Spa Education Trust
Acceptable Use Policy

Name of School	**Spa Education Trust**
AUP Review Date	**February 2026**
Date of next Review	**February 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.
- 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 school reserves the right to amend this list at any time. The Headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4. 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 take 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 were 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.

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. ages 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 Online Safety 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, breech 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 ………………………...

5. 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: ……………………...................................