Special Partnership Trust

STAFF AND VOLUNTEER ICT ACCEPTABLE USE POLICY

Date Last Reviewed: September 2026

Review Date: September 2027

Staff and Volunteer ICT Acceptable Use Policy

This should be read in conjunction with the Trust's Child Protection & Safeguarding Policy, Staff Code of Conduct, Data Protection Policy, Mobile Phone and Personal Devices Policy, and Disciplinary Policy.

1. Policy Statement

The Special Partnership Trust's ICT resources are provided primarily to enable employees, volunteers and other authorised users to carry out their duties effectively, safely and securely. The Trust values its ICT systems, information and data as important educational and business assets.

The objectives of this policy are to ensure as far as reasonably possible, that:

- the Special Partnership Trust's ICT systems, including email, internet access, networks, devices, applications and cloud-based services, are used safely, securely and effectively;
- pupils, staff, volunteers and other users are protected from accidental or deliberate misuse of technology;
- Trust information and personal data are appropriately protected;
- staff and volunteers maintain professional boundaries when using technology;
- the Trust is protected from legal, financial, operational, safeguarding or reputational harm arising from the inappropriate use of its ICT facilities; and
- the Trust meets its safeguarding, data-protection, cyber-security, employment and regulatory responsibilities across all its schools and services.

2. Scope

This policy applies to:

- all Trust employees, including temporary, casual and supply staff;
- volunteers, agency workers and individuals on placements or secondment;
- any person given permission to access Trust ICT systems, networks, accounts, devices or information; and
- the use of Trust systems and information both on and away from Trust premises.

The policy applies to Trust-owned or managed equipment, accounts, networks, applications and services. It also applies to personal devices where these are used on Trust premises, connected to a Trust network, used to access Trust information, or used for communications connected with Trust duties.

Employees may also be subject to the Trust's Staff Code of Conduct and disciplinary procedures. Where concerns relate to a volunteer, contractor, agency worker or other non-employee, the Trust will consider the appropriate action under the relevant agreement, placement or contractual arrangements.

3. Roles & Responsibilities

Trust leaders, Designated Safeguarding Leads, the Data Protection Officer and the Trust's managed ICT provider are responsible for ensuring appropriate safeguarding, filtering, monitoring, cyber security and data-protection arrangements are in place. All users are responsible for complying with this policy and reporting concerns promptly.

4. General acceptable-use agreement

I understand that I must use Trust ICT systems in a responsible way and not create unnecessary risks to pupils, colleagues, other users, Trust information or the security and operation of the Trust's systems.

I recognise the value of technology in enhancing teaching, learning, communication and the effective delivery of Trust services. I will promote safe and responsible online behaviour and will embed online safety in my work where this forms part of my role.

Staff working directly with pupils are expected to model safe and responsible online behaviour and to support pupils to develop online-safety knowledge, understanding and behaviours appropriate to their age, communication needs, cognitive understanding and stage of development.

I will comply with any additional Trust instructions, technical controls or guidance introduced in response to changes in legislation, statutory guidance, safeguarding risk, cyber-security threats, technology or operational requirements. If I am uncertain whether a proposed use of technology is permitted, I will seek advice from the Trust before proceeding.

4.1. **Professional Use of Trust Systems**

I will:

- use Trust ICT systems, accounts, devices and online services responsibly, professionally and only for authorised purposes;
- I will immediately report any safeguarding, cyber-security, data-protection or online-safety concern through the appropriate Trust reporting route;
- use only the accounts and access permissions allocated to me;
- keep usernames, passwords and authentication information secure and report any suspected compromise immediately;
- use strong passwords and any additional security measures required by the Trust;
- lock devices whenever they are left unattended;
- access information only where I have a legitimate work-related reason and authority to do so;
- communicate professionally and respectfully when using Trust email, messaging platforms, video conferencing systems and other digital communication tools;
- maintain appropriate professional boundaries with pupils, families, colleagues and other users;
- use approved Trust systems, accounts and devices when communicating with pupils or families as part of my role;
- promote safe and responsible online behaviour and model appropriate use of technology.

I will not:

- disclose my password, authentication code or security credentials to another person;
- attempt to access another user's account or information without authority;
- access information about pupils, families, colleagues or other individuals out of curiosity or for an unauthorised purpose;
- use abusive, threatening, discriminatory, harassing or otherwise inappropriate language;
- use a personal email account, personal telephone number, social-media account or unapproved messaging application to communicate with pupils;
- initiate or accept personal social-media contact with current pupils;
- use disappearing-message functions or communication methods that prevent an appropriate Trust record being retained;

- disclose confidential information or discuss pupils, families, colleagues, employment matters or Trust business without authority;
- impersonate another person or misrepresent my identity, authority or the Trust's position;
- operate a private business, undertake unauthorised commercial activity, gamble online or participate in illegal file sharing using Trust systems; or
- engage in online activity, whether at work or outside work, that could reasonably compromise safeguarding, professional standards, working relationships, public confidence or the reputation of the Trust.

I understand that online activity undertaken outside work may become public and may have implications for my professional responsibilities. Personal views expressed online must not be presented as the views of the Trust, and privacy settings should not be relied upon to guarantee confidentiality.

I understand that access to Trust systems and information is based on my role and may be amended, restricted or withdrawn where appropriate. I also understand that use of Trust systems, accounts and communications may be monitored in accordance with Trust policies and legal requirements.

4.2. Personal Devices, Images and Recordings

I will:

- comply with the Trust's Mobile Phone and Personal Devices Policy;
- keep personal devices secure and use them only in accordance with local school or setting requirements;
- not allow pupils to use my personal devices;
- not connect personal devices or removable media to Trust systems without authorisation;
- immediately report the loss, theft or suspected compromise of any device containing, or capable of accessing, Trust information;
- use only Trust-owned or approved equipment to create photographs, audio recordings or video recordings for Trust purposes;
- ensure appropriate permissions, restrictions and safeguarding considerations are followed before creating, using, storing, sharing or publishing images or recordings;
- store images and recordings only within approved Trust systems;

- not store, transfer or access Trust confidential information, personal data, images or recordings using personal devices, personal accounts, personal applications or personal cloud services unless specifically authorised and appropriate security controls are in place;
- take reasonable steps to avoid recording individuals unintentionally; and
- not edit, manipulate, retain, share or publish images or recordings in a misleading, inappropriate or unauthorised manner.

I will not:

- use a personal device to photograph, film or record pupils or Trust activities unless expressly authorised by the Trust;
- transfer images or recordings to personal devices, personal accounts, storage services or social-media platforms; or
- use photographs, recordings or digital content in any way that could compromise safeguarding, confidentiality, dignity or professional standards.

Any publication or wider sharing of photographs, audio recordings or video recordings must be separately authorised and comply with Trust safeguarding, consent, data-protection and image-use arrangements.

Where the Trust authorises the use of a personal device for work, users must comply with any security requirements specified by the Trust. Reasonable adjustments involving personal or assistive technology will be considered where appropriate.

4.3. Data Protection, Information Security and Incident Reporting

I will only access, use, share or store personal and confidential information where this is necessary for an authorised Trust purpose and permitted under Trust policies and procedures.

I will:

- protect personal, safeguarding and confidential information and handle it securely;
- use Trust-approved systems and services to create, store and share Trust information;
- verify recipients before sending information and ensure only the minimum necessary information is shared;

- use appropriate security measures, including encryption where required;
- use the BCC field where appropriate when emailing multiple external recipients;
- comply with the Trust's data-protection, retention and secure-disposal requirements;
- report actual or suspected data breaches, cyber-security incidents or unauthorised disclosures immediately;
- preserve evidence and cooperate with any safeguarding, technical or data-protection investigation.

I understand that Trust records, including emails, messages and system activity, may be disclosed where required in connection with safeguarding investigations, disciplinary or grievance proceedings, legal proceedings, regulatory enquiries, subject access requests, Freedom of Information requests or other lawful requirements.

4.4. Generative artificial intelligence

Staff may only use Trust-approved AI tools. Personal data, safeguarding information, confidential information, passwords or commercially sensitive information must not be entered unless specifically authorised. Users remain responsible for checking the accuracy, appropriateness and legality of AI generated content and must not rely on AI as the sole basis for decisions affecting pupils, staff or volunteers.

4.5. Software, applications and cloud services

I will not:

- install, copy, download or run software, browser extensions or applications without authorisation;
- change security, network or device settings without permission;
- register for an online service using a Trust email address where the service has not been approved for Trust use;
- create an online account for a pupil without appropriate authority and consideration of age, privacy and safeguarding requirements;
- use an unapproved cloud service to process or store Trust information;
- disable or damage Trust equipment or equipment belonging to another person; or
- make large downloads or uploads that unreasonably affect network capacity

unless agreed in advance with ICT support.

- New technology, applications and online services must be subject to the Trust's approval and procurement processes, including appropriate consideration of safeguarding, accessibility, cyber security, contractual terms, data protection, international transfers, retention and supplier access.

4.6. Filtering and monitoring

The Trust operates appropriate filtering and monitoring arrangements across its networks and managed devices in accordance with KCSIE and relevant DfE standards. Filtering is intended to help prevent access to illegal, inappropriate or harmful content. Monitoring supports the identification and management of potentially harmful activity.

I will:

- not attempt to disable, bypass, evade or interfere with filtering, monitoring or security arrangements;
- not use a virtual private network, proxy, personal hotspot, unauthorised browser, application or other method to circumvent Trust controls;
- never allow a pupil to use staff access, staff credentials or any facility intended to provide a different level of internet access;
- follow the authorised process where access to a blocked resource is required for a legitimate educational or business purpose;
- report any apparent failure, over-blocking, under-blocking, inappropriate access or safeguarding concern promptly; and
- not assume that material is appropriate merely because it has not been blocked by the Trust's filtering system.

Filtering and monitoring do not replace professional supervision, safeguarding vigilance or the responsibility to check that resources are appropriate before they are used with pupils.

Staff remain responsible for ensuring resources are appropriate for the pupils they support, taking account of age, SEND needs, communication abilities and potential online risks. The Trust will review filtering and monitoring arrangements regularly to ensure they remain effective and appropriate.

4.7. Internet content and copyright

I will:

- use internet access for authorised educational, professional or reasonable personal purposes;
- check the accuracy, suitability, provenance and reliability of online material before using it;
- ensure that resources used with pupils are appropriate to their age, needs and stage of development;
- obtain appropriate permission or rely on an applicable licence or legal exception before using the work of another person;
- acknowledge sources where required; and
- comply with copyright, licensing and intellectual-property requirements.

I will not knowingly create, search for, access, upload, download, store, send or share:

- illegal content;
- content that presents a safeguarding, radicalisation, abuse or exploitation concern;
- material that is discriminatory, threatening, harassing or likely to cause harm;
- malicious software or material intended to compromise a device, account, network or service;
- content that infringes copyright or other intellectual-property rights; or
- other material prohibited by law or Trust policy.

This includes, but is not limited to, child sexual abuse material, terrorist or extremist content, material promoting radicalisation, pornography, criminally racist material, hate content, content encouraging violence, abuse, exploitation or self-harm, and material that may place children, young people or vulnerable individuals at risk.

Unintentional access to concerning content will not, by itself, be treated as misconduct where the individual stops further access and immediately follows the reporting requirements in this policy.

4.8. Safeguarding concerns and harmful content

If I encounter illegal, harmful, inappropriate or otherwise concerning content, or become aware of unsafe online activity, including content or activity linked to extremism, radicalisation, terrorism, hate crime, child abuse, exploitation, self-harm or

online grooming, I will:

- stop further viewing or interaction;
- prevent pupils or others from seeing the content where this can be done safely;
- preserve the device and any available evidence;
- report the concern immediately to the Designated Safeguarding Lead and ICT support using the appropriate reporting routes;
- provide an accurate factual account; and
- follow any instructions given by the DSL, ICT support, senior leadership or law-enforcement professionals.

I will not:

- forward, share, download, copy, print or screenshot the content;
- undertake further searches;
- delete browser history, messages, files or other potential evidence;
- question pupils or colleagues beyond what is immediately necessary to establish that a concern exists; or
- attempt to investigate the matter myself.

Users must not delete internet history, messages, logs, files or other records where these may be relevant to a safeguarding, disciplinary, data-protection, cyber-security or other investigation. Relevant devices, information and records must be preserved and reported through the appropriate Trust procedure.

Where the concern relates to the conduct of an adult working with children, it must be reported through the Trust's managing allegations or low-level concerns procedure, as appropriate.

Staff must not investigate the concern or discuss it more widely than necessary.

Concerns relating to possible radicalisation must be treated as safeguarding concerns and referred through the Trust's safeguarding procedures. The Trust recognises that online activity can be a source of radicalisation risk. Staff must remain alert to indicators of extremist ideology, terrorist influence, online grooming and other harmful influence. Decisions will be risk-based, proportionate and consistent with the Prevent duty, data-protection obligations and the Equality Act 2010.

4.9. Remote and flexible working

The requirements of this policy apply equally when working on Trust premises, remotely, at home or at any other location. Users must ensure that Trust information, devices and communications remain secure and confidential at all times.

5. Limited personal use

Trust ICT systems are provided primarily for educational and business purposes. Limited and reasonable personal use may be permitted during non-working time where it:

- does not interfere with duties, productivity or the operation of Trust systems;
- does not create additional cost, security risk or legal liability;
- does not involve prohibited, unlawful, commercial or inappropriate activity;
- does not breach this or another Trust policy; and
- does not involve using a Trust email address to register for unnecessary personal or commercial services

The Trust may withdraw permission for personal use where this is necessary or appropriate.

6. Monitoring and privacy

The Trust may monitor the use of its ICT systems, networks, devices and communications for safeguarding, security, legal and operational purposes. Monitoring will be lawful, proportionate and carried out in accordance with data-protection legislation.

7. Responding to potential breaches

Actual or suspected breaches of this policy will be considered fairly and proportionately, taking account of the circumstances of each case.

Breaches may be addressed through the Trust's disciplinary procedures, safeguarding procedures, contractual arrangements or referral to external agencies where appropriate, including the police, DBS, TRA, ICO or Children's Social Care.

Any suspension will be considered on a case-by-case basis, used only where necessary and treated as a neutral precautionary measure.

8. Equality, accessibility and reasonable adjustments

The Trust will implement this policy consistently and in accordance with the Equality Act 2010.

Where a disabled employee, volunteer or other authorised user requires assistive technology or a reasonable adjustment affecting the use of ICT or personal devices, the Trust will consider appropriate arrangements with the individual, their manager, HR and ICT support. Adjustments must be compatible with safeguarding, data-protection and cyber-security requirements, but will not be unreasonably withheld.

9. Training, assurance and review

Staff and volunteers will receive appropriate information, instruction and training about acceptable use, online safety, cyber security, data protection, safeguarding and incident reporting. Additional training may be required for users with specialist responsibilities or privileged access.
The Trust may require users to refresh their acceptance of this policy following a review, a substantive amendment, a change in role or a relevant incident.

This policy will be reviewed at least annually and sooner where there is a material change in legislation, statutory guidance, safeguarding risk, technology, cyber-security threats or Trust arrangements.

ACCEPTABLE USE DECLARATION

I confirm that:

- I have read and understood this Staff and Volunteer ICT Acceptable Use Policy;
- I understand that the policy applies to my use of Trust systems and equipment both on and away from Trust premises;
- I understand that relevant requirements also apply to my personal devices and accounts where they are used on Trust premises, connected to Trust systems or used for Trust-related activity;
- I understand my responsibility to protect pupils, colleagues, Trust information and ICT systems;

- I will comply with the Trust's policies, procedures, technical controls and lawful instructions;
- I will seek advice where I am unsure whether an activity is permitted;
- I will report safeguarding, data-protection and cyber-security concerns promptly; and
- I understand that a failure to comply may result in action under the appropriate Trust procedure or contractual arrangement.