Somerset Road Education Trust

ICT and Internet acceptable use policy

Contents

Approved by: LGC		**Date:** 11th September 2023
Last reviewed on:	June 2023	
Next review due by:	June 2024	

1. Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.
However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.
This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.
Breaches of this policy may be dealt with under our behaviour policy, staff code of conduct.

2. Relevant legislation and guidance

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

- 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 2019
- Searching, screening and confiscation: advice for schools

3. Definitions

- **"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
- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **"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 Acceptable use

We expect, encourage and train all users of school ICT equipment, tools and systems to be:

- Responsible – following rules, guidelines, processes as directed and advised by senior and technical staff
- Respectful – to demonstrate the highest levels of politeness and conduct when communicating electronically
- Careful – treating equipment and systems with respect and reporting any issues, breakages or faults
- Positive and purposeful – using tools to positively impact others, learning and other school duties
- Apply school values of hope, wisdom, community, dignity and love when using IT systems

5 Unacceptable use

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 (see section 4.2 below).

- Unacceptable use of the school's ICT facilities includes:
- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using any removable storage to transfer data from the system
- Sharing or using others logons or passwords or other confidential information
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Using personal cameras or recording devices
- 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
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, 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
- Trespassing in others folders, work or files that you don't have permission to access
- 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
- This is not an exhaustive list. The school reserves the right to amend this list at any time. The [Headteacher or any other relevant member of staff e.g. the Network Manager] 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.

5.1 Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the head teacher's discretion.
Requests in writing/email to the Data Security and E-Safety group explaining and describing the need for these exemptions to be lifted. Requests and decisions to be documented and filed by the Network Manager.

5.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on [behaviour/ staff code of conduct/etc.].

- Behaviour Policy
- SRET Code of Conduct

Or found at https://www.st-marks.wilts.sch.uk/page/policies/79602 and www.somersetroadeducationtrust.uk

6 Staff (including governors, volunteers, visitors and contractors)

6.1 Access to school ICT facilities and materials

- The school's Network Manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:
    - Computers, tablets and other devices
    - Access permissions for certain programmes or files
- Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.
- Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, must contact the Data Security Group with the request and reasons why they need this access. Requests and decisions will be documented and kept by the Network Manager.

6.1.1 Use of phones and email

- The school provides each member of staff with an email address.
- It is compulsory and your responsibility that you make sure you can access your emails, be contactable and check them at least once a day.
- This email account must be used for work purposes only.
- All work-related business must be conducted using the email address the school has provided.
- Staff must not share their personal email addresses with parents and pupils and must not send any work-related materials using their personal email account.

- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the General Data Protection Regulations [GDPR] 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages must be treated as potentially retrievable.
- Staff must take extra care when sending sensitive or confidential information by email to addresses outside SRET or wilts.gov or nhs.net. Any attachments containing sensitive or confidential information must be password protected so that the information is only accessible by the intended recipient, for email recipients outside these domains. The password to open the document must be sent by a different communication method.
- If staff receive an email in error, the sender must 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.
- If staff send an email in error which contains the personal information of another person, they must inform the Headteacher and Network Manager immediately and follow our data breach procedure.
- Staff must not give their personal phone numbers to parents or pupils.
- Staff must use phones provided by the school to conduct all work-related business unless on a community trip where colleagues may share personal numbers to maintain contact with each other to ensure the safety of the whole group.
- School phones must not be used for personal matters unless in exceptional circumstances. (see below 5.2)
- 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.

6.2 Personal use

- Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Network Manager may withdraw permission for it at any time or restrict access at their discretion.
- Personal use is permitted provided that such use:
    - Does not take place during [contact time/teaching hours/non-break time]
    - Does not constitute 'unacceptable use', as defined in section 4
    - Takes place when no pupils are present
    - Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes
- Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).
- Staff must be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.
- Staff must be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.
- Staff must take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.
- Staff must not allow other individuals, including children and other family members, to use their allocated devices.

6.2.1 Personal social media accounts

- Members of staff must ensure that their use of social media, either for work or personal purposes, is appropriate at all times.
- The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

6.3 Remote access

- We allow staff to access the school's ICT facilities and materials remotely through Office 365/SharePoint
- Also using a secure VPN connection
- Managed by the Network Manager
- Encrypted school owned devices
- Only school owned devices that have been authorised and given appropriate permissions can access Office 365 & VPN
- Staff can request remote access via the Data Security Group Requests and decisions to be documented and kept by the Network Manager

- 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.
- 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.
- Data Protection Policy can be found at https://www.st-marks.wilts.sch.uk/page/policies/79602

6.4 School social media accounts

- Not applicable at this present time.

6.5 Monitoring of school network and use of ICT facilities

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

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:

- 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

6.6 Cloud Services/3CX phone App and Home working

- There are times that staff will have the need to work from home. We provide staff with school devices which are encrypted. Staff may only access Office 365/Teams/SharePoint, Sleuth and MyConcern using a school owned device.
- If using video conferencing facilities or Teams for meetings, you must be in a secure confidential environment away from others and free from distraction and have nothing personal on show that could identify your home or address. This must be used in conjunction with the guidelines for using video conferencing.
- All data will be kept secure and not disclosed to anyone else in your household. They must not be party to any conversations that could identify a parent, pupil or member of staff.
- The 3CX phone app may only be used for work purposes and must not be used for private use. The video conferencing protocol is also applied here. The phone app may only be installed on school owned devices unless it has been agreed with the Head Teacher and Network Manager.

7. Pupils

7.1 Access to ICT facilities

- Computers and equipment in the school are available to pupils only under the direct supervision and guidance of staff

7.2 Search and deletion

- 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 pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.
- 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.

8 Parents

8.1 Access to ICT facilities and materials

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

8.2 Communicating with or about the school online

- We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.
- 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 sign the agreement in appendix 2.

9 Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities must use safe computing practices at all times.

9.1 Passwords

- All users of the school's ICT facilities must set strong passwords for their accounts and keep these passwords secure.
- Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.
- Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.
- A password must be at least 8 characters long using a capital letter, numbers and special characters. Passwords will be changed every 180 days and the last 4 passwords cannot be reused.

9.2 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.

9.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy. https://www.st-marks.wilts.sch.uk/page/policies/79602

9.4 Access to facilities and materials

- All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.
- These access rights are managed by the Network Manager. Requests for access must be made to the Data Security Team

- Users must 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 must alert the Headteacher immediately.
- Users must always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems must always be logged out of and closed down completely at the end of each working day.

9.5 Encryption

- The school ensures that its devices and systems have an appropriate level of encryption.
- School staff may not use personal devices to access school data, work remotely, or take personal data (such as pupil information) out of school unless they have been specifically authorised to do so by the headteacher.
- Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Network Manager.

10 Internet access

- The school wireless internet connection is secured.
- Wi-Fi connections are filtered in line with the filtering policy
- Filtering is provided by the school's internet provider
- Two tiered connections are for students/staff and a guest Wi-Fi provided for visitors. This is generated on a request basis.
- If staff or pupils discover unsuitable sites or any material which would be unsuitable, this must be reported to the DSL, DDSL, Data Security Group and Network Manager.

10.1 Pupils

- Wi-Fi is only available to students on a school owned device. In some circumstances where BYOD is necessary, the parents will sign the policy to agree to our Acceptable User Policy and our management system will be installed on the device.
- Filtering is enhanced for pupils and guests

10.2 Parents and visitors

- Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the Network Manager
- The Network Manger will only grant authorisation if:
- Parents are working with the school in an official capacity (e.g. as a volunteer, governor or as a member of the PTA)
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

11 Monitoring and review

- The Data Security Group monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.
- This policy will be reviewed annually.
- The Data Security Group is responsible for approving this policy.

12 Related policies

This policy must be read alongside the school's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Code of Conduct
- Data protection
- Information Security Policy
- Electronic and Communications Policy

Appendix 1: Best Practice guidelines for school staff on social media

1. Don't accept friend requests from pupils, former pupils or parents/carers (except if maintaining an existing friendship) on social media
2. Consider changing your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
3. Consider changing your profile picture to something unidentifiable, or if not, ensure that the image is professional
4. Consider your privacy settings regularly
5. To be be mindful about tagging other staff members in images or posts
6. Don't share anything publicly that you wouldn't be just as happy showing your pupils
7. Don't use social media sites during your working hours
8. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) can find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or pupils)

Check your privacy settings

Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list

Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts

The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster

Google your name to see what information about you is visible to the public

Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this

Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if…

A pupil or former pupil sends you a friend request on social media

In the first instance, ignore and delete the request. Block the pupil from viewing your profile

Check your privacy settings again, and consider changing your display name or profile picture

If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages

Notify the senior leadership team or the Headteacher about what's happening

You're being harassed on social media, or somebody is spreading something offensive about you

Do not retaliate or respond in any way

Save evidence of any abuse by taking screenshots and recording the time and date it occurred

Report the material to Facebook or the relevant social network and ask them to remove it

If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents

If the perpetrator is a parent or other external adult, a senior member of staff must invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material

If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader must consider contacting the police

Appendix 2: Acceptable use agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers

Name of parent/carer: **Name of child:**

The Internet and other communications technologies are powerful tools, which open up opportunities for everyone. These technologies are great for learning as they can stimulate discussion and collaboration, promote creativity and help us find information quickly. This agreement is intended to make sure that we are all aware of our responsibilities and expectations as members of this school community to keep ourselves, others and our equipment safe. We are part of our school community at school and also at home so it is important that we apply these rules at all times and in all places. Circumstances and technologies vary and change and we must think and apply these expectations and our school values of: hope, wisdom, community, dignity and love to any situation we are in.

Online channels are an important way for parents/carers to communicate with, or about, our school.
The school uses the following channels: Email/text groups for parents (for school announcements and information), Arbor, school website
Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, Facebook, WhatsApp, email groups, email groups.

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers
- *identify children by referring to them by name when commenting on groups or comments online.*
- *send children to school with devices that are enabled to access the phone network or take photos or media, eg smart watches.*

We appreciate that parents and carers have a crucial role and responsibility to teach children about online safety and behaviour. I have read through the pupil agreement with my child and reinforced the importance of online safety at school and home.
I will consider the following steps

- *Have a family agreement for when and where my child can use the Internet. I will ensure they have a balance of technology and other activities, e.g. physical/social activities. I will bear in mind the health risks related to too much screen time, e.g. near to bed time.*
- *I will talk to my child about their use of technology and show an interest in what they are doing.*
- *I will keep myself informed of online safety topics, for example by reading the Vodafone Digital Parenting magazine or visiting links on the Internet eg www.Internetmatters.org (There are lots of other links on the school website)*
- *I am aware of the dangers of using computers and the Internet and understand how to take precautions to protect my child at home, for example using children logins, filtering and monitoring, supervised use and family agreements.*
- *I have read through the pupil acceptable use agreement with my child and reinforced the importance of online safety at school and home.*

Signed:	**Date:**

Appendix 3: Acceptable use agreement for staff, governors, volunteers and contractors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and contractors

Name of staff member/governor/volunteer/contractor:

The Internet and other communications technologies are powerful tools, which open up opportunities for everyone. These technologies are great for learning as they can stimulate discussion and collaboration, promote creativity and help us find information quickly. This agreement is intended to make sure that we are all aware of our responsibilities and expectations as members of this school community to keep ourselves, others and our equipment safe. We are part of our school community at school and also at home so it is important that we apply these rules at all times and in all places. Circumstances and technologies vary and change and we must think and apply these expectations and our school values of hope, wisdom, community, dignity and love to any situation we are in.

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device:

Content

- *I am aware that the Internet is an amazing resource, but also contains content that is: inaccurate, harmful, illegal, commercial and inappropriate and so I will be careful to avoid such content* (and will not create, share, link to or send such material)
- *I will immediately report any illegal, inappropriate or harmful material or incident to the* Designated Safeguarding Lead (DSL) and Network Manager

Conduct

- I will not use school systems in any way which could harm the school's reputation or *engage in any activity in or out of school to damage the reputation of the school or profession, e.g. content/comments on social media.*
- I will use school equipment and systems for school business only and personal equipment for personal business only

Respect and dignity

- *I will always be polite and respectful online - whether in internal or external email or messaging.*
- *I will make sure people are happy before I take and/or use photos and videos of them.*
- *I will only use the photos and videos I've taken with permission and will not name children in my photos or give any information so they can be identified.*
- *I will respect other people's work on the Internet and not copy it without saying where it came from. I will ensure that I have permission to use the original work of others in my own work. Where work is protected by copyright, I will not download or distribute copies (including music and videos).*

Data

- *I will keep school data on school devices and systems, not saving to personal devices or systems.*
- *I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential (except when required by law or by school policy to disclose such information to an appropriate authority).* I will not access, modify or share data I'm not authorised to access, modify or share

Systems and equipment

- I will not share my password with others or log in to the school's network using someone else's details
- *I will only open emails and attachments from people I trust and use official school platforms to store and transfer work*
- *I will treat school equipment with great care and as directed and will immediately report any damage or faults involving equipment or software, however this may have happened.*
- *I will take care not to overload the school system or equipment with large quantities of files, e.g. outdated or duplicated files. I will be organised in storing data and regularly check, tidy and delete unneeded files, e.g. photos and videos.*
- I will not install any unauthorised software, or connect unauthorised hardware or devices to the school's network

Pupils and teaching

- *I will demonstrate high standards and examples in all expectations and responsibilities.* I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.
- *I will embed online safety ideas and skills in my practice and teaching.*
- *I will always directly supervise and guide children in their use of the Internet.*
- *I will communicate with pupils and parents through official school systems.*

I understand that the school will monitor my use of the school's ICT facilities and systems.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: Acceptable use agreement for pupils

Acceptable use of the school's ICT facilities and the internet: agreement for pupils

Name of pupil:

The Internet and other communications technologies are powerful tools, which open up opportunities for everyone. These technologies are great for learning as they can stimulate discussion and collaboration, promote creativity and help us find information quickly. This agreement is intended to make sure that we are all aware of our responsibilities and expectations as members of this school community to keep ourselves, others and our equipment safe. We are part of our school community at school and also at home so it is important that we apply these rules at all times and in all places. Circumstances and technologies vary and change and we must think and apply these expectations and our school values of hope, wisdom, community, dignity and love to any situation we are in.

When using the school's ICT facilities and accessing the internet in school:

Using computers and IT equipment

- *I will only use computers and devices when I have permission and am directly supervised by a member of staff.*
- *I understand that school equipment and systems are for supporting my learning and that is what I will use it for*
- *I will not share my password or use anyone else's. I will always log out or lock when I leave a computer. I will use suitably complex passwords and change them if I think they may be known to anyone else.*
- *I will not use any personal device in school to access the Internet or take photos or record media.*
- *I will not log into personal accounts in school*
- *I will ask a member of staff if I am unsure about anything*

Content

- *I am aware that the Internet is an amazing resource, but also contains information that is: inaccurate, harmful, illegal, commercial and inappropriate and so I will be careful to avoid such content.*
- *I will tell a member of staff if I find any inappropriate content online or anything that upsets me or I am unsure about*

Respect and dignity

- *I will always be polite and respectful with others online.*
- *I will make sure people are happy before I take and/or use photos and videos of them.*
- *I will only use the photos and videos I've taken with permission and will not name children in my photos or give any information so they can be identified.*
- *I will respect other people's work on the Internet and not copy it without saying where it came from. I will ensure that I have permission to use the original work of others in my own work.*
- *Where work is protected by copyright, I will not download or distribute copies (including music and videos).*

Data security

- *I will use sensible names for documents and save regularly to protect my work.*
- *I will immediately report any illegal, inappropriate or harmful material or incident.*

Equipment and systems

- *I will treat school equipment with great care and as directed.*
- *I will immediately report any damage or faults involving equipment or software, however this may have happened.*

Home

- *At home, I will follow family agreements about using computers and devices.*
- *I will agree with my parents about a balance of using technology and other activities, bearing in mind the health risks of too much screen time.*
- *I will be aware of stranger-danger when communicating online, for example, I will not share personal information like my surname or a named photograph, address, telephone number, email, school etc or arrange to meet with anyone.*
- *I will immediately report to an adult anything unpleasant or that I know is inappropriate or makes me feel uncomfortable.*
- *I will try to use websites that my parents/teachers know about and are happy with.*

Signed (pupil):	**Date:**