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 SGS-GS Human Resources Department

Prepared by:	Tim Hanks
Job Title/Role:	Group IT Director
Ref. No.: **QPG 148**	**Date of this version:** 28th January 2019 **Review date:** 30th June 2020 (Subject to any legislative changes) **Upload to College website?** No **Upload to e-Campus?** No
Approved by:	SGSAT Board of Trustees
Date of Approval:	

Mandatory Initial Equality and Diversity Impact Screening

Main aim and purpose of the policy:	The main aim and purpose of this document is to outline what is acceptable for users of the Trust's IT facilities.			
Is this policy (or its constituent parts) relevant to a general equality duty? (please tick)	This policy development will assist in the elimination of unlawful discrimination and/or harassment of identified groups?	Implementation of this policy will promote equal opportunities for identified groups?	Implementation of this policy will promote positive attitudes and participation between groups?	Implementation of this policy will promote good relations between groups?
Age	☐	☐	☐	✓
Disability	☐	☐	☐	✓
Gender Reassignment	☐	☐	☐	✓
Race or Ethnicity	☐	☐	☐	✓
Religion or Belief	☐	☐	☐	✓
Marriage	☐	☐	☐	✓
Pregnancy/ Maternity	☐	☐	☐	✓
Sex	☐	☐	☐	✓
Sexual Orientation	☐	☐	☐	✓
Carers/ Care givers	☐	☐	☐	✓
Persons in care	☐	☐	☐	✓
Specify any groups for which there is evidence or reason to believe that some groups or individuals could be affected differently:				

How much evidence is there:	None	A little	Some	A lot
	✓	☐	☐	☐
Is there any concern that the policy may operate in a discriminatory way?	None	A little	Some	A lot
	✓	☐	☐	☐

Assessed relevance to equality (tick one row only)	High	Med	Low	None	Brief reason for this assessment
Age	☐	☐	☐	✓	
Disability	☐	☐	☐	✓	
Gender Reassignment	☐	☐	☐	✓	
Race or Ethnicity	☐	☐	☐	✓	
Religion or Belief	☐	☐	☐	✓	
Marriage	☐	☐	☐	✓	
Pregnancy/ Maternity	☐	☐	☐	✓	
Sex	☐	☐	☐	✓	
Sexual Orientation	☐	☐	☐	✓	
Carers/ Care givers	☐	☐	☐	✓	

What is the next step? (tick one only)	What priority level is this policy?			Has the Policy been sent for Full EQIA, or do you believe the policy should have a Full EQIA?	
	High ✓	Medium ☐	Low ☐	Yes ☐	No ✓

I am satisfied that an initial screening has been carried out on this policy/procedure and a full Impact Assessment is not required

Completed by: Tim Hanks *Position: Group IT Director* *Date: 28/01/2019*

IT Acceptable Use Policy – Users

1. Introduction

1.1. This policy outlines the acceptable use of Information Technology (IT) from a user perspective.

2. Statement

2.1. This policy applies to all users of SGS Academy Trust's ('the Trust') IT facilities (including software) owned, leased or hired, on or off premises.

2.2. The Trust reserves the right to investigate computer 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 Trust policy.

3. Objectives

3.1. The objective of this document is to outline what is acceptable for users of the Trust's IT facilities.

4. Implementation

4.1. Legal Framework

4.1.1. The use of the IT facilities are subject to the provisions of the following Acts:

4.1.1.1. Data Protection Act 2018

4.1.1.2. Copyright Designs and Patents Act 1988

4.1.1.3. Computer Misuse Act 1990

4.1.1.4. Freedom of Information Act 2000

4.1.1.5. Regulation of Investigatory Powers Act 2000

4.1.1.6. Electronic Communications Act 2000

4.1.1.7. Digital Economy Act 2010

4.1.1.8. Human Rights Act 1998

4.1.1.9. And any regulations made pursuant to these Acts.

4.1.1.10. Where appropriate offences may be reported to the Police for further investigation.

4.2. Authorisation

4.2.1. Access to IT facilities is restricted to members of the Trust.

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

4.3. Registration of User Access

4.3.1. Use of the facilities is conditional upon individuals being registered centrally within the Trust's management information system. Once this has been successfully completed a username and password will be generated automatically.

4.4. Termination of user access

4.4.1. At the point an account holder no longer appears within the data provided by the 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.

4.5. Password Policy

4.5.1. 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.

4.5.2. 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.

4.6. Access to facilities

4.6.1. Access to on-site IT facilities is during published site opening hours.

4.6.2. Although some systems are available 24/7 this is provisioned as “best endeavour”.

4.6.3. All access is subject to facilities maintenance requirements.

4.7. Use of IT Facilities

4.7.1. Users must not in any way cause any form of damage to the Trust’s computing equipment or software, nor to any of the rooms and their 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 the Trust.

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

4.7.3. 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.

4.7.4. Users must comply with any instructions or regulations displayed in and around computing facilities.

4.7.5. 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 the Trust to prevent "infection" of its machines.

4.7.6. Users must not use the IT facilities for 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 mail must be relevant to the user's course of study or job within the Trust and it must be sent only to those users to whom it is relevant.

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

4.7.8. Users must not use another user's Username, nor permit or allow another user to use his/her own Username.

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

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

4.7.11. Users **must not** connect any equipment to the Trust's wired network.

4.7.12. Users must terminate each session in accordance with published instructions.

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

4.8. **Behaviour**

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

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

4.8.3. No equipment should be moved from its designated place or be tampered with in any way.

4.9. **Private and Commercial Use**

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

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

4.10.1. 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).

4.10.2. 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:

4.10.3. JANET may NOT be used for any of the following (4.8.4 to 4.8.11.8 inclusive):

4.10.4. 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.

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

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

4.10.7. Creation or transmission of defamatory material.

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

4.10.9. 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.

4.10.10. Deliberate unauthorised access to networked facilities or services.

4.10.11. Deliberate activities with any of the following characteristics:

4.10.11.1. 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;

4.10.11.2. corrupting or destroying other users' data;

4.10.11.3. violating the privacy of other users;

4.10.11.4. disrupting the work of other users;

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

4.10.11.6. 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;

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

4.10.11.8. 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.

4.11. Disclaimers

4.11.1. The Trust 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.

4.11.2. Student files and access will be removed once the student is no longer on his/her course. Students are advised to make copies on removable media of any data that they store on Trust services if they wish to keep it beyond this time, as the Trust will not be liable for its non-retention.

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

4.12. **Monitoring & Access of IT Systems including User Accounts**

4.12.1. The Trust may at any time permit the inspection, monitoring, or disclosure of IT Systems and Data;

4.12.1.1. When required by and consistent with English law which the Trust 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.

4.12.1.2. To ensure policy compliance.

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

4.13. **The Trust reserves the right to monitor IT Systems:**

4.13.1. 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.

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

4.13.3. 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.

4.14. **Disciplinary Procedures**

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

4.14.1.1. 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.

4.14.1.2. Recommendation to invoke Trust disciplinary processes.

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

5. Responsibilities

5.1. All.

6. Related Policies, Procedures and Legislation

6.1. Legislation as listed above in 4.1 Legal Framework

6.2. Data Privacy & Protection Policy

6.3. Disciplinary Procedures

6.4. Safeguarding Policies and Procedures

6.5. Single Equality Policy