to fight online child abuse. The site includes advice, information and support for adults and children.

- http://www.kidsmart.org.uk/ has some useful tips.

- http://www.teach-ict.com/ks3/internet_safety/staying_safe/stayingsafe1.htm also has some useful tips.

Appendix 1: Acceptable Use Agreement Years 7-11

1.0 Using technology in School

- I will only use ICT systems, e.g. computers, laptops and tablets, which I have been given permission to use.
- I will only use the approved email account that has been provided to me by The King's School.
- I will not store or use any personal data relating to a student or staff member for non-school related activities. If I have any queries about storing or using personal data, I will speak to my classroom teacher.
- I will delete any chain letters, spam, and other emails from unknown senders without opening them.
- I will ensure that I gain permission from my classroom teacher before accessing learning. materials, e.g. source documents, from unapproved sources.
- I will not share my passwords, e.g. to my school email address, with anyone.
- I will not install any software onto School ICT systems unless instructed to do so by a member of staff.
- I will only use recommended removable media, e.g. encrypted USB drives, and I will keep all school-related information stored on these secure.
- I will adhere to the e-safety guidelines I have been taught.
- I will only use the School's ICT facilities to:
    - Complete homework and coursework, and to prepare for lessons and exams.
    - Undertake revision and research.
    - Gather or process information for extra-curricular activities, e.g. creating the School newsletter.
- I will not use the School's ICT facilities to access, download, upload, send, receive, view or display any of the following:
    - Illegal material.
    - Any content that could constitute a threat, bullying or harassment, or anything negative about other persons or the School.
    - Content relating to a person's sexual orientation, gender assignment, religion, race, disability or age.
    - Online gambling.
    - Content which may adversely affect the reputation of any organisation (including the School) or person, whether or not they are known to be true or false.
    - Any sexually explicit content.
    - Any personal data or information.

2.0 Mobile devices

- I will use School-owned mobile devices, e.g. laptops and tablets, for educational purposes only.
- In line with the "Off and Away" policy, I will ensure that my mobile device is switched off during School hours, and will only use my device to make or receive calls when a member of staff permits me to do so.
- I will seek permission from a member of staff before a School-owned mobile device is used to take images or recordings.
- I will not use any mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and School-owned mobile devices do not contain any inappropriate or illegal content.
- I will not access the WiFi system using personal mobile devices.

- I will not take or store images or videos of staff members on any mobile device, regardless of whether or not it is School-owned.

3.0 Social media

- I will not use any School-owned mobile devices to access personal social networking platforms.
- I will not communicate or attempt to communicate with any staff members over personal social networking platforms.
- I will not accept or send 'friend requests' from/to any staff members over personal social networking platforms.
- I will ensure that I apply the necessary privacy settings to any social networking sites.
- I will not publish any comments or posts about the School on any social networking platforms which may affect the School's reputation.
- I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of students, staff or parents, on any online website.
- I will not post any material online that:
    - Is offensive.
    - Is private or sensitive.
    - Infringes copyright laws.
    - Damages the School's reputation.
    - Is an image or video of any staff, parent or non-consenting student(s).

4.0 Reporting misuse

- I will ensure that I report any misuse or breaches of this agreement by students or staff members to a member of staff.
- I understand that my use of the internet will be monitored and recognise the consequences if I breach the terms of this agreement, e.g. access restriction and/or confiscation of my personal mobile device.
- I understand that the School may decide to take disciplinary action against me in accordance with the School's behaviour rewards and sanctions policy if I breach this agreement.

I certify that I have read and understood this agreement and ensure that I will abide by each principle.

Name:	
Signed: [student]	
Date:	
Signed: [parent/carer]	
Date:	

Appendix 2: Acceptable Use Agreement 6th Form

1.0 Summary

The King's School understands the benefits technology can have on enhancing the curriculum and students' learning; however, we must ensure that students respect School property and use technology appropriately. To achieve this, we have created this acceptable use agreement which outlines our expectations of students when using technology, whether this is on personal or School devices and on or off the School premises.

Please read this document carefully and sign below to accept that you agree to the terms outlined.

2.0 Using technology in School

- I will only use ICT systems, e.g. computers, laptops and tablets, which I have been given permission to use.
- I will only use the approved email account that has been provided to me by The King's School.
- I will not store or use any personal data relating to a student or staff member for non-School related activities. If I have any queries about storing or using personal data, I will speak to my classroom teacher.
- I will delete any chain letters, spam, and other emails from unknown senders without opening them.
- I will ensure that I get permission from my classroom teacher before accessing learning materials, e.g. source documents, from unapproved sources.
- I will only use the internet for personal use during out-of-School hours, including break and lunchtimes. During School hours, I will use the internet for School work only.
- I will not share my passwords, e.g. to my School email address, with anyone.
- I will not install any software onto School ICT systems unless instructed to do so by a member of staff.
- I will only use recommended removable media, e.g. encrypted USB drives, and I will keep all School-related information stored on these secure.
- I will adhere to the e-safety guidelines I have been taught.
- I will only use the School's ICT facilities to:
    - Complete homework and coursework, and to prepare for lessons and exams.
    - Undertake revision and research.
    - Gather or process information for extra-curricular activities, e.g. creating the School newsletter.
- I will not use the School's ICT facilities to access, download, upload, send, receive, view or display any of the following:
    - Illegal material.
    - Any content that could constitute a threat, bullying or harassment, or anything negative about other persons or the School.
    - Content relating to a person's sexual orientation, gender assignment, religion, race, disability or age.
    - Online gambling.
    - Content which may adversely affect the reputation of any organisation (including the School) or person, whether or not they are known to be true or false.
    - Any sexually explicit content.
    - Any personal data or information.

3.0 Mobile devices

- I will use School-owned mobile devices, e.g. laptops and tablets, for educational purposes only.
- I will ensure that my mobile device is either switched off or set to silent mode during School hours, and will only use my device to make or receive calls in Post 16 common areas or when a member of staff permits me to do so.
- I will seek permission from a member of staff before a School-owned mobile device is used to take images or recordings.
- I will not use any mobile devices to take pictures of students unless I have their consent.
- I will not use any mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and School-owned mobile devices do not contain any inappropriate or illegal content.
- I will not use the School WiFi for data heavy or entertainment services, examples include but is not limited to: Software updates, Video, Software, Games (sixth form)
- I will not take or store images or videos of staff members on any mobile device, regardless of whether or not it is School-owned.

4.0 Social media

- I will not use any School-owned mobile devices to access personal social networking platforms.
- I will not communicate or attempt to communicate with any staff members over personal social networking platforms.
- I will not accept or send 'friend requests' from/to any staff members over personal social networking platforms.
- I will ensure that I apply the necessary privacy settings to any social networking sites.
- I will not publish any comments or posts about the School on any social networking platforms which may affect the School's reputation.
- I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of students, staff or parents, on any online website.
- I will not post any material online that:
    - Is offensive.
    - Is private or sensitive.
    - Infringes copyright laws.
    - Damages the School's reputation.
    - Is an image or video of any staff, parent or non-consenting student(s).

5.0 Reporting misuse

- I will ensure that I report any misuse or breaches of this agreement by students or staff members to a member of staff.
- I understand that my use of the internet will be monitored and recognise the consequences if I breach the terms of this agreement, e.g. access restriction and/or confiscation of my personal mobile device.
- I understand that the School may decide to take disciplinary action against me in accordance with the School's Behaviour rewards and sanctions policy if I breach this agreement.

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

Name:	
Signed:	
Date:	
Signed:	
Date:	

Appendix 3: Computer Security/SIMS User Policy: Staff

Policy

1.0 Summary

This Acceptable use policy applies to all The King's school staff. Whilst our school promotes the use of technology, and understands the positive effects it can have on enhancing students' learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly and will be reported to the senior leadership team in order for any necessary further action to be taken.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises, and applies to all staff, volunteers, contractors and visitors.

Please read this document carefully, and sign below to show you agree to the terms outlined.

2.0 Using technology in school

- I will only use ICT systems and services, such as computers (including laptops), tablets and online services (such as remote desktop) which have been permitted for my use.
- I will not leave a computer or device unattended without logging off or locking that computer\device
- I will only use the approved email accounts that have been provided to me.
- I will not use personal emails to send and receive personal data or information.
- I will not share sensitive personal data with any other students, staff or third parties unless explicit consent has been received.
- I will ensure that any personal data is stored in line with the GDPR.
- I will delete any chain letters, spam and other emails from unknown sources without opening them.
- I will ensure that I check the content of all online sources that I use in lessons before showing it to students e.g. youtube clips, websites (particularly for any inappropriate adverts/pop-ups), use of language etc.
- I will only use the internet for personal use outside of working hours.
- I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- I will not share school-related passwords with students, staff or third parties unless permission has been given for me to do so.
- I will not install any software onto school ICT systems unless instructed to do so by the Network Manager.
- I will ensure any personal school-connected device is both protected by anti-virus software and the software is updated and that I check this on a weekly basis.
- I will only use recommended removable media and will keep this securely stored in line with the GDPR.
- I will only store data on school systems, removable media or other technological devices that has been encrypted or pseudonymised.
- I will only store sensitive personal data where it is absolutely necessary and which is encrypted.
- I will provide removable media to the IT services team for safe disposal once I am finished with it.

3.0 Mobile devices

- I will only use school-owned mobile devices for purposes relating to the school and my role.
- I will only use mobile devices for personal use outside of working hours.
- I will ensure that mobile devices are either switched off or set to silent mode during school hours, and will only make or receive calls in specific areas, e.g. the staffroom.
- I will ensure mobile devices are stored in a secure space or area during lesson times.
- I will not use personal mobile devices to take images or videos of students or staff – I will comply with the GDPR and/or seek advice from the Network manager or DPO before any school-owned mobile device is used to take images or recordings.
- I will not use mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not use personal mobile devices to communicate with students or parents.
- I will ensure contact with parents or students using school owned mobile devices in the communication log
- I will not store any images or videos of students, staff or parents on any mobile device unless consent has been sought from the individual(s) in the images or videos.
- In line with the above, I will only process images or videos of students, staff or parents for the activities for which consent has been sought.
- I will ensure that any school data stored on personal mobile devices is encrypted and pseudonymised and give permission for the ICT services team to erase and wipe data off my device if it is lost or as part of exit procedures.

4.0 Social media and online professionalism

- If I am representing the school online, e.g. through blogging or on school social media account, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not use any school-owned mobile devices to access personal social networking sites, unless it is beneficial to the material being taught.
- I will not communicate with students or parents over personal social networking sites.
- I will not accept 'friend requests' from any parents over personal social networking sites.
- I will ensure that I apply the necessary privacy settings to any social networking sites.
- I will not publish any comments or posts about the school on any social networking sites which may affect the school's reputability.
- I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of students, staff or parents, on any online website.
- I will not post or upload any images and videos of students, staff or parents on any online website without consent from the individual(s) in the images or videos.
- In line with the above, I will only post images or videos of students, staff or parents for the activities for which consent has been sought.
- I will not give my home address, phone number, mobile number, social networking details or email addresses to students or parents – any contact with parents will be done through authorised school contact channels.

5.0 Working at home

- I will adhere to the principles of the GDPR when taking work home.
- I will ensure I obtain permission from the network manager or data protection officer (DPO) before any personal data is transferred from a school-owned device to a personal device.

- I will ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised.
- I will ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted, inaccessible to other users of that personal device and with the written approval of the DPO.
- I will ensure my personal device has been assessed for security by the IT services team before it is used for lone-working.
- I will ensure no unauthorised persons, such as family members or friends, can access any personal data on or from personal devices used for lone-working.
- I will act in accordance with the school's data protection and use of new technologies policy when transporting school equipment and data.

6.0 Training

- I will ensure I participate in any e-safety or online training offered to me, and will remain up-to-date with current developments in social media and the internet as a whole.
- I will ensure that I allow the Network Manager and DPO to undertake regular audits to identify any areas of need I may have in relation to training.
- I will ensure I employ methods of good practice and act as a role model for students when using the internet and other digital devices.
- I will ensure that I deliver any training to students as required.

7.0 Reporting misuse

- I will ensure that I adhere to any responsibility I have for monitoring e.g. to monitor students' internet usage.
- I will ensure that I report any misuse by students, or by staff members breaching the procedures outlined in this agreement, to the Network Manager or DPO.
- I understand that my use of the internet is monitored and recognise the consequences if I breach the terms of this agreement.
- I understand that the Headteacher may decide to take disciplinary action against me in accordance with the Disciplinary Procedure, if I breach this agreement.

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

Date:	
Signed:	

Appendix 4: Acceptable use- staff

1.0 Introduction

- This policy applies to all employees, volunteers, supply staff and contractors using school ICT facilities.
- The school acceptable use policy is divided into the following three sections:
    - General policy and code of practice.
    - Internet policy and code of practice.
    - Email policy and code of practice.

This policy should be read in conjunction with the school's Acceptable Use Agreement, Data Protection Policy and Privacy Notices Policy.

2.0 General Policy and code of practice

- The school has well-developed and advanced ICT systems, which it intends for you to benefit from.
- This policy sets out the rules that you must comply with to ensure that the system works effectively for everyone.

3.0 Privacy

- The GDPR and Data Protection Act 2018 require all personal and special category data to be processed with the utmost credibility, integrity and accuracy. This applies to all data the school stores on its network regarding staff, students and other natural persons it deals with whilst carrying out its functions.
- The school will only process data in line with its lawful basis to uphold the rights of both students and staff and other third parties.
- In order to protect students' safety and wellbeing, and to protect the school from any third party claims or legal action, the school may view any data, information or material on the school's ICT systems (whether contained in an email, on the network, notebooks or laptops) and in certain circumstances, disclose that data, information or material to third parties, such as the police or social services. The school's Privacy Notices details the lawful basis under which the school is lawfully allowed to do so.
- The school disclaimer that automatically appears at the end of each of your emails notifies the recipient that any email correspondence between you may be monitored. You must not remove this disclaimer. You should bring to the attention of any person who wishes or intends to send you an email that the school may monitor the content of their email.

4.0 Code of practice: general

The school's philosophy	In using ICT, you will follow the School's ethos and consider the work and feelings of others. You must not use the system in a way that might cause annoyance or loss of service to other users.
Times of access	The network is available during term time. Out of term time the network will be subject to maintenance downtime and so may not be available for brief periods.
User ID and password and logging on	You will be given your own user ID and password. You must keep these private and not tell or show anyone what they are. Your password must be a mix of the following: • Contain at least eight characters • A mixture of lower case and capital letters • At least one numbers • At least one symbol If you forget or accidentally disclose your password to anyone else, you must report it immediately to a member of the ICT support staff. You must not use another person's account or allow another person to use your account. The facilities are allocated to you on a personal basis and you are responsible for the use of the machine when you are logged on. The school's system records and senior ICT staff monitor your use of the system. Use of the school's facilities by a third party using your user name or password will be attributable to you, and you will be held accountable for the misuse. You must not log on to more than one computer at the same time.
Printing	The school may wish to check that expensive resources are being used efficiently and the member of staff may suggest other strategies to you to save on resources.
Logging off	You must log off from the computer you are using at the end of each of your sessions and wait for the standard login screen to reappear before leaving. This signals to the system that you are no longer using the service; it ensures security and frees up resources for others to use.
Access to information not normally available	You must not use the system or the internet to find or use facilities or flaws in the system that might give access to information or areas of the network not normally available. You must not attempt to install software to explore or harm the system. Use of hacking tools, e.g. 'loggers', 'sniffers' or 'evidence elimination software', is expressly forbidden.
Connections to the system	You must not connect any hardware which may be detrimental to the school's network.

Connections to the computer	You should use the keyboard, mouse and any headphones provided. You must not adjust or alter any settings or switches without first obtaining the written permission of a member of the ICT staff. You must never attempt to use any of the connectors on the back of any desktop computer. You may use USB memory sticks, or other portable storage media where a port is provided on the front of the computers. You are not permitted to connect anything else to the computer without first getting the permission of a member of the ICT staff.
Virus	If you suspect that your computer has a virus, you must report it to a member of the ICT staff immediately.
Installation of software, files or media	You must not install or attempt to install software of any kind to network drives or local hard drives of networked desktop computers. You must not alter or re-configure software on any part of the school's system.
File space	You must manage your own file space by deleting old data rigorously and by deleting emails that you no longer require. To comply with GDPR, where there is no legal basis for retention of data you are legally required to remove any data that that refers to a departed Student, their parents\guardians or member of staff. If you are unsure you should retain an email, refer to the DPO for guidance. If you believe that you have a real need for additional space, please discuss this with a senior member of the ICT support staff.
Transferring files	You may transfer files to and from your network home directories using removable devices. When transferring files to and from your network home directories, you must not import or export any material unless the owner of that material expressly permits you to do so.
Reporting faults and malfunctions	You must report any faults or malfunctions in writing to the ICT support staff, including full details and all error messages, as soon as possible.
Food and drink	You must not eat or drink, or bring food or drink, including sweets and chewing gum, into the ICT rooms. You must always maintain a clean and quiet working environment.
Copying and plagiarising	You must not plagiarise or copy any material which does not belong to you.
Copies of important work	Any data containing personal and special category data must not be stored on unencrypted media and paper copies must be stored in a secure lockable location.

Securing Passwords\access	Usernames and passwords should not be written down, they should be stored digitally within your user area or within a password vault Use of password caching is forbidden

5.0 Internet policy and code of practice

- The school can provide access to the internet from desktop PCs via the computer network and through a variety of electronic devices connected wirelessly to the network.
- Whenever accessing the internet using the school's or personal equipment you must observe the code of practice below.
- This policy and code of practice is designed to reduce and control the risk of offences being committed, liabilities being incurred, staff or other students being offended and the school's facilities and information being damaged.
- Any breach of this policy and the code of practice will be treated extremely seriously, and it may result in disciplinary or legal action or expulsion.
- The school may take steps, including legal action where appropriate, to recover from an individual any expenses or liabilities the school incurs because of the breach of this policy and code of practice.

6.0 Why is a code of practice necessary?

There are four main issues:

- Although the internet is often described as 'free', there is a significant cost to the school for using it. This cost includes line charges, subscription costs (which may depend on how much a service is used) and the computer hardware and software needed to support internet access.
- Although there is much useful information on the internet, there is a great deal more material which is misleading or irrelevant. Using the internet effectively requires training and self-discipline. Training is available on request from ICT staff.
- Unfortunately, the internet carries a great deal of unsuitable and offensive material. It is important for legal reasons, reasons of principle, and to protect to protect the staff and students who access to the internet, that it is properly managed. Accessing to attempting to access certain websites and services, and viewing, copying or changing certain material, could amount to a criminal offence and give rise to legal liabilities.
- There is a danger of importing viruses on to the School's network, or passing viruses to a third party, via material downloaded from or received via the internet, or brought into the school on disks or other storage media.

7.0 Code of practice: internet use

Use of the internet	The Internet should not normally be used for private or leisure purposes; it is provided primarily for education or business use. You may use the internet for other purposes provided that: • Such use is occasional and reasonable; • Such use does not interfere in any way with your duties; and • You always follow the code of practice.
Inappropriate material	You must not use the internet to access any newsgroups, links, list-servers, web pages or other areas of cyberspace that could be offensive because of pornographic, indecent, racist, violent, illegal, illicit, or other inappropriate content. "Inappropriate" in this context includes material which is unsuitable for viewing by students. You are responsible for rejecting any links to such material which may appear inadvertently during research. If you encounter any material which could be regarded as offensive, you must leave that website or service immediately and not make any copy of that material. If you encounter any difficulty in leaving a website or service, you must inform the ICT support staff immediately.
Misuse, abuse and access restrictions	You must not misuse or abuse any website or service or attempt to bypass any access controls or restrictions on any website or service.
Monitoring	The internet access system used by the school maintains a record which identifies who uses the facilities and the use that you make of them. The information collected includes which website and services you visit, how long you remain there and which material you view. This information will be analysed and retained, and it may be used in disciplinary and legal proceedings.
Giving out information	You must not give any information concerning the school, its students or parents, or any member of staff when accessing any website or service. This prohibition covers the giving of names of any of these people – the only exception being the use of the school's name and your name when accessing a service which the school subscribes to.
Personal safety	You should take care with who you correspond with. You should not disclose where you are or arrange meetings with strangers you have got in contact with over the internet.
Hardware and software	You must not make any changes to any of the school's hardware or software. This prohibition also covers changes to any of the browser settings. The settings put in place by the school are an important part of the school security arrangements and making any changes, however innocuous they might seem, could allow hackers and computer viruses to access or damage the school's systems.
Copyright	You should assume that all material on the internet is protected by copyright and must be treated appropriately and in accordance with the owner's rights. You must not copy, download or plagiarise material on the internet unless the owner of the website expressly permits you to do so.

	You must ensure copyrighted resources or self-made resources which incorporate copyright material are not publicly accessible over the internet without obtaining permission from the copyright holder.

8.0 Email policy and code of practice

- The school's computer system enables members of the school to communicate by email with any individual or organisation with email facilities throughout the world.
- For the reason outlined above, it is essential that a written policy and code of practice exists, which sets out the rules and principles for use of email by all.
- Any breach of this policy and code of practice will be treated seriously and it may result in disciplinary or legal action or expulsion.
- The school may take steps, including legal action where appropriate, to recover from an individual any expenses or liabilities the school incurs because of the breach of this policy and code of practice.

9.0 Code of practice: email

Purpose	You should only use the school's email system for work related emails. You are only permitted to send a reasonable number of emails.
Trust's disclaimer	The school's email disclaimer is automatically attached to all outgoing emails and you must not cancel or dis-apply it.
Monitoring	Copies of all incoming and outgoing emails, together with details of their duration and destinations are stored centrally (in electronic form). The frequency and content of incoming and outgoing external emails are checked termly to determine whether the email system is being used in accordance with this policy and code of practice. The Headteacher, senior staff and technical staff are entitled to have read-only access to your emails.
Security	As with anything else sent over the internet, emails are not completely secure. There is no proof of receipt, emails can be 'lost', they can suffer from computer failure and a determined 'hacker' could intercept, read and possibly alter the contents. As with other methods of written communication, you must make a judgment about the potential damage if the communication is lost or intercepted. Never send bank account information, including passwords, by email. Where an email contains personal or confidential data, you must make use of encryption tools available.
Program files and non-business documents	You must not introduce program files or non-business documents from external sources on to the school's network. This might happen by opening an email attachment or by downloading a file from a website. Although virus detection software is installed, it can never be guaranteed 100 percent successful, so introducing nonessential software is an unacceptable risk for the school.

	If you have any reason for suspecting that a virus may have entered the school's system, you must contact the ICT support staff immediately.
Quality	Emails constitute records of the school and are subject to the same rules, care and checks as other written communications sent by the school. Emails will be checked under the same scrutiny as other written communications. Staff members should consider the following when sending emails: • Whether it is appropriate for material to be sent to third parties • The emails sent and received may have to be disclosed in legal proceedings • The emails sent and received maybe have to be disclosed as part of fulfilling an SAR • Whether any authorisation is required before sending • Printed copies of emails should be retained in the same way as other correspondence, e.g. letter • The confidentiality between sender and recipient • Transmitting the work of other people, without their permission, may infringe copyright laws. • The sending and storing messages or attachments containing statements which could be construed as abusive, libelous, harassment may result in disciplinary or legal action being taken. • Sending or storing messages or attachments containing statements which could be construed as improper, abusive, harassing the recipient, libelous, malicious, threatening or contravening discrimination legislation or detrimental to the is a disciplinary offence and may also be a legal offence.
Inappropriate emails or attachments	You must not use email to access or send offensive material, chain messages or list-servers or for the purposes of bullying or plagiarising work. You must not send personal or inappropriate information by email about yourself, other members of staff, students or other members of the school community. If you receive any inappropriate emails or attachments you must report them to technical staff.
Viruses	If you suspect that an email has a virus attached to it, you must inform the technical staff immediately.
Spam	You must not send spam (sending the same message to multiple email addresses) without the permission of senior staff.
Storage	You are asked to regularly delete any material you no longer require and to archive material that you wish to keep. To comply with GDPR, where there is no legal basis for retention of that email you are legally required to remove any email that that refers to a departed Student, their parents\guardians or member of staff. It is important you remove this from both your inbox and sent items folder. If you are unsure you should retain an email, refer to the DPO for guidance.

Message size	Staff are limited to sending messages with attachments which are up to 50Mb in size. If you wish to distribute files within the school, you can do so by using shared areas.
Confidential Emails	You must ensure that confidential emails are always suitably protected. If working at home or remotely, you should be aware of the potential for an unauthorised third party to be privy to the content of the email. Confidential emails should be deleted when no longer required.

10.0 Email policy – advice to staff

- Staff should remind themselves of the ICT Acceptable Use Policy which relates to the monitoring, security and quality of emails. In addition, staff should be guided by the following good practice:
- Staff should check their emails daily and respond, as appropriate, within a reasonable period if the email is directly addressed to them.
- Staff should avoid spam, as outlined in this policy.
- Staff should avoid using the email system as a message board and thus avoid sending trivial global messages.
- Whilst accepting the convenience of the staff distribution list, staff should try to restrict its use to important or urgent matters.
- Staff should send emails to the minimum number of recipients.
- Staff are advised to create their own distribution lists, as convenient and appropriate.
- Staff should always include a subject line.
- Staff are advised to keep old emails for the minimum time necessary.

11.0 Further guidelines

- Emails remain a written record and can be forwarded to others or printed for formal use.
- "tone" can be misinterpreted on the printed page and once it is sent it could end up in the public domain forever. Email lacks the other cues and clues that convey the sense in which what you say is to be taken, and you can easily convey the wrong impression.
- Remember that sending emails from your school account is similar to sending a letter on school letterhead, so don't say anything that might bring discredit or embarrassment to yourself or the school.
- Linked with this and given the popularity and simplicity for recording both visual and audio material, staff are advised to remember the possibility of being recorded in all that they say or do.

Appendix 5: Acceptable use: IT Technical support staff

1.0 Introduction

Whilst our school promotes the use of technology, and understands the positive effects it can have on enhancing students' learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly and will be reported to the Headteacher in order for any necessary further action to be taken.

As our ICT technicians have greater access to our computer systems and security, the school has taken the appropriate measures to ensure our ICT technicians understand what is expected of them as they carry out their duties.

Please read this document carefully, and sign below to show you agree to the terms outlined.

2.0 Using technology in school

- I will only use ICT systems, such as computers (including laptops) and tablets, which have been permitted for my use.
- I will not leave a computer or device unattended without logging off or locking that computer\device.
- I will only use the approved email accounts that have been provided to me.
- I will not use personal emails to send and receive personal data or information.
- I will not share sensitive personal data with any students, staff or third parties unless explicit consent has been received.
- I will ensure that any personal data is stored in line with the GDPR.
- I will delete any chain letters, spam and other emails from unknown sources without opening them.
- I will ensure that I obtain permission prior to accessing learning materials from unapproved sources.
- I will only use the internet for personal use outside of working hours.
- I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- I will not share school-related passwords with students, staff or third parties unless permission has been given for me to do so.
- I will ensure any personal school-connected device is both protected by anti-virus software and the software is updated and that I check this on a weekly basis.
- I will only use recommended removable media and will keep this securely stored in line with the GDPR.
- I will only store data on removable media or other technological devices that has been encrypted of pseudonymised.
- I will only store sensitive personal data where it is absolutely necessary and which is encrypted.
- I will provide safely dispose of sensitive data on removable media using either shredding or destructive methods once I am finished with it.
- I will assist in the recording and maintenance of all school software and hardware using an inventory, which I will audit on a termly basis.
- I will document all changes to software and hardware using the inventory.
- I will remove all out-of-date and 'end of life' software and detailing this in the inventory.
- I will make sure all devices and user accounts are password protected.
- I will work with colleagues in IT services to ensure the delivery of high-quality firewall protection.
- I will work with my colleagues in the ICT Services department to ensure the delivery of high-quality firewall protection.

- I will undertake regular malware scans on all devices to make sure they are suitably protected from the threat of infection.
- I will install and maintain mail security software to block and filter all spam and harmful emails.
- I will not remotely access any devices without appropriate reason – any remote access I do undertake will be documented.
- I will check the school's internet filtering software for updates to protect users from inappropriate and malicious content.
- I will ensure all new users are safely added to the school system and ensure they understand what they can and can't access.
- I will safely remove all inactive users from the school's systems to ensure no student or member of staff can regain access to the school network after they have left.
- I will, at the start of every school year, remind all users to update their passwords.
- I will maintain secure and safe records of user passwords to help users reset passwords where necessary.
- I will work with the data protection officer (DPO) to ensure the safe and proper review, back-up and disposal of all data the school holds.
- I will not access any personal or sensitive personal data pertaining to any member of staff, student, visitor or other person, without the express permission of the individual in question and/or the DPO.
- I will assist with the school's helpdesk provision – ensuring timely resolutions to requests and problems, and offer updates on the status of requests.

3.0 Mobile devices

- I will only use school-owned mobile devices for purposes relating to the school and my role.
- I will only use mobile devices for personal use outside of working hours.
- I will ensure that mobile devices are either switched off or set to silent mode during school hours, and will only make or receive calls in specific areas, e.g. the staffroom.
- I will ensure mobile devices are stored in a secure space or area during lesson times.
- I will not use personal mobile devices to take images or videos of students or staff – I will comply with the GDPR and seek advice from the Network manager or DPO before any school-owned mobile device is used to take images or recordings.
- I will not use any mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not use personal mobile devices to communicate with students or parents.
- I will not store any images or videos of students, staff or parents on any mobile device unless consent has been sought from the individual(s) in the images or videos.
- In line with the above, I will only process images or videos of students, staff or parents for the activities for which consent has been sought.
- I will ensure that any school data stored on personal mobile devices is encrypted and pseudonymised and give permission for the ICT services team to erase and wipe data off my device if it is lost or as part of exit procedures.
- I will ensure all apps on mobile devices are kept up-to-date and secure.

4.0 Social media and online professionalism

- If I am representing the school online, e.g. through blogging or on a school social media account, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not use any school-owned mobile devices to access personal social networking sites, unless it is beneficial to the material being taught;

- I will not communicate with students or parents over personal social networking sites.
- I will not accept 'friend requests' from any students or parents over personal social networking sites.
- I will ensure that I apply the necessary privacy settings to any social networking sites.
- I will not publish any comments or posts about the school on any social networking sites which may affect the school's reputability.
- I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of students, staff or parents, on any online website.
- I will not post or upload any images and videos of students, staff or parents on any online website without consent from the individual(s) in the images or videos.
- In line with the above, I will only post images or videos of students, staff or parents for the activities for which consent has been sought.
- I will not give my home address, phone number, mobile number, social networking details or email addresses to students or parents – any contact with parents will be done through authorised school contact channels.

5.0 Working at home

- I will adhere to the principles of the GDPR when taking work home.
- I will ensure I obtain permission from the network manager or data protection officer (DPO) before any personal data is transferred from a school-owned device to a personal device.
- I will ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised.
- I will ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted, inaccessible to other users of that personal device and with the written approval of the DPO.
- I will ensure my personal device has been assessed for security by the IT services team before it is used for lone-working.
- I will ensure no unauthorised persons, such as family members or friends, can access any personal data on or from personal devices used for lone-working.
- I will act in accordance with the school's Data protection and use of new technologies policy when transporting school equipment and data.
- I will ensure all school-owned devices, e.g. laptops, mobile phones and tablets, are encrypted and password protected before they are used away from the school premises.
- I will review all devices before they are used away from the premises to ensure (where possible) the correct tracking software is installed – so any lost or stolen items can be retrieved.

6.0 Training

- I will ensure I participate in any e-safety or online training offered to me, and will remain up-to-date with current developments in social media and the internet as a whole.
- I will ensure that I allow the Network Manager and DPO to undertake regular audits to identify any areas of need I may have in relation to training.
- I will ensure I employ methods of good practice and act as a role model for students when using the internet and other digital devices.
- I will ensure that I deliver any training to students as required.
- I will proactively identify staff training needs and ensure all staff members and students receive the correct training to identify and block any potential cyber-attacks, data breaches or suspicious emails they could receive.

7.0 Reporting misuse

- I will ensure that I adhere to any responsibility I have for monitoring e.g. to monitor students' and staff internet usage.
- I will ensure that I report any misuse by students, or by staff members breaching the procedures outlined in this agreement, to the Network Manager or DPO.
- I understand that my use of the internet is monitored and recognise the consequences if I breach the terms of this agreement.
- I understand that the Headteacher may decide to take disciplinary action against me in accordance with the Disciplinary Procedure, if I breach this agreement.
- I will keep a record of all users who have accessed and/or tried to access inappropriate content on school devices.

Date:	
Signed:	