The following policy has been approved by the Trustees of Solomon Academic Trust.

Any amendments to the policy require the Trustees' approval.

All staff and volunteers working for the Centre for Muslim-Christian Studies, Oxford (CMCS) and other programmes under the control of SAT, are required to comply with an information policy of this form. Support and guidance may be offered by SAT trustees.

Information Security is not a new requirement, and to a large extent the policy and accompanying procedures formalise and regularise existing good practice within the Centre.

Solomon Academic Trust will review this policy at least yearly to ensure any new developments are covered and protected.

Information Security and Data Protection Policy
Solomon Academic Trust
March 2019

1. Introduction

The Solomon Academic Trust (SAT) seeks to maintain the confidentiality, integrity and availability of information about its staff, visitors, donors, external networks and associated scholars, and its affairs generally. It is extremely important to the Trust to preserve its reputation, and compliance with legal and regulatory requirements with respect to this Information is fundamental to its operations.

2. Objective

This Information Security Policy defines the framework within which information security will be managed by SAT and demonstrates management direction and support for information security. This policy is meant to keep information secure and highlights the risks of unauthorised access or loss of data.

In support of this objective all users of data assets, whether they are manual or electronic, accept their roles and responsibilities in ensuring information is protected and are committed to:

- Treating information security seriously
- Identifying information risks, such that they can be managed and mitigated to an acceptable level
- Allowing authorised users to access information securely, to perform their roles
- Maintaining an awareness of security issues
- Adhering to applicable security policies / following applicable guidance.

Information relating to living individuals (such as may be found in Donation, Gift Aid, Personnel or Payroll systems, lists of academic visitors and the wider network, or any other personal record systems) should only be stored in the appropriate secure systems and is subject to legal protection. All users of the computing systems are obliged, under the terms of the General Data Protection Regulations, to ensure the appropriate security measures are in place to prevent any unauthorised access to personal data, whether this is on a workstation or on paper.

3. Scope and definitions

The scope of this Information Security Policy extends to all SAT information and its operational activities, including but not limited to:

- Records held by SAT of donors, donations and gift aid claims
- Records held relating to staff, visitors, conference guests, the wider network of scholars, and external contractors where applicable
- Operational plans, accounting records, and minutes
- All processing facilities used in support of operational activities to store, process and transmit information
- Any information that can identify a person, e.g. names and addresses

The policy applies to all data held by SAT whether in electronic or physical format including by way of example:
- electronic data stored on and processed by fixed and portable computers and storage devices
- data transmitted on networks
- all paper records.

This Policy covers all data access and processing pertaining to SAT, and all staff and other persons (including Lecturers, Trustee body members, and other officers and delegates not already part of these groups) must be familiar with this Policy and any supporting guidance. Any reference to 'staff' shall be regarded as relating to permanent, temporary, contract, and other support staff as applicable.

4. Policy

SAT aims, as far as reasonably practicable, to:
- Protect the confidentiality, integrity and availability of all data it holds in its systems. This includes the protection of any device that is owned by the Trust that can carry data or access data, as well as protecting physical paper copies of data wherever possible (e.g. through the discipline of clean desk policies)
- Meet legislative and contractual obligations
- Protect the Trust's intellectual property rights
- Produce, maintain and test business continuity plans in regards to data backup and recovery
- Prohibit unauthorised use of the Trust's information and systems
- Communicate this Information Security Policy to all persons who process or handle SAT data
- Provide information security training to all persons appropriate to the role
- Report any breaches of information security, actual or suspected to the Data Controller within CMCS, (who acts for SAT) within the space of 24 hours.

4.1 Specific Policy Aims

4.1.1 General approach

All information assets shall be 'owned' by a named officer or staff member within the Centre. A list of those assets and their owners, and associated responsibilities, shall be maintained by the Trust.

- Access to information shall be restricted to authorised users and shall be protected by appropriate practical, physical and/or logical controls.

[The former may include locked storage facilities, cupboards and doors for all offices; clean desk policies (cf section 4.1.5).
The latter may include effective system passwording and access control (cf section 4.1.2)]

- Access privileges should be allocated based on the minimum privilege required to fulfil duties, and they shall be authorised by the information asset owner, or someone with authority to act on that person's behalf, or that of the Trustees of SAT.

4.1.2. Network and Computer Security
Responsibility for management and security of CMCS's internal network is in the hands of the Centre's Data Protection and Security Officer (see CMCS Information Security and Data Protection Policy).

4.1.3 Control of Mobile Devices
Mobile Computing rules apply to any mobile hardware that is used to access SAT resources, whether the device is owned by the user, or by SAT.

Persons with laptop computers and other mobile computing devices including mobile phones shall take all sensible and reasonable steps to protect them, and data contained therein, from damage, loss or theft. Such steps may include:
• Persons using computing equipment in public places shall ensure that confidential information cannot be viewed by unauthorised persons
• Mobile computer and smart phone users are required to ensure that software controls and updates are installed and regularly updated to protect the devices from viruses, spyware and similar malicious programmes
• Use of any mobile computing device owned by SAT, or that is used to access SAT data (including email) must be in accordance with this Policy
• Anyone using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a suitable password or PIN, and that password or PIN must never be shared with anyone
• Mobile devices should not be used to carry sensitive SAT data for any longer than absolutely necessary and any data on the device should be encrypted if possible.

4.1.4 Information Backup
• The Data Protection and Security Officer of CMCS shall be responsible for ensuring that systems and information are backed up in accordance with the defined requirements (see CMCS Information Security and Data Protection Policy).

5. Responsibilities
The following bodies and individuals have specific information security responsibilities:

- The Chair of SAT Trustees is accountable for the effective implementation of this Information Security Policy, and supporting information security rules and standards, within SAT
- The Board of Trustees has governance responsibility for information security. Specifically, the Board has responsibility for overseeing the management of the security risks to staff and associate scholars, its infrastructure and its information
- The Data Protection and Security Officer of CMCS, acting on behalf of SAT, is responsible for establishing and maintaining SAT's information security management framework to ensure the availability, integrity and confidentiality of all information
- All Users are responsible for making informed decisions to protect the information that they process.

6. Data Breach or Loss

The GDPR introduces a duty on the Trust to report certain types of personal data breach to the Information Commissioner's Office (ICO). This must be done within 72 hours of becoming aware of the breach.

6.1. Defined procedures shall be in place to handle loss of data.

Such breaches shall include any breaches of this policy. Breaches include but are not limited to:

- data breach/loss/theft
- loss of equipment due to theft
- inappropriate access controls allowing unauthorised access
- equipment failure
- human error
- unforeseen circumstances such as fire and flood
- hacking
- 'blagging' or 'phishing' offences where data is obtained by deception.

6.2. Reporting of Breaches

Any breach should be immediately reported as per the Trust's defined policy. All investigations should be carried out urgently and reviewed once the issue has been resolved.

Responsibility for the reporting of any data breach is up to the information owner, or the person who first notices that a breach has occurred.

7. Governance

This Policy will be reviewed regularly on behalf of SAT by the Data Protection and Security Officer of CMCS and should be reviewed and approved annually, irrespective of whether changes have been made, by the Board of Trustees. Version control will be applied and made clear within the document. The review will ensure that it is:

- remaining operationally fit for purpose
- reflecting changes in technologies
- aligned to industry best practice, and
- supporting continued regulatory, contractual and legal compliance.

8. Enforcement

Breaches of the Systems and Data Access Control Policy could lead to civil or criminal actions against the individual or the Trust, taken by individuals, or by the Information Commissioner's Office on behalf of the UK Government.

Non-compliance with the general principles and conditions of this policy within the Centre may lead to disciplinary action being taken up to and including dismissal.

Version 1.2, Feb 2020