South Gloucestershire and Stroud Academy Trust (SGSAT)

IT Security Policy

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 174**	**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

IT Security Policy

1. Policy Intent

1.1. The intent of the IT Security Policy is to set out SGS Academy Trust (SGSAT)'s definition of, commitment to and requirements for information security.

1.2. To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

2. Scope

2.1. This policy applies to all users of SGSAT's IT facilities.

3. Procedures

3.1. Business continuity management and planning

3.1.1. IT Systems shall undergo a risk assessment exercise to determine where business continuity planning is needed which is subsequently reflected in the IT Business Continuity Plan.

3.1.2. The IT Business Continuity plan will be periodically tested as per the schedule outlined in the plan.

3.1.3. All relevant staff will receive appropriate training to be able to carry out their roles with respect to business continuity plans.

3.1.4. Each business continuity plan will be reviewed, and if necessary updated. The frequency of reviews will be as defined for the appropriate criticality level.

3.2. Compliance

3.2.1. The "IT Acceptable Use Policy – Users" sets out the responsibilities with respect to the use of computer-based information systems and data. Line managers must provide specific guidance on legal compliance to any member of staff whose duties require it.

3.2.2. All members of the organisation will comply with the IT Security Policy and, where appropriate, their compliance will be monitored.

3.2.3. The organisation's "IT Acceptable Use Policy – Users" forbids the use of information systems to send or publish derogatory remarks about people or organisations.

3.2.4. The organisation's data retention policy defines the appropriate length of time for different types of information to be held. Data will not be destroyed prior to the expiry of the relevant retention period and will not be retained beyond that period. During the retention period appropriate technical systems will be maintained to ensure that the data can be accessed.

3.2.5. The organisation will only process personal data in accordance with the requirements of the data protection legislation. Personal or confidential information will only be disclosed or shared where an employee has been authorised to do so.

3.2.6. Where it is necessary to collect evidence from the information systems, it shall be collected and presented to conform to the relevant rules of evidence. Expert guidance will normally be sought.

3.3. Personnel Specific

3.3.1. Disaffected and Departing Staff

3.3.1.1. Management must respond quickly yet discreetly to indications of staff disaffection, liaising as necessary with Human Resources management and the Group IT Director.

3.3.1.2. Upon notification of staff resignations, Human Resources management must consider the potential implications and inform the Group IT Director whether the member of staff's continued system access rights constitutes an unacceptable risk to the organisation and, if so, revoke all access rights.

3.3.1.3. Departing staff are to be treated sensitively, particularly with regard to the termination of their access privileges.

3.3.1.4. Departing staff must return all information assets and equipment belonging to the organisation.

3.4. Operations

3.4.1. Areas and offices where sensitive or critical information is processed shall be given an appropriate level of physical security and access control. Staff with authorisation to enter such areas are to be provided with information on the potential security risks and the measures used to control them.

3.4.2. The procedures for the operation and administration of the organisation's business systems and activities must be documented with those procedures and documents being regularly reviewed and maintained.

3.4.3. Duties and areas of responsibility shall be segregated to reduce the risk and consequential impact of information security incidents that might result in financial or other material damage to the organisation.

3.4.4. All security incidents are to be reported to cert@sgscol.ac.uk which is a specific helpdesk queue allowing for the management and tracking of events.

3.4.5. Faults and malfunctions are logged and monitored via the IT Helpdesk and timely corrective action taken.

3.4.6. Changes to operational procedures must be controlled to ensure ongoing compliance with the requirements of information security and must have management approval.

3.4.7. Development and testing facilities for business-critical systems shall be separated from operational facilities and the migration of software from development to operational status shall be subject to formal change control procedures.

3.4.8. Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to migration to operational status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place.

3.5. System Planning

3.5.1. New information systems, or enhancements to existing systems, must be planned jointly by the individual(s) responsible for the information and the Group IT Director. The business requirements of all authorised systems must specify requirements for security controls.

3.5.2. The implementation of new or upgraded software must be carefully planned and managed, to ensure that the information security risks associated with such changes are mitigated using a combination of procedural and technical controls.

3.5.3. Equipment supporting business systems shall be planned to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance.

3.5.4. Equipment shall be correctly maintained.

3.5.5. Equipment supporting business systems shall be given adequate protection from unauthorised access, environmental hazards and failures of electrical power or other utilities.

3.5.6. Access controls for all information and information systems are to be set at appropriate levels in accordance with the value and classification of the information assets being protected.

3.5.7. Prior to acceptance, all new or upgraded systems shall be tested to ensure that they comply with the organisation's information security policies, access control standards and requirements for ongoing information security management.

3.6. System Management

3.6.1. The organisation's systems shall be managed by suitably trained and qualified staff to oversee their day to day running and to preserve security and integrity in collaboration with individual system owners. All systems management staff shall be given relevant training.

3.6.2. Access controls shall be maintained at appropriate levels for all systems by ongoing proactive management and any changes of access permissions must be authorised by the manager of the system or application. A record of access permissions granted must be maintained.

3.6.3. Access to all information services shall use a secure log on process and access to the organisation's business systems shall also be limited by time of day or by the location of the initiating terminal or both. All access to information services is to be logged and monitored to identify potential misuse of systems or information.

3.6.4. Inactive connections to the organisation's business systems shall shut down after a defined period of inactivity to prevent access by unauthorised persons.

3.6.5. Password management procedures are in place to ensure the implementation of the requirement of the information security policies and to assist users in complying with best practice guidelines.

3.6.6. Capacity demands of systems supporting business processes shall be monitored and projections of future capacity requirements made to enable adequate processing power, storage and network capacity to be made available.

3.6.7. Security event logs, operational audit logs and error logs must be properly reviewed and managed by qualified staff.

3.6.8. System clocks must be regularly synchronised with the organisations central time services.

3.7. Network Management

3.7.1. The organisation's network shall be managed by suitably authorised and qualified staff to oversee its day to day running and to preserve its

security and integrity in collaboration with individual system owners. All network management staff shall be given relevant training.

3.7.2. The network must be designed and configured to deliver high performance and reliability to meet the organisation's needs whilst providing a high degree of access control and a range of privilege restrictions.

3.7.3. Remote access to the network is subject to robust authentication and VPN connections to the network are only permitted for authorised users ensuring that use is authenticated and data is encrypted during transit across the network.

3.7.4. The implementation of new or upgraded software or firmware must be carefully planned and managed. Formal change control procedures, with audit trails, shall be used for all changes to critical systems or network components.

3.7.5. All changes must be properly tested and authorised before moving to the live environment.

3.7.6. Moves, changes and other reconfigurations of users' network access points will only be carried out by staff authorised by IT Services according to procedures laid down by them.

3.7.7. Networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorised intrusion.

3.8. Software Management

3.8.1. The organisation's business applications are to be managed by suitably trained and qualified staff to oversee their day to day running and to preserve security and integrity in collaboration with nominated individual application owners. All business application staff shall be given relevant training in information security issues.

3.8.2. The procurement or implementation of new, or upgraded, software must be carefully planned and managed and any development for or by the organisation must always follow a formalised development process. Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls.

3.8.3. Business requirements for new software or enhancement of existing software shall specify the requirements for information security controls.

3.8.4. Formal change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to business software. All changes must be properly authorised and all software, including that which interacts with the amended software, must be tested before changes are moved to the live environment.

3.8.5. Modifications to vendor supplied software shall be discouraged, only strictly controlled essential changes shall be permitted and the development of interfacing software shall only be undertaken in a planned and controlled manner.

3.8.6. The implementation, use or modification of all software on the organisation's business systems shall be controlled.

3.8.7. All software shall be checked before implementation to protect against malicious code.

3.9. Vulnerability Assessment

3.9.1. Vulnerability assessment is an automated process undertaken using "AlienVault". Automated scans are scheduled to minimise disruption.

3.9.2. Secondary user-initiated scanning is undertaken using Nessus.

3.9.3. Access to this system is restricted to specified individuals authorised by the Group IT Director.

3.9.4. Detailed information of update and configuration procedures is located in the "IT Operations Manual".

3.10. Security Appliance Management (Firewalls)

3.10.1. Read and write access to these systems is restricted to specified individuals authorised by the Group IT Director.

3.10.2. Detailed information of update and configuration procedures is located in the "IT Operations Manual".

3.11. Anti-virus and Malware Management

3.11.1. Read and write access to these systems is restricted to specified individuals authorised by the Group IT Director.

3.11.2. Detailed information of update and configuration procedures is located in the "IT Operations Manual".

3.12. Privileged Account Management

3.12.1. Access to the “Domain Administrator” and higher-level security groups in Active Directory is restricted to specified individuals authorised by the Group IT Director.

3.13. **Cryptography**

3.13.1. Microsoft’s BitLocker cryptography solution has been adopted for use on all Windows based staff devices providing encryption of all portable media (such as USB keys).

3.13.2. Write access will be denied on all Microsoft Windows based staff machines to all portable media NOT encrypted via BitLocker.

3.13.3. All Microsoft Windows tablets and laptops designated specifically as “Staff Only” will be fully encrypted.

3.13.4. Confidential information shall only be taken for use away from the organisation in an encrypted form unless its confidentiality can otherwise be assured.

3.13.5. Procedures shall be established to ensure that authorised staff may gain access, when needed, to any important business information being held in encrypted form.

3.13.6. The confidentiality of information being transferred on portable media or across networks must be protected by use of appropriate encryption techniques.

3.13.7. Encryption shall be used whenever appropriate on all remote access connections to the organisation’s network and resources.

4. Policy Implementation

4.1. All users who will have access to SGSAT held data or systems are responsible for the implantation of this policy.

5. Enforcement

5.1. Failure to adhere to the requirements, advice or guidance outlined in this document may result in disciplinary action in accordance with the SGSAT’s disciplinary policy and procedure.

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

6.1. Related SGSAT policies, procedures and guidance can be found on SharePoint and include:

- IT Acceptable Use Policy – Users
- Data Privacy & Protection Policy
- Disciplinary Procedures

- Safeguarding Policies and Procedures
- Single Equality Policy
- 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

7. Impact

7.1. The impact of this policy is to ensure that all users are aware of IT Security requirements within SGSAT. 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:	☐