South Gloucestershire and Stroud Academy Trust (SGSAT)

IT Acceptable Use Policy - Users

If you would like this document in an alternate format

Please contact the Human Resources Department

Prepared by:	Tim Hanks
Job Title/Role:	Group IT Director
Ref. No.: **Q/P 148**	**Date of this version:** 07/11/2022 **Review date:** 01/11/2024 (Subject to any legislative changes) **Upload to website?** No **Upload to e-Campus?** No
Approved by:	SGSAT Trust Board
Date:	23/11/2022

Policy Template

1. Policy Intent

1.1. The intention of this document is to ensure users of SGS Academy Trusts (SGSAT) Digital and Information Technology (IT) resources have a clear understanding of what is acceptable usage.

1.2. It is also to inform users that SGSAT reserves the right to investigate computer use or digital activity that is suspected to be detrimental to any persons, service or network or to be in breach of this document or any other relevant SGSAT policy.

2. Scope

2.1. This policy applies to all users of SGS Academy Trusts (SGSAT) IT and digital facilities (including software) owned, leased or hired, on or off premises.

3. Procedures

3.1. Legal Framework

3.1.1. The use of the IT and digital facilities and resources are subject to the provisions of the following Acts:

- Data Protection Act 2018
- Copyright Designs and Patents Act 1988
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000
- Digital Economy Act 2010
- Human Rights Act 1998
- And any regulations made pursuant to these Acts.
- Where appropriate offences may be reported to the Police for further investigation.

3.2. Authorisation

3.2.1. Access to IT and digital facilities and resources is restricted to members of SGSAT.

3.2.2. Other users may be authorised via IT Services (e.g. visiting lecturers).

3.3. Registration of user access

3.3.1. Use of the facilities is conditional upon individuals being registered centrally within SGSAT's management information systems. Once this

has been successfully completed a username and password will be generated.

3.3.2. Access to systems and services is role based and governed by type of user and organisational role.

3.4. Termination of user access

3.4.1. At the point an account holder no longer appears within the data provided by the organisations management information systems the account will be disabled and user files archived. Accounts will be manually deleted as part of a check process to ensure no errors have occurred.

3.5. Password Policy

3.5.1. All user passwords will be a minimum of 8 characters with staff having a requirement to use “complex” passwords which means that passwords must contain characters from three of the following five categories:

- Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

3.5.2. For users or departments requiring password management solutions to securely store usernames and passwords for business related use “KeePass” is the approved mechanism for doing this. Please speak to IT Services for further guidance.

3.6. Access to facilities

3.6.1. Access to on-site IT and digital facilities is during published site opening hours.

3.6.2. Although some systems are available remotely, 24/7 this is provisioned as “best endeavour” with some systems being updated out of normal working hours regularly.

3.6.3. All access is subject to facilities maintenance requirements.

3.7. Use of IT and Digital Facilities

3.7.1. Users must not in any way cause any form of damage to SGSAT’s computing equipment or software, nor to any of the rooms and the facilities and services which contain that equipment or software; nor to

any of the network wiring infrastructure or communications equipment. The term "damage" includes modifications to hardware, software or infrastructure which, whether or not causing harm to the hardware or software, incur time and/or cost in restoring the system to its original state. All costs associated with repairing or replacing damaged equipment or software and/or in providing temporary replacements will be charged to the person or persons causing the damage. The costs will be determined by SGSAT.

3.7.2. Users must comply with the terms and conditions of all licence agreements.

3.7.3. Users must not modify any software, nor incorporate parts of any software into their own work, without written permission from the copyright/intellectual property owner.

3.7.4. Users must comply with any instructions or regulations displayed in and around onsite computing and digital facilities, and also comply with those guidelines provided when using facilities and resources remotely.

3.7.5. Users must not introduce any virus, worm, malware, trojan horse or any other "nuisance" program or file onto any system or take any action to circumvent or modify any precautions taken by SGSAT to prevent "infection" of its machines.

3.7.6. Users must not use the IT and digital facilities for viewing or sending any message textual or graphic or voice or video that is offensive, abusive, obscene, defamatory, racist or otherwise unlawful. Users must not initiate or spread electronic chain mail. Any electronic communication must be relevant to the user's course of study or job within SGSAT and it must be sent only to those users to whom it is relevant. If digital systems are used for personal use then this use must follow the guidance provided in the ‘IT acceptable use – electronic communication’ policy.

3.7.7. Users may only access their own files and files which they have been given express permission to access.

3.7.8. Users must not use another user's Username, nor permit or allow another user to use their own Username.

3.7.9. Users must not allow any password associated with their Username to become known to another user. The user will be held responsible for any unlawful action carried out under their computer account unless there is evidence to prove otherwise.

3.7.10. Users must not make known any other passwords which may be supplied to them in order to enable access to subscribed electronic resources.

3.7.11. Users must not connect any equipment to SGSAT’s wired network.

3.7.12. Users must terminate each session in accordance with published instructions or by simply logging out.

3.7.13. Interference with or removal of printout which belongs to another person is not permitted. Uncollected printout will be disposed of.

3.8. **Behaviour**

3.8.1. The creation, display, production, downloading, uploading and circulation of offensive material in any form or on any medium is forbidden.

3.8.2. Users must respect the rights of others and should conduct themselves in a quiet and orderly manner when using onsite facilities.

3.8.3. No onsite, fixed equipment should be moved from its designated place or be tampered with in any way.

3.8.4. If staff have any safeguarding concerns about the content or the nature of material, other users are accessing or posting online then they should log these using the “My Concern” system.

3.9. **Private and Commercial Use**

3.10. The use of any of SGSAT’s IT and digital facilities for commercial gain as well as for private work (unconnected with a student's course or study at SGSAT or a member of staff's legitimate activities) or for work on behalf of others is not allowed.

3.11. **Use of JANET and the Internet**

3.11.1. Use of JANET and the internet in general must comply with the JANET Acceptable Use Policy (available from http://www.ja.net/documents/publications/policy/aup.pdf), as published by the United Kingdom Education and Research Networking Association (UKERNA).

3.11.2. Subject to the following paragraphs, JANET may be used for any legal activity that is in furtherance of the aims and policies of the organisation.

The following constitutes Unacceptable Use of JANET:

3.11.3. JANET may NOT be used for any of the following (3.12.1 to 3.11.11.8 inclusive):

3.11.4. Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.

3.11.5. Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.

3.11.6. Creation or transmission of material with the intent to defraud.

3.11.7. Creation or transmission of defamatory material.

3.11.8. Creation or transmission of material such that this infringes the copyright of another person.

3.11.9. Deliberate creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their User Organisation has chosen to subscribe.

3.11.10. Deliberate unauthorised access to networked facilities or services.

3.11.11. Deliberate activities with any of the following characteristics:

3.11.11.1. wasting staff effort or networked resources, including time on end systems accessible via JANET and the effort of staff involved in the support of those systems;

3.11.11.2. corrupting or destroying other users' data;

3.11.11.3. violating the privacy of other users;

3.11.11.4. disrupting the work of other users;

3.11.11.5. denying service to other users (for example, by deliberate or reckless overloading of access links or of switching equipment)

3.11.11.6. continuing to use an item of networking software or hardware after UKERNA has requested that use cease because it is causing disruption to the correct functioning of JANET;

3.11.11.7. Other misuse of JANET or networked resources, such as the introduction of 'viruses'.

3.11.11.8. Where JANET is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of JANET.

3.12. **Disclaimers**

3.12.1. SGSAT accepts no responsibility for the malfunctioning of any equipment or software that results in the failure of security or integrity of any stored program or data.

3.12.2. Student files and access will be removed once the student is no longer on their course. Students are advised to make copies on

removable media of any data that they store on SGSAT services if they wish to keep it beyond this time, as SGSAT will not be liable for its non-retention.

3.12.3. A staff computer account will be disabled once the member of staff's contract has been terminated. SGSAT will not be liable for the non-retention of the member of staff's files beyond this time.

3.13. Monitoring & Access of IT and Digital Systems including User Accounts

3.13.1. SGSAT may at any time permit the inspection, monitoring, or disclosure of IT Systems and Data:

3.13.2. When required by and consistent with English law which the College evaluates against the precise provisions of the Freedom of Information Act, Data Protection Act, The Regulation of Investigatory Powers Act, and other laws concerning disclosure and privacy, or other applicable law.

3.13.3. To ensure policy compliance.

3.13.4. At the written request of SGSAT's Senior Leadership Team, if there are reasonable grounds to believe that violations of SGSAT policies have taken place.

3.14. SGSAT reserves the right to monitor IT Systems

3.14.1. To carry out system management, problem resolution, maintenance and capacity planning, to correct problems or for similar reasons related to performance or availability of the system.

3.14.2. To comply with the Prevent Strategy, which aims to reduce the threat to the UK from terrorism, by preventing people from being drawn into terrorism, SGSAT carries out appropriate monitoring and filtering of SGSAT systems.

3.14.3. To address security issues, including virus management and authorised surveillance, including tracking unauthorised access to a system.

3.14.4. To meet time-dependent, critical business or operational needs or to carry out records management responsibilities; e.g. to conduct business during a crisis if an employee is absent when information is required, or prolonged absence of an employee when information in the User's account is required. The User will generally be informed at the earliest opportunity if this form of access is necessary.

3.14.5. To ensure compliance with this and other policies.

3.14.6. To identify and provide support regarding safeguarding matters.

4. Policy Implementation

4.1. All users of SGS Academy Trusts (SGSAT) IT and digital facilities (including software) owned, leased or hired, on or off premises.

5. Enforcement

5.1. Failure to abide by the conditions of use for IT and digital facilities may result in the following:

5.1.1. Withdrawal of access on a permanent or temporary basis which may be actioned upon suspected breach of policy with reinstatement of access to IT facilities being via normal disciplinary procedures.

5.1.2. Recommendation to invoke SGSAT disciplinary processes.

5.1.3. Where appropriate, referral to Police for possible prosecution.

6. Related Policies, Procedures, Charters, Plans, Guidance and Legislation

6.1. Legislation as listed above in 4.1 Legal Framework
6.2. IT Security Policy
6.3. Data Privacy & Protection Policy
6.4. Disciplinary Procedures
6.5. Safeguarding Policies and Procedures
6.6. Single Equality Policy
6.7. Keeping Children Safe In Education (2021, Annex D) Statutory Guidance

7. Impact

7.1. The impact of this policy is to ensure all users of IT and digital facilities within SGSAT adhere to this policy and are aware of key requirements for using these systems. This in turn ensures the overall integrity of systems and ensures the ongoing positive reputation of SGSAT.

8. Additional useful information

8.1. The Group IT Director will review and monitor the policy and procedures and will recommend and implement approved changes where necessary.

9. MANDATORY INITIAL IMPACT SCREENING

Completed by:		
Tim Hanks	Group IT Director	07/11/2022

I have read the guidance document: Completing a Policy Impact Assessment?	✓
If this policy has been up-dated, please tick to confirm that the initial impact screening has also been reviewed:	✓

EQUALITY AND DIVERSITY IMPACT ASSESSMENT	
Characteristic	This policy seeks to:
Age	Choose an item.
Disability	Choose an item.
Faith or Belief	Choose an item.
Gender	Choose an item.
Race or Ethnicity	Choose an item.
Orientation	Choose an item.
Gender reassignment	Choose an item.
Economic disadvantage	Choose an item.
Rural isolation	Choose an item.
Marriage	Choose an item.
Pregnancy & maternity	Choose an item.
Carers & care leavers	Choose an item.
Vulnerable persons	Choose an item.
Please identify any sections of the policy that specifically seek to maximise opportunities to improve diversity within any of the Trust's stakeholder groups:	NA
Please identify any sections of the policy that specifically seek to improve equality of opportunity within any of the Trust's stakeholder groups:	NA

Is there any possibility that this policy could operate in a discriminatory way?	☐	×	If you have ticked yes (red), which characteristic will be most affected? Choose an item.
If yes please confirm that the Policy has been sent for a full Equality & Diversity Impact Assessment, and note the date:	☐		Click or tap to enter a date.

Note: if the policy does not seek to increase diversity or improve equality you should go back and review it before submitting it for approval.

MAPPING OF FUNDAMENTAL RIGHTS	
Which United Nations Convention on the Rights of the Child (UNCRC), Right does this policy most protect:	Choose an item. Choose an item. Choose an item.
Which Human Right (HRA) does this policy most protect:	Art. 7 No punishment without law Art. 8 Right to private & family life

DATA PROTECTION & PRIVACY BY DESIGN SCREENING	
Tick to confirm that you have considered any data protection issues as part of the design and implementation of this policy; and, that implementing this policy will not result in the collection, storage or processing of personal data outside of official Trust systems:	✓
Tick to indicated that this policy has or requires a Data Privacy Impact Assessment:	☐