

Spa Education Trust

ICT and internet acceptable use policy

Approved by:	Steph Lea	Date: 1 st September 2026
Last reviewed on:	September 2026	
Next review due by:	September 2027	

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way the Trust works, and is a critical resource for pupils, staff (including the senior leadership team), trustees, governors, volunteers and visitors.

However, the ICT resources and facilities our school uses could 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/carers and trustees, governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur 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 trustees, governors, staff, pupils, volunteers, contractors and visitors.

This policy is coordinated by the Executive Headteacher, Headteachers and Deputy Heads. They are the Digital Leads across the trust. They work directly with Allied Technical Services (ATS) who provide ICT support across the Trust.

Breaches of this policy may be dealt with under our staff code of conduct.

2. Relevant legislation and guidance

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

- [Data Protection Act 2018](#)
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- [Data \(Use and Access\) Act 2025](#)

- > [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](#)
- > [Education and Inspections Act 2006](#)
- > Keeping Children Safe in Education 2026
- > [Searching, screening and confiscation: advice for schools 2022](#)
- > [National Cyber Security Centre \(NCSC\): Cyber Security for Schools](#)
- > [Education and Training \(Welfare of Children\) Act 2021](#)
- > UK Council for Internet Safety (et al.) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- > [Meeting digital and technology standards in schools and colleges](#)

3. Definitions

- > **ICT facilities:** 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 that may become available in the future which is provided as part of the school's ICT service
- > **Users:** anyone authorised by the school to use the school's ICT facilities, including trustees, governors, staff, pupils, volunteers, contractors and visitors
- > **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- > **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 school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 2 for a glossary of cyber security terminology.

4. Unacceptable use

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

Unacceptable use of the school's ICT facilities includes:

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

- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing any web page or downloading any image, document, application, or file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste, or immoral
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- 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 programme, tool or item of software designed to interfere with the functioning of the school's 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 the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel 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 or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Executive Headteacher will use their 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 (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the executive headteacher's discretion.

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

5.1 Access to school ICT facilities and materials

The school's network is managed by ATS. They manage access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain 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 files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact Head or Deputy in the first instance.

5.1.1 Use of school-supplied equipment

School-issued devices (including laptops, tablets and other digital devices) are provided to staff for the purpose of supporting teaching, learning and the efficient running of the school. All school-supplied equipment remains the property of the school and staff must return the equipment at the end of employment, or when it is no longer required. Staff must:

- Use equipment and devices primarily for school purposes and in line with the school's policies on safeguarding, data protection and confidentiality
- Store devices securely when not in use, particularly when travelling. Devices should not be left unattended in public places or in unsecured locations
- Be actively aware of data security and confidentiality and follow best practice when accessing the equipment away from school. E.g. when travelling on public transport, be aware that other passengers may be able to read any documents displayed on the screen of your device
- Lock devices with a password when unattended. Passwords must:
 - Not be shared with others and must be changed regularly
 - Be suitably strong, in accordance with the school's password policy (see section [8.1])
 - Not be reused across multiple accounts
- Update software, operating systems and applications when prompted, or as directed by the ICT manager
- Connect to the school network using approved and secure methods. When connecting to wi-fi networks outside of the school, staff must ensure connections are secure and avoid transmitting sensitive data over public or unsecured networks
- Report any loss, theft, damage or compromise of a school device promptly to the headteacher, designated safeguarding lead and data protection officer

5.1.2 Use of phones and email

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

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/carers 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 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.

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.

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 that contains the personal information of another person, they must inform Nusrat Raja and Georgina Quigley / Steph Lea immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers 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.

5.1.3 Use of AI including LLM “assistants”

The school has access to Microsoft Co-pilot and this can be accessed by staff as part of their normal ways of working. Identifying information about pupils and staff should not be uploaded nor should sensitive information such as e mail addresses or similar.

Staff should not use ChatGPT or similar LLM software to conduct school business

Staff should teach pupils to be wary of Gemini Google search results and should have the same caution themselves. Gemini has been removed from the school search bar but will continue to provide results to Google Searches

Spa has a separate AI policy and changes will be shared with staff as they are made. It is possible this will be updated more frequently due to the way AI itself is evolving

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The school may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- > Does not take place during contact 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 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 are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's handbook

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/carers could see them.

Staff should take care to follow the school's guidelines on use of 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 make sure 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 social media accounts (see appendix 1).

5.3 Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

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

Only authorised ICT personnel may filter, 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

Trustees are responsible for making sure that:

- The school meets the DfE's [filtering and monitoring standards](#)
- Appropriate filtering and monitoring systems are in place

- Staff are aware of those systems and trained in their related roles and responsibilities
 - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Filtering software is provided by LGfL's School Protect. Monitoring is provided by SENSO's managed service

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

6. Pupils

6.1 Access to ICT facilities

Pupils may use computers at the direction of their class teacher. Any activity that requires the use of the internet should be planned in advance and websites carefully checked. Pupils in KS3 and below should not have access to the internet outside of those websites that are part of the walled garden.

Pupils should be taught how to save and retrieve the work using the shared pupil network, rather than saving documents to class N drives.

Pupils should never be given access to the internet without a member of staff present and monitoring.

Pupils should never use a machine that is logged in with a staff member login.

Pupils should not have their own devices in classrooms and should hand these into reception upon arrival. Pupils should not have their mobile phones in classrooms.

6.2 Unacceptable use of ICT and the internet outside of school

The school will identify and take any necessary actions 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 making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute

- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Parents/carers

7.1 Access to ICT facilities and materials

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

However, parents/carers working for, or with, the school in an official capacity (for instance, as a governor) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents/carers 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/carers 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.

7.3 Communicating with parents/carers about pupil activity

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

We offer regular online safety training for parents and subscribe to Online Safety Weekly to ensure staff are kept informed about this ever-changing landscape.

8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on [digital and technology standards in schools and colleges](#), including the use of:

- Firewalls
- Security features

- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

The trust will ensure the password policy meets National Cyber Security Centre recommendations.

All users of the school's ICT facilities should 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.

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 have these installed, and 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.

The data protection policy is found on SharePoint in the policy folder as well as on our website.

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.

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 DSL or DDSL immediately.

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

The Executive Headteacher has the right to access all staff members email accounts and files based on legitimate organisational need, including business continuity and all aspects of operational need. Where appropriate this access may be delegated to a Headteacher or Deputy headteacher.

Working Remotely

Users working remotely should ensure the confidentiality of all sensitive information is maintained. Information should not be accessed in public spaces. Information should not be saved on personal devices. All devices must be locked / shut down when not in use.

8.5 Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Headteacher or Executive Headteacher

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by ATS

9. Protection from cyber attacks

Please see the glossary (appendix 2) to help you understand cyber security terminology.

The school will:

- Work with Trustees and ATS to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
 - The methods hackers use for tricking people into disclosing personal information, including phishing
 - Online safety and password security
 - Social engineering, including not using websites that host unsuitable material, and could also contain malware and viruses
 - The physical security of devices, for example not leaving a laptop unlocked and unattended
 - The risks of using removable storage media, such as USBs
 - Multi-factor authentication
 - How and when to report a cyber incident or attack
 - How and when to report a data breach
 - Data protection for all staff. Staff who are exposed to higher-risk data will have more frequent training
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
 - **Proportionate:** the school will verify this using a third-party audit (such as [360 degree safe](#)) at least annually to objectively test that what it has in place is effective
 - **Multi-layered:** everyone will be clear on what to look out for to keep our systems safe
 - **Up to date:** with a system in place to monitor when the school needs to update its software
 - **Regularly reviewed and tested:** to make sure the systems are as effective and secure as they can be
- Back up critical data daily and store these backups on cloud-based backup systems
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to ATS
- Make sure staff:
 - Enable multi-factor authentication where they can, on things like CPOMS

➤ Store passwords securely using a password manager

- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Make sure all necessary firewalls are in place and switched on (and that all areas of the network are secured effectively)
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the [Cyber Essentials](#) certification
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify [Action Fraud](#) of the incident. This plan will be reviewed and tested annually and after a significant event has occurred.
- Conduct a cyber risk assessment at least annually, and revisit it every term, or after a significant event has occurred
 - Appoint a digital lead (from the senior leadership team) to oversee cyber risk assessment
-

10. Internet access

The schools' wireless internet connections are secure.

Firewalls are in place and are tested regularly. Pupils have access to a “walled garden”. Any requests for websites to be added to the garden should be made via the Headteacher.

Staff have a responsibility to report any concerns about school filters immediately

11. Monitoring and review

The Executive Headteacher and ATS support manager monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

12. Related policies

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

- Online safety
- Cyber Response Plan
- Safeguarding and child protection
- Behaviour Policy
- Staff handbook
- Code of Conduct
- Data protection
- AI Policy

Do not accept friend requests from pupils on social media

10 rules 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 you don't, make sure 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 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. Check your followers often – block and report if a pupil or parent follows you on social media

What to do if ...

A pupil or parent/carers 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/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- If a parent or carer sends you a message, report this to the head of school
- Notify the senior leadership team or the head of school 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 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/carers 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: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) [glossary](#).

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.

TERM	DEFINITION
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

Spa Education Trust

Acceptable Use Policy

	Name of School	Spa Education Trust
	AUP Review Date	September 2026
	Date of next Review	September 2027
	Who reviewed this AUP?	Georgina Quigley

1. Introduction and aims.

An Acceptable Use Policy (AUP) sets out the roles, responsibilities, and procedures for the acceptable, safe and responsible use of all technologies to safeguard adults, children and young people within a school or other educational setting. The policy recognises the ever-changing nature of emerging technologies and highlights the need for regular review to incorporate development within an area. At present the internet technologies used extensively by young people in both home and school environments include:

- Websites/blogs
- Social networking and chat rooms
- Gaming/forums on Xbox live etc.
- Music downloading
- Mobile phones with wireless connectivity
- Email and instant messaging
- Learning platforms
- Video broadcasting
- Apple/Windows apps.

Despite there being significant educational and social benefits associated with the use of these technologies, there are risks which need to be emphasised to all users and steps taken to safeguard against them. This policy explains procedures for any unacceptable use of these technologies by adults, children or young people and has been developed to ensure staff within Spa are aware of their professional responsibilities when using ICT equipment and systems.

Spa is committed to safeguarding its ICT infrastructure to ensure it can be used in the most effective manner to support teaching and learning and all necessary administrative processes. Ensuring the safety and integrity of the school ICT infrastructure is the responsibility of all staff.

This policy aims to:

- protect the school networks and equipment
- protect the school data
- protect the school and its employees from activities that might expose them to legal action from other parties.
- Prevent disruption to the school through the misuse or attempted misuse of ICT systems.

2. 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 who is authorised by Spa to use the ICT facilities, including trustees, governors, staff and pupils.
- **Personal use:** any user activity that is not directly related to the users' employment, study or purpose.
- **Materials:** Any files and data created using ICT facilities including but not limited to photos, audio, video, printed documents, webpages, social networking sites and blogs.

3. Unacceptable Use

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright.
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing any web page or downloading any image, document, application, or file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste, or immoral
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- 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 school reserves the right to amend this list at any time. The Headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

Acceptable Use Policy (AUP): Staff Agreement Form

Staff

When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements:

- I have read and understand the implications and my personal responsibilities in relation to the use of ICT equipment which is detailed within this policy.
- I will access the internet and other ICT systems using a secure password. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any suspicion or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems to the headteacher/DSL.
- I will not allow pupils to use my login
- I will not write down my log in or password details
- I will ensure that I use a suitably complex password for access to the internet and ICT systems and that I will use a unique password for each system.
- I will seek consent from the ICT manager/DSL/Headteacher prior to the use of any new technologies (hardware, software, cloud-based services) within the school.
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material, I will report it immediately to the DSL or Headteacher.
- I will take a professional and pro-active approach to assessing the effectiveness of the internet content-filtering platform (provided by Senso.Cloud) in relation to the educational content that can be viewed by the pupils in my care.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Manager/DSL/Headteacher (as appropriate).
- I will ensure that all devices taken off site (laptops, tablets, cameras, removal media or phones) will be secured in accordance with the school's data protection registration and any information handling procedures both on and off site.
- I understand my personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information.
- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site. Devices will not be stored in a car overnight or left in sight when not in use.
- I will secure any equipment taken off site for school trips.
- I will only use school-owned or provided portable storage (USB sticks, portable hard drives etc). I will use my One Drive to store information rather than an external device where possible
- I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it without prior authorisation from the ICT manager.
- I will return any school-owned ICT equipment or software to the relevant individual within the school (ICT manager) on or before my last working day if my employment with Spa Education Trust is ending or at any point if instructed to do so by the Headteacher.

- I understand that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and any breach will be reported to the appropriate authorities.
- I understand that my files, communications, and internet activity may be monitored at all times to protect my own and others' safety and action may be taken if deemed necessary to safeguard me or others.
- I understand that if I do not follow all statements in this Acceptable Use Policy relating to the use of ICT equipment, I may be subject to disciplinary action in line with the school's disciplinary procedures.
- I will not use AI LLM software, except for Microsoft Co-pilot. I will not upload any identifying information to any LLM software engine.

Managing digital content

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.
- I will only use school equipment to create digital images, video and sound. Images and video will be of appropriate activities and participants will be in appropriate dress. No resources are to be published online without the permission of the staff and parents/pupils involved.
- Under no circumstances will I use any personally owned equipment for video, sound or images without prior consent from the designated member of staff (DSL/Headteacher)
- Images, videos or sound clips of pupils are stored on the school network and never transferred to personally owned equipment.

Teaching and Learning

- I will support and promote Spa's ICT and Internet Acceptable Use Policy at all times and will model safe and responsible behaviour when using ICT to support teaching and learning.
- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of the misuse of technology by any member of the school community.
- I will ensure that any use of AI is in line with DfE Recommendations: [AI in Education](#) and the school's AI policy
- I will ensure that all internet use by students is carefully planned, only using key stage specific pupil login and that the screen can be viewed at all times
- I will report any concerns immediately if I am worried about the safety of a pupil

Email

- Spa provides each member of staff with an email address which will be used for work purposes only.
- All work-related communication should be conducted using the school provided email address and not a personal one.
- I must not share my personal email address with parents and pupils
- Email messages are required to be disclosed in legal proceedings or in response to a Subject Access Request (SAR) under the Data Protection act 2018 in the same way as paper documents. All emails should be considerate of the content and not include incorrect, improper statements that may give rise to claims of discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Attachments containing sensitive or confidential information should be encrypted so that information is only accessible by the intended recipient using such programs as Egress Switch.

- I will take care in opening any attachments sent by email and will only open emails and attachments sent by trusted senders.
- I will report any data breach immediately to Nusrat Raja and the Headteacher, in line with the whole school policy
- I will record any parent contact, including emails, on CPOMS

Social Media

- I will ensure that my online activity both inside and outside school will not bring my professional role into dispute.
- I will be aware of my digital footprint and exercise caution in my use of social media or other web-based platforms.
- I will not accept or initiate friend requests, nor follow pupils or ex pupils on any social media platform.

Mobile phones and devices

- I will ensure my mobile phone and any other personally owned device is switched off or on silent during school hours.
- I will not contact any parents or pupils on personally owned devices.
- I will not use any personally owned devices to take photos, videos or sound recordings.

Filtering and Monitoring of internet usage

Spa has a responsibility to monitor the use of ICT facilities and networks. The Headteacher at each site is appointed to monitor the use of filtering and monitoring systems. David May is the allocated Trustee responsible for filtering and monitoring.

Monitoring includes, but is not limited to:

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

Only authorised members of staff may inspect, monitor, intercept, assess, record and disclose the above.

Agreement

I have read and understood the Spa School staff and Volunteer Acceptable Use Policy relating to my use of technology within school. I understand that if I fail to comply with this agreement that I could be subject to disciplinary action.

Name:

Role:

Signed

Date

Pupils

This will be shared with pupils as appropriate

Access to ICT facilities

- Students have access to computers and equipment in school. These are available for use under the conditions set out in the Acceptable Use Policy.
- Students are provided with a school email address for the purposes of school-related activities.

Unacceptable Use of ICT and the Internet Outside of School

The school will respond to any unacceptable use by pupils in line with the Behaviour Policy. This includes any of the following at any time that are school related (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright.
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- 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 school network, or to any password protected information.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities.
- Causing intentional damage to school 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.

Agreement

I have read the online safety rules with my parent/guardian, and I understand the importance of being safe online.

Pupil's name:

Class:

Date: