

SHERBORNE AREA SCHOOLS' TRUST



Staff and Volunteer ICT Acceptable Use Policy Including Virtual Classroom Delivery

Revised	January 2023
Review due	January 2025
Author	Head of IT DPO

SAST Document Control Table			
Document Title		Staff and Volunteer ICT Acceptable Use Policy Including Virtual Classroom Delivery	
Author		Head of IT DPO	
Version No.		5	
Date Approved			
Approved By			
Date of Next Review		November 2024	
Version		Document History	
	Date	Author	Notes of Revisions
1	Mar 2018	IT Lead	N/A
2	May 2020	DPO	New paragraph regarding virtual classroom and data protection.
3	Jan 2021	DPO	Addition of section regarding the use of cameras during virtual lessons.
4	Nov 2022	DPO	Retitled to 'Staff and Volunteer' to include those with governor, trustee and member roles. S3; use of SAST email for personal purposes is now not permitted to align with Data Protection and FoI Policy. S4; removal of reference to SWGfL S5; compromised passwords also to be reported to the Data Protection Officer. S6; first sentence regarding conduct made clearer. S8; updated from General Data Protection Regulation 2016 (GDPR) to 2020 and Data Protection Act 2018 added. Inclusion of area for signature by LGB representative, trustees and members as volunteers. Addition of 'My Responsibilities' section
1.5	Aug 2023	DPO	6. Obligation to comply with consent with regard to recording of others by audio or via images.

1. Purpose

This Staff and Volunteer ICT Acceptable Use Policy is aimed at encouraging responsible behaviour and good practice. It has been created with the view to:

- Ensure compliance and enforcement of relevant legislation which includes but is not limited to the Computer Misuse Act 1990, General Data Protection Regulation 2016 and the Data Protection Act 2018.
- Ensure the safety and integrity of pupils, staff and others;
- Prevent damage to our schools and physical property;
- Ensure that staff and volunteers have access to technology to enable efficient and effective work practice, enabling learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users.

2. Policy Statement

SAST reserves the right to amend this Staff and Volunteer ICT Acceptable Use Policy, at any time, without notice. It is your responsibility to ensure that you are up to date with such changes. This policy replaces and supersedes all previous versions.

3. Electronic mail (Email)

All members of staff and individuals with governance, trustee or members roles will be provided with email services for school-related communication. Caution should be exercised when sending confidential information via e-mail - email containing confidential information should be encrypted before sending and confidential attached files must be password-protected. The transmission of confidential information via e-mail to unauthorised persons is strictly prohibited. Any email sent to multiple recipients must be sent using the "BCC" field whenever possible to ensure personal email addresses are kept confidential from other recipients. The use of email for personal purposes is not permitted. While SAST respects the privacy of staff, governors and volunteers, where there is reason for concern, the school reserves the right to monitor and intercept email communication. The content of any email communication made must not bring SAST into disrepute; this includes, but is not limited to, content which could be construed as libellous, defamatory, criminal and that which is distributed in breach of data protection law.

4. Internet Access

SAST will only provide access to the internet on receipt of a signed Staff and Volunteer ICT Acceptable Use Policy Acknowledgement slip. All Internet access is logged for the purposes of maintaining standards of security and policy compliance. Attempts to access inappropriate websites or websites which attempt to bypass filtering systems constitute a breach of this ICT Acceptable Use Policy. Inappropriate websites include, but are not limited to any site which contains:

- Pornographic Material (of either a legal or illegal nature);
- Material which incites hatred or discrimination;
- Material which promotes illegal activity;
- Material which is in breach of the Copyright Designs and Patents Act 1998;
- Material which is offensive or degrading to persons or groups of persons;

Staff are required to report any website that they become aware of, which is not filtered, that is deemed inappropriate. Staff should refrain from downloading large files during school hours as this may affect the quality of service for other users. While the Trust internet filtering systems uses sophisticated filtering technology and takes all precautions to ensure that users only access appropriate material, it is not possible to guarantee that unsuitable material will be inaccessible. SAST cannot accept liability for the material accessed, or any consequences of such access.

5. Network Access

Staff or volunteer logins must only be used by those to whom they are issued to. Liability remains with the logged in user. Allowing another person to use your login is a breach of this Staff and Volunteer ICT Acceptable Use Policy

and contravenes Computer Use legislation. Pupils must not use staff logins under any circumstance. Passwords must never be divulged to anyone at any time. If it is suspected that a password has been compromised it must be notified to IT Support and changed immediately and also reported to the Data Protection Officer as a data breach. Staff and volunteers are not permitted to download or install software onto the network or IT equipment. It is prohibited to copy any software or inappropriate material on to the network. Staff and volunteers will not store confidential material on network areas which are accessible to persons who do not have clearance to access such material. Staff and volunteers understand that SAST reserves the right to remotely monitor and intercept network activity. Staff and volunteers should understand that any attempt to bypass SAST or other network security systems, including the introduction of viruses or applications of a destructive nature could lead to prosecution. Where it is believed that a member of staff or volunteer in breach of legislation, appropriate action will be taken.

6. Data Protection

All conduct by staff while using SAST ICT equipment, for any use, must be in accordance with the SAST Data Protection Policy and UK GDPR and the Data Protection Act 2018. This includes, but is not limited to, compliance with rules around consent with regard to recording of others by audio or via images, security of passwords, securing and encrypting electronic files with passwords if they are shared, securing data storage devices by logging out or locking the computer, tablet or portable devices when not in use. Any hardcopy data converted to or from electronic form via a scanner or photocopier must be similarly kept secure. No data relating to pupils, parents, governors or staff (Data Subjects) may be stored on personal devices. Access to remote servers or other Cloud data storage via the internet will be provided by SAST.

7. Virtual Classroom

This guidance should be read in conjunction with DFE guidance on remote education practice for schools, the SAST Staff Code of Conduct, Pupil ICT Acceptable Use Policy and the schools' Safeguarding Policy available at www.sast.org.uk.

Live and pre-recorded lessons can be particularly useful when staff, or pupils, are absent from school for extended periods. As with all lessons, the principles behind their use must be underpinned by clear safeguarding guidelines in order to protect staff, pupils and families.

All virtual lessons must be:

- conducted using software approved by SAST;
- recorded on cloud-based SAST drives;
- agreed by a member of the school's SLT;
- open to members of the school's SLT so they may conduct unannounced "drop-ins".

Ideally virtual lessons should be:

- conducted from the school. If this is not possible and therefore the lesson is being conducted from a member of staff's home the lesson should not be conducted from a bedroom or other personal space;
- Conducted using school equipment. No element of a live lesson should be recorded on a member of staff's personal equipment or school equipment, only cloud-based SAST drives.

Pupils must be:

- made aware that if they are taking part in a live lesson and if recorded, they must give their consent to this if they are 12 years or over. For pupil's under 12 years, consent must be obtained from the parent/carer. If permission is not granted then the pupil cannot take part in the live lesson;
- over 12 years of age if they are to take part in a live lesson without an adult present in their household. The parent / carer present in the household, for a child under 12, must give their permission for the child to take part, if this permission is not granted then the child cannot take part in the live lesson;
- in a public area of the house i.e. must not be closed off from the rest of the household and must be visible to a parent / carer at any point during the lesson;
- appropriately dressed;

- aware the school's Behaviour for Learning Policy applies to virtual lessons and that inappropriate behaviour could lead to them being asked to leave the lesson. Teachers will follow up poor behaviour at a later point with the pupil and their parent / carer;
- made aware that cameras must be switched on for the whole of the lesson.

Teachers leading live lessons should:

- Make a note of the date and time of each live lesson
- Note the class invited or the names of individuals invited if the lesson is not for a whole class
- Note any issues that arose with the lesson and refer these to other staff as appropriate.

Seniors leaders in the school should:

- Drop into live lessons – unannounced – to conduct safeguarding checks;
- View a sample of recorded lessons for quality assurance and safeguarding checks;
- Obtain feedback from staff, pupils, parents and carers as to the effectiveness of virtual lessons.

Recordings of live teaching sessions remain the property of the school and under no circumstances must they be stored on personal ICT equipment or distributed without the express permission of the school.

8. Legislation

All network users (including but not limited to, staff, pupils and governors) are bound by SAST policies and current relevant legislation. The applicable laws include, but are not limited to:

- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1998
- Criminal Justice Act 1988
- Data Protection Act 2018 &
- Defamation Acts 1952 and 1996
- Freedom of Information Act 2000
- General Data Protection Regulation 2020 (GDPR)
- Data Protection Act 2018 (UK GDPR)
- Human Rights Act 1998
- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1988
- Protection from Harassment Act 1997
- Public Order Act 1986
- Race Relations Amendment Act 2000
- Telecommunications Act 1984
- Sex Discrimination Act 1986
- Regulation of Investigatory Powers Act (RIPA) 2000

9. ICT Equipment and Suites

Staff may not move or authorise any person to move any ICT equipment. Staff may not pass on any ICT equipment to any other person. It must first be passed back to the ICT Support department and then reissued. Any equipment issued to staff or volunteers remains the property of SAST and must be returned upon request. Upon termination of employment at SAST all equipment must be returned. Staff are responsible for all equipment issued to them and must take reasonable precautions to protect such equipment, including complying with insurance and data protection law by securing equipment at all times. Staff are responsible for all equipment and use of workstations by pupils during their lessons in ICT Suites. Staff must ensure that ICT Suites are locked upon leaving the room. Pupils should not be allowed access to keys to ICT Suites at any time. Staff should report unlocked ICT Suites. No pupils may be allowed to use ICT Suites without suitable supervision by a member of staff. (This does not apply to sixth form students using sixth form suites).

10. Personal Use of ICT Equipment

The computers and other ICT equipment provided by SAST are for business use to assist staff in the performance of their jobs. Limited, occasional or incidental use of the equipment for non-business purposes is accepted by SAST, however, all such use should be undertaken in a manner that does not negatively affect the equipment's use for business purposes. Staff are expected to demonstrate a sense of responsibility and not abuse this privilege.

11. Additional Systems

Members of staff may have access to additional systems. These systems require additional passwords. It is the responsibility of the member of staff to ensure that their password has basic complexity to it and that their password is only known by them.

12. Sanctions

In the event that this Staff and Volunteer ICT Acceptable Use Policy is breached, staff will be subject to sanctions which may include, but are not limited to:

- Disciplinary procedures;
- Temporary or permanent restriction of network access;
- Temporary or permanent revocation of network rights;
- Restriction to or denial of access to ICT Suites;
- Investigation under the Regulation of Investigatory Powers Act (RIPA) 2000.

Key Point Summary

The aim of the policy is to protect both staff, volunteers and pupils/students when using ICT equipment.

The document covers:

- E mail usage
- Internet Usage
- Network Access
- Data Protection
- Virtual Classroom
- Key Legislation
- ICT Equipment and Suites
- Personal Use of ICT equipment
- Additional Systems
- Sanctions

With large quantities of pupil and staff data held on our systems, and wide internet access for staff, it is important that users are responsible. This includes:

- Reporting any incidents which occur to the ICT team and/or the Data Protection Officer / Designated Safeguarding Lead so that they can be dealt with quickly and appropriately
- Not letting pupils use staff user accounts
- Not leaving pupils to work unsupervised on machines which are connected to the school network.
- Locking the machine you are using if you need to leave the room temporarily and logging out if leaving for longer
- Respecting bans that pupils may have been given for previous misuse.

If you have any concerns regarding computer usage, please talk to Neil Burroughs (SAST Head of IT Infrastructure).

My Responsibilities

I agree to:

- read, understand, sign and act in accordance with the school Data Protection Policy and UK GDPR
- report any suspected misuse or concerns to the Data Protection Officer or Head of IT
- monitor technology activity in lessons, extracurricular and extended school activities, including awareness of any access to extremist views
- model the safe and effective use of technology
- demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with school ethos and policies especially at the time of a Critical Incident

Education

I agree to:

- provide age-appropriate online safety learning opportunities as part of a progressive online safety curriculum; and reinforce the learning throughout the school's curriculum
- respect copyright and educate the pupils to respect it as well
- teach about the need for using responsible and caring language when communicating with others

Training

I agree to:

- participate in online safety training
- request training if I identify an opportunity to improve my professional abilities

Online bullying

I agree to:

- ensure the Trust's zero tolerance of bullying is adhered to. In this context, online bullying is seen as no different to other types of bullying
- report any incidents of bullying in accordance with school procedures

Sexting

- I will secure and switch off any device discovered with a sexting image and report immediately to the safeguarding lead.
- I will not investigate, delete or resend the image.

Prevent

- I will continually develop children's ability to evaluate information accessed online.
- I will follow the agreed reporting procedure where children are purposefully searching for inappropriate sites or inadvertently accessing inappropriate sites.

Technical Infrastructure

I understand that the Trust will monitor my use of computing devices and the internet. Unless I have permission, I will not try to by-pass any of the technical security measures that have been put in place by the Trust which include:

- the proxy or firewall settings of the Trust's network;
- not having the rights to install software on a computer;
- not using removable media e.g. memory sticks.

Passwords

- I will only use my own passwords;
- I will never log another user onto the system using my login.

Filtering

- I will not try to by-pass the filtering system used by the Trust;
- If I am granted special access to sites that are normally filtered I will not leave my computer unsupervised;

- I will report any filtering issues immediately.

Data Protection

- I understand my responsibilities towards the data protection regulations and will ensure the safe keeping of personal and sensitive personal data at all times;
- I will ensure that all data held in personal folders is regularly backed up and kept secure;
- If I believe there has been a loss of personal or sensitive data, I will immediately report it to the SAST Data Protection Officer or school's Senior Information Risk Officer (usually the headteacher).
- I will comply with UK GDPR and the DPA 2018 and will not record others without their consent.

Use of digital images, video and sound

- I will follow the Trust's Data Protection policy when using digital images, video and sound, especially in making sure that only those pupils whose parental permission has been given are published;
- I will not use personal devices for taking or sharing digital images or sound.

Communication

- I will be professional in all my communications and actions when using the Trust's technology systems;
- I understand that I need to be open and transparent in all my communications.

Email

- I will use the Trust provided email for all business matters;
- I will not open any attachments to emails, unless the source is known and trusted (due to the risk of the attachment containing viruses or other harmful programmes).

Social Media and Personal Publishing

- I will ask permission before I use social media e.g. blogs, social networks or online communication tools with pupils or for other school related work. These will never be my personal accounts;
- I will check with the SLT before I use sites/apps with learner log ins to ensure that any pupil personal data is being held securely;
- I will follow policy concerning the personal use of social media, never publishing disparaging or harmful comments or expressing extreme views. These are considered to bring the Trust into disrepute;
- I will not post any comments about the Trust, any school, any pupil, employer or colleagues on any personal social networking and publishing accounts;
- When there is a Critical Incident, I will not post any comments online.

Personal devices

- I will not use personal devices during contact time with pupils. They will be turned off at other times;
- I will check that any personal devices I have in school are pin code or fingerprint protected and not discoverable by third parties;
- I will not use my personal devices to contact pupils or parents;
- I am responsible for any use of my own technology and ensuring that my use complies with the Trust's policies.

Reporting incidents

- I will report and record any incidents relating to online safety to the Data Protection Officer / Designated Safeguarding Lead and check actions taken have been recorded
- I understand that in some cases the Police may need to be informed.

Sanctions and Disciplinary procedures

- I understand that there are regulations in place when pupils use technology and will apply sanctions if they do not follow the rules.
- I understand that if I misuse the Trust's technology systems in any way then there are disciplinary procedures that will be followed.

Staff and Volunteer Agreement

I have read and understand the SAST Staff and Volunteer ICT Acceptable Use Policy and agree to use the Trust's technology systems, both in and out of school, and my own devices (in school, and when carrying out communications related to Trust business) in a responsible and professional manner as outlined in this document.

I understand that should I be found in breach of this policy I may be liable to disciplinary procedures and, if appropriate, the Police and local authorities may become involved.

I understand my personal responsibilities in terms of preserving data privacy under UK data protection law and the GDPR.

Staff Name	
Volunteer Name (LGB representatives, Trustees, Members)	
Signature	
Date	