School of Anthropology and Museum Ethnography & School of Interdisciplinary Area Studies **Information Security Policy**

Contents

1 Preamble 3

2 Purpose 3

3 Scope 3

4 Roles and responsibilities 3

5 Risk Assessment & Review 4

6 Data Classification 4

7 Data Storage & Information Sharing 4

8 Mobile Devices [laptop, phone, tablet, usb key] 5

9 Computers & Software 5

10 Authentication & Authorisation 5

11 Building Security 5

12 Network and IT Systems Security 6

13 Information Handling & Disposal 6

14 Backup and Archiving 7

15 Off-Site & Remote Access 7

16 Disaster Recovery, Risk Assessment & Business Continuity 7

17 Incident Management & Procedures 7

18 Related Policies & Guidance 7

1 Preamble

1.1 This policy is the overarching Information Security Policy for the School of Anthropology and Museum Ethnology (SAME) and the School of Interdisciplinary Areas Studies (SIAS). It is the primary policy under which all other related policies reside. Annexe A provides a list of all of the SAME and SIAS policies that support this Policy.

1.2 The policy is designed to ensure that SAME and SIAS comply with all relevant University and legal requirements in respect of information security. The policy outlines specific SAME and SIAS rules on information security and references any subservient policies that serve this policy in more detail. Annexe C provides a list of relevant security legislation and University regulations to which this Policy makes specific reference.

2 Purpose

2.1 The purpose and objective of this Information Security Policy is to protect SAME and SIAS information assets from all threats, whether internal or external, deliberate or accidental. It also describes measures to ensure business continuity, minimise damage and maximise return on investment.

2.2 Information will be protected from a loss of: confidentiality, integrity and availability.

3 Scope

3.1 This policy is intended for all staff, students and any visitors using the SAME or SIAS IT systems, data or any other information asset.

4 Roles and responsibilities

4.1 The Policy is approved by the Heads of School.

4.2 The relevant Senior Management Group in each School is ultimately responsible for the maintenance and implementation of this policy within either SAME or SIAS.

4.3 The appropriate Departmental Administrator will act as the information Security Co-ordinator.

4.4 The joint SAME/SIAS IT Committee (ITC) is responsible for both identifying and assessing security requirements and risks, recommending mitigating actions, and for reviewing this policy on an annual basis. Members of this group will provide clear direction, visible support and promote information security through appropriate commitment and adequate resourcing.

4.5 The Information Security Co-ordinators for each of SAME and SIAS will act as the contact for all staff to report any suspected breach of this or any other related policy. The Information Security Co-ordinator will then ensure that the department adheres to the University incident response procedures: http://www.it.ox.ac.uk/infosec/istoolkit/incidentresponse

4.6 Line Managers, supervisors and sponsors are responsible for ensuring that all staff for which they are responsible are (1) made fully aware of the policy; and (2) given appropriate support and resources to comply.

4.7 It is the responsibility of each user to comply with this policy, and with all other policies and procedures relating to information security. If a user is uncertain whether a particular activity is permissible under this or related policies, they should consult their line manager or supervisor.

4.8 All students, staff and visitors of SAME and SIAS are required to be aware of the University Regulations and Policies applying to all users of University ICT Facilities: http://www.ict.ox.ac.uk/oxford/rules.

4.9 All new members of staff and students will be given a copy of this policy and be made aware of associated policies and guidance relating to it.

5 Risk Assessment & Review

5.1 SAME & SIAS via the ITC will carry out an assessment of risk and will review this annually.

5.2 All new projects, software, hardware, procedures or other activity with an information systems element must be subject to risk assessment and the SAME & SIAS Information Security risk register must be updated following this, accordingly.

6 Data Classification

6.1 For the purposes of Information Security individuals should assess their data and classify it according to the risk of it being made public using the classifications provided in Annexe B for guidance - summarised below - and secure it accordingly;

6.1.1 **Confidential**: Any information that is not intended to be publicly available. If the loss or unauthorised disclosure of information could have adverse consequences for the University or individuals, it is confidential. This includes data covered by the Data Protection Act (DPA); all personal data should be considered to be confidential.

6.1.2 **Restricted:** Information intended for a defined audience but is not particularly sensitive.

6.1.3 **Open:** Information intended for the public domain or that carries no appreciable confidentiality risk.

7 Data Storage & Information Sharing

7.1 Confidential data should be stored on departmental file storage and not on local hard drives.

7.2 Confidential data must be encrypted when stored on mobile devices or removable media (e.g. USB keys).

7.3 Email should not be considered secure. Confidential information, including confidential examination material, should not be sent or stored using email.

7.4 Staff, students and visitors should obtain explicit authorisation from their line managers (or equivalent) for the storage, exchange or synching of confidential data using either free or commercial cloud storage services (e.g. Dropbox, SkyDrive, Google Docs etc.).

7.5 Further information is available from the IT team.

8 Mobile Devices [laptop, phone, tablet, usb key]

8.1 Mobile devices present a high risk as they are easily lost or stolen. It is therefore essential that these are appropriately secured. Detail is provided by the IT Team.

8.2 This policy applies to all mobile devices whether they are personally-owned or owned by the department; if a device is used for any work-related purpose and the data is considered confidential.

8.3 Confidential information should not be stored or processed on unencrypted, unsecured mobile devices.

9 Computers & Software

9.1 Control measures for SAME and SIAS hardware and software are such that no hardware or software purchased from University funds should be installed without first consulting IT in order to ensure it meets this policy and the IT Security Policy.

9.2 All staff are expected to have read and understood the SAME and SIAS IT Security Policy and agree to adhere to it. A hard copy of the policy will be given to every new member of staff in their induction pack and will be referenced during student inductions.

9.3 Supervisors and line managers will ensure that their staff adhere to the SAME and SIAS IT Security Policy. Any breaches should be reported in the first instance to the IT Manager.

10 Authentication & Authorisation

10.1 All members of staff are issued with a University card that gives authority for the user to become an authorised user of the SAME or SIAS computer network and to use the University of Oxford Nexus email system. The rights and responsibilities of University of Oxford card holders are detailed at: http://www.admin.ox.ac.uk/card/.

10.2 SAME and SIAS user accounts will only allow access to areas appropriate to the account holder's job and responsibilities. Variations to this must have supervisory or line management approval.

10.3 Visitor access will be determined by a combination of University card status and entitlements: http://www.it.ox.ac.uk/entitlements and department fee paying status.

10.4 Passwords and computer accounts must not be shared or disclosed to any third party.

11 Building Security

11.1 All external doors to the SAME and SIAS buildings will be locked at ALL times, as regulated access to buildings is the first line of security. Internal offices must be locked when not in use, unless these are emergency exits.[1]

11.2 Staff will be issued with swipe cards and keys that are appropriate to their level of work. Staff are responsible for their keys and swipe cards and must notify the

[1] The Latin American Centre and Nissan Institute external doors are locked only out of hours due to the nature of their use and are subject to the building security policy of St. Anthony's college.

relevant unit administration team immediately in the event of loss. Staff must not share or give keys or swipe cards to any third party.

11.3 The Building Security Policy provides further detail.

12 Network and IT Systems Security

12.1 The SAME and SIAS computer network is part of the University of Oxford network and is managed by both SAME and SIAS local IT and IT Services. The IT Manager is responsible for auditing and monitoring SAME and SIAS systems.

12.2 Full details of the structure, operation and responsibilities for the network and computer systems are available from the SAME and SIAS IT Team.

12.3 Connection to the SAME and SIAS network (and hence the University and Janet networks) is conditional on adhering to the University's IT Regulations and Policies, the University Information Security Policy, this department Security Policy and the IT Security Policy.

13 Information Handling & Disposal

13.1 Information handling in respect of IT systems is constrained by the entitlements governed by University card status, status within the department (Staff, Student, Visitor) and the IT Authentication and Authorisation policy based on status and job role.

13.2 All confidential data must be stored securely; in a locked cupboard or office or, if stored electronically, then secured using appropriate access permissions agreed with the data owner.

13.3 All confidential data should be removed from office equipment prior to re-use or disposal.

13.4 SAME and SIAS provide or can arrange for cross cut shredders for the secure disposal of any hardcopy and/or CDs or DVDs.

13.5 Computer hard disks, USB sticks and other storage media must be wiped prior to disposal (e.g. at end of life, on an individual leaving the department). The local IT team can arrange this.

13.6 Confidentiality risks associated with storage location of data collected online via external services (e.g., Qualtrics) should be considered during project development and both funders and data owner(s) should be satisfied that the risks are acceptable.

14 Backup and Archiving

14.1 Data stored on the SAME and SIAS file server is backed up daily. All data - especially critical files - should be stored here for security.

14.2 If encrypting a device or data (e.g. a laptop or USB stick prior to taking off site) individuals should ensure that they have a copy of any critical data stored on the department file server such that the encrypted copy is not the only copy of the data.

14.3 Confidential data on mobile devices must be securely stored (see Section 8 and the IT Security Policy).

15 Off-Site & Remote Access

15.1 Only trusted machines, not public kiosk machines (e.g. airports, hotels, and coffee shops) should be used to connect to the University network remotely.

15.2 Home computers used for remote access must be protected by a firewall, anti-virus software and by the installation of security updates. Users should preferably use departmentally supplied and secured equipment if possible.

15.3 Whenever possible all connections to University systems should be made over the Virtual Private Network (VPN) as an additional security measure.

15.4 Any member of staff wishing to work from home must undertake an Information Security self-assessment based on the University assessment flow chart (http://www.it.ox.ac.uk/infosec/wde section: How do I know whether I need to encrypt or not?) and understand the rules pertaining to Remote Working available from the IT Team.

16 Disaster Recovery, Risk Assessment & Business Continuity

16.1 SAME and SIAS have both a disaster recovery plan and a risk assessment is in place (both for Information Security and IT Security). Disaster Recovery and Business Continuity plans are available in SharePoint for each unit. The plans will be reviewed annually.

17 Incident Management & Procedures

17.1 In the first instance any suspected breach of the Information Security Policy outlined in this document should be reported to the Information Security Co-ordinator.

17.2 In the event of a reported suspected breach, the Information Security Co-ordinator will invoke the University Incident Management procedures http://www.it.ox.ac.uk/infosec/istoolkit/incidentresponse

18 Related Policies & Guidance

18.1 University Regulations and Policies applying to all users of University ICT facilities: http://www.ict.ox.ac.uk/oxford/rules/

18.2 University Policy on Information Security: http://www.it.ox.ac.uk/infosec/ispolicy/

18.3 A SAME and SIAS IT Information Security Toolkit is currently being developed.

Annexe A: SAME and SIAS Information Security Related Policies

i. The SAME and SIAS IT Security Policy [*Link: in draft*]

ii. Disaster Recovery and Business Continuity
https://sharepoint.nexus.ox.ac.uk/sites/SAME/DR/SitePages/Home.aspx

iii. Building Security Policy [*Link: in draft*]

Annexe B: Data Classification Scheme

Confidential	Confidential information should be available only to small, tightly restricted groups of authorised users. Disclosure of such information will have a severe adverse impact on the business of the University, its reputation, or the safety or wellbeing of its staff/members. Unauthorised disclosure of such information may have a severe financial impact on the University. The confidentiality of such assets will far outweigh the importance of their availability. Information assets in this category would include highly sensitive personal information as well as those with a high financial value, legal requirements for confidentiality and information, which is critical to the business operation of the University.	-Student recruitment information -Admissions information -Legally privileged documents -Senior Management and Strategic -discussion papers -Live examination papers -Contracts, commercial data -Unpublished research -University budget / TRAC data -Personal details (DPA) -Salary and Payroll data -Patient identifiable data -Credit / payment card details
Restricted	Information intended for a defined audience but not particularly sensitive.	-Committee minutes (except Council and Senate). -Draft discussion papers - restricted -Intranet web sites -Most internal documents
Open	Information intended for the public domain or that carries no appreciable confidentiality risk.	All information is assumed to be open unless specifically designated otherwise.

Annexe C: Relevant Legislation, University Rules and Sources

Legislation:

i. Data Protection Act (1988): http://www.legislation.gov.uk/ukpga/1998/29/contents

University Rules:

ii. University Regulations Relating to the use of Information Technology Facilities: http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml

iii. University Information Security Policy: http://www.it.ox.ac.uk/infosec/ispolicy/

iv. JANET(UK) Statement of acceptable use Policy: https://community.ja.net/library/acceptable-use-policy

v. University Policy on Data Protection: http://www.admin.ox.ac.uk/dataprotection/

vi. University Policy on Freedom of Information: http://www.admin.ox.ac.uk/foi/

vii. University Privacy Policy: http://www.admin.ox.ac.uk/dataprotection/privacypolicy/

viii. Trade Mark and Domain Name Policy: http://www.admin.ox.ac.uk/lso/faq/#d.en.30994

ix. Mobile Wireless Networking Regulations: http://www.oucs.ox.ac.uk/network/wireless/rules/index.xml?splitLevel=-1

x. Rules for University Web Sites: http://www.ox.ac.uk/web/rules/

xi. Computer disposal: http://www.ict.ox.ac.uk/oxford/disposal/

xii. Handling Illegal Material: http://www.ict.ox.ac.uk/oxford/rules/soaguidelines.xml

xiii. Other related policies can be viewed here: http://www.it.ox.ac.uk/legal/rules/

Sources:

xiv. Example policies and wording from here: http://www.it.ox.ac.uk/infosec/istoolkit/tools/

xv. Data classifications: http://www.it.ox.ac.uk/media/global/wwwitservicesoxacuk/sectionimages/security/classification_scheme26.08.11.pdf & http://www.ictf.ox.ac.uk/conference/2013/presentations/wks-a1-tightening-it-security.pdf (accessible to IT Support Staff only