Acceptable Use Policy

Key document details

Author:	EPM- adapted by SRAT	**Approver:**	Trust Board
Owner:		**Version no.:**	1
Written:	January 2025	**Review Date:**	January 2027
Ratified:			

Related Documents/Policies

References	Title
	E-Safety
	Safeguarding and child protection
	Behaviour Policy
	Disciplinary Policy
	Data Protection Policy
	Use of Photographic Images Policy
	Staff Code of Conduct Policy

Contents

1. Introduction and aims ***5***

2. Legislation and guidance ***5***

3. Definitions ***6***

4. Unacceptable use ***6***

4.1 Exceptions from unacceptable use **7**

4.2 Sanctions **7**

5. Staff (including governors, volunteers, supply teachers and contractors) ***8***

5.1 Access to school ICT facilities and materials **8**

5.1.1 Use of phones and email **8**

5.1.2 Use of printers **9**

5.2 Personal use **9**

5.2.1 Personal social media accounts 10

5.2.2 Communication platforms 10

5.3 Remote access **11**

5.4 School social media accounts **11**

5.5 Images of pupils **11**

5.6 Monitoring of school network and use of ICT facilities **12**

6. Pupils ***12***

6.1 Access to ICT facilities **12**

6.2 Search and deletion **12**

6.3 Unacceptable use of ICT and the internet outside of school **13**

7. Parents ***13***

7.1 Access to ICT facilities and materials **13**

7.2 Communicating with or about the school online **13**

8. Data security ***14***

8.1 Passwords **14**

8.2 Software updates, firewalls, and anti-virus software **14**

8.3 Data protection **14**

8.4 Access to facilities and materials **15**

8.5 Encryption **15**

9. Internet access ***15***

9.1 Parents and visitors **15**

10. Monitoring and review ***15***

Appendix 1: Social media guidance sheet for staff ***16***

Appendix 2: Acceptable use of the internet: agreement for parents and carers ***17***

Appendix 3: Acceptable use agreement for pupils ***19***

Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors ***20***

1. Introduction and aims

The purpose of the policy is to ensure the trusts network is operated safely and all users of ICT are safe. It refers to our school' ICT networks and to the use of mobile technologies, both within it and external to it, and explains the behaviours which are acceptable and unacceptable within our school.

ICT is an integral part of the way our schools work, 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 schools 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/trustees
- Establish clear expectations for the way all members of the trust communities engage with each other and with stakeholders online
- Support the trust's policy on data protection, online safety and safeguarding
- Prevent disruption to the schools through the misuse, or attempted misuse, of ICT systems
- Support the schools 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.

All members of staff have a responsibility to use the school's computer system in a professional, lawful and ethical manner. Our AUP must be fully complied with at all times. All users of the school network should note that it is monitored on a regular basis. Any person who is found to have misused the school system or not followed our AUP could face disciplinary action and in the more serious cases legal action may also be taken.

2. Legislation and guidance

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

- The General Data Protection Regulation
- Data Protection Act 2018
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools

- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011

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, communication applications such as WhatsApp, Facebook Messenger, SMS messaging 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 system 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. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities and online platforms 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 the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- 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
- 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 trust reserves the right to amend this list at any time. The CEO/Headteacher or other delegated member of SLT will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 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 Headteacher's discretion.

In such circumstances, permission must be sought from the Headteacher.

4.2 Sanctions

Staff or pupils who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies including the Behaviour Policy (Pupils), Disciplinary Policy and Staff Code of Conduct (Staff).

In the case of adults who are not staff members other sanctions are available such as revoking permission to use the school's systems.

Members of staff will have been provided access to the above policies as part of your induction. If you require access to a copy these are available from each school office.

5. Staff (including governors/trustees, volunteers, supply teachers and contractors)

5.1 Access to school ICT facilities and materials

The school's IT & Electrical Manager and IT Support Team manage 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 services, programmes or files

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

Staff who have access to services or files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT Support Team.

5.1.1 Use of phones and email

The school provides each member of staff with an email account.

This email account should be used for work purposes only.

All work-related business should 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.

Email attachments should only be opened if the source is known and trusted. There have been an increasing number of spam emails received by staff in schools which contain links that can be damaging to ICT systems and also lead to serious network and equipment hacking.

If you are required to send an email to more than one recipient, ensure that the email addresses are entered in to the 'bcc' box to ensure that you are not sharing personal email addresses with others.

Email should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety. 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 Data Protection Act 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 should be treated as potentially retrievable and public.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. A double checking system should also be implemented whereby one member of staff asks another to check the content of their message before sending.

If staff receive an email in error the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the IT Support Team or Data Protection Officer 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.

School phones must not be used for personal matters.

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.

If for any reason a member of staff feels there is a need to attempt to record a telephone conversation this should be discussed first with the Headteacher.

5.1.2 Use of printers

If printing or scanning documents, ensure that any document containing personal or sensitive information is only printed at a time when you are able to collect it immediately, so as not to leave sensitive information lying on printers / photocopiers. It is advised that photocopiers are used for this purpose as print release is in use on these devices.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities and mobile phones for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The IT & Electrical Manager or Headteacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use of ICT facilities is permitted provided that such use:

- Does not take place during worktime
- 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 should 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 should 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.

Personal mobile phones should not be used in areas of school where pupils have access.

During teaching time, mobile phones should be turned off or put on silent mode and stored in an area away from sight of pupils.

Staff are allowed to access their personal phones on breaks, lunch times and after school in designated areas e.g. staff room (safe, suitable places where the children are not present).

It is forbidden to take photographs / videos of pupils on personal mobile phones.

Staff should 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.

5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times. Remember that damage to professional reputations can inadvertently be caused by quite innocent postings or images.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see Appendix 1).

5.2.2 Communication platforms

Members of staff should consider how they communicate with each other both inside and outside of school when discussing any work matters. This includes during personal time on messaging platforms such as WhatsApp and Facebook Messenger. Remember that what you may deem as 'personal' messages could unintentionally become public and therefore if school matters are being discussed you should consider carefully your use of language and subject matter.

School will always encourage staff that any messages relating to school, even in 'personal' forums should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety. Incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely through Google Workspace for Education.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials onsite. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the school 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.

No school related information should be stored on any personal equipment. You must not download or save any information onto personal equipment such as mobile phones or laptops / pcs.

If you have a need to work offsite and require electronic or paper-based information to be taken from school to work on you must:

- First seek permission from the Headteacher for the removal of the information e.g. pupil file, laptop, encrypted school memory stick
- Ensure the secure transit of the information
- Ensure that no information is downloaded or stored on personal equipment
- Be aware of other people within the immediate area when viewing personal or sensitive information in areas outside of school and limiting such activity away from public places

5.4 School social media accounts

The school has official Facebook, Twitter, Instagram and YouTube pages, managed by appointed communications staff. Staff members who have not been authorised to manage or post to the account, must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.5 Images of pupils

All pupils need parental permission to have photographs or videos published electronically or in a public area even if they are unidentifiable. If in doubt as to whether a pupil has permission you must check with the school office before publishing / displaying.

No photos or videos which include nudity or inappropriate actions are permitted to be taken or downloaded under any circumstance.

Images of students must be stored in the designated area of the ICT network. It is not permitted to remove images off site (on camera, phone or storage device).

Images should be deleted from electronic devices once after uploading to the above storage area.

5.6 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 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. Pupils

6.1 Access to ICT facilities

- Activities should be planned by staff so that 'open searching' is kept to a minimum
- Computers and equipment in school are available to pupils only under the supervision of staff
- When searching the internet with pupils, adults should encourage the children to use 'child safe' search engines if applicable (depending on age)

6.2 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 any 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.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is 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, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Parents

7.1 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) may be granted an appropriate level of access, or be permitted to use the school's facilities at the Headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the school online

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.

8. 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 should use safe computing practices at all times.

8.1 Passwords

Each adult working within the school must log on to the computers using the username and password given to them (individual account) and these must be changed to an individual specific password where stated. Passwords need to be kept a secret, not written down and stored in or around the computer. If for any reason an adult needs to leave their computer, they have to lock the computer to prevent others from using their account.

Any supply teachers or visitors to the school must obtain a guest account and password. Their password will need to be kept private and not shared.

You should ensure you use dual factor authentication when possible if dealing with sensitive information. This is enforced for some services, for example CPOMS and Google Workspace, and encouraged for other services, for example Microsoft Teams.

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.

8.2 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.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy. Our data protection policy requires that any staff or pupil data to which members of staff have access, will be kept private and

confidential, except when it is deemed necessary that by a requirement of law or by school policy to disclose such information to an appropriate authority.

8.4 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 IT Support Team.

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

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

8.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption. Therefore, personal equipment such as USB sticks or other personal devices are not permitted.

9. Internet access

The school's internet connection is secured and content filtering is in operation. If you should happen to access an inappropriate site that the filter has not identified, or 'safe' sites that are filtered in error, please inform the IT Support Team.

9.1 Parents and visitors

Parents and visitors to the school will need to request guest access to use the school's Wi-Fi.

These will only be provided if:

- Parents are working with the school in an official capacity (e.g. as a volunteer 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)

10. Monitoring and review

The IT & Electrical Manager alongside the Director of Business & Finance and Data Protection Officer 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 every year.

The governing body is responsible for approving this policy.

Appendix 1: Social media guidance sheet for staff

Don't accept friend requests from pupils on social media

12 guidelines for school staff on social media

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
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) is able to 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)
11. Consider very carefully any friend requests from parents / carers
12. Never use Facebook to respond to parents / carers regarding queries or questions around school business

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 adds you 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

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
    - Parents sometimes feel that they can contact you through your personal Facebook account to ask questions or raise issues in relation to school. To respond to such communication would be in breach of school policies
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or someone 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 should 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 should consider contacting the police

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Our official Facebook, Twitter and Instagram pages • Email/text groups for parents (for school announcements and information) • Arbor • Google Classroom Sometimes parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
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 social media channels or personal social media to complain about or criticise the school or 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 social media channels 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 the other children's parents/carers	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils	
Name of pupil:	
When using the school's ICT facilities and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Use them to break school rules • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share my password with others or log in to the school's network using someone else's details • Bully other people I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed:	**Date:**

Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors

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

Name of staff member / governor / volunteer / visitor:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Begin to use any new methods of collecting or storing personal or sensitive information- e.g. new apps which require input of pupils personal data without first seeking permission
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school
- Delay in reporting any data breach as set out in the schools Data Protection Policy and breach procedure

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

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and IT & Electrical Manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed:	**Date:**