Security Overview

Version 1.14

Created date:	26 January 2012
Last updated:	18 July 2019
Review Due:	January 2020
Authors:	Tony Austin, Tim Evans, Ray Moore, Paul Young and Donna Page
Maintained by:	Archives Manager, Systems Manager and Administrator
Previous version:	Version 1.13

1. Purpose of this document

This document provides signposting to the security policies provided by the University of York, alongside the specific policies and procedures that the ADS adheres too. This document is to be used in conjunction with specific policies outlined in

- ADS Information Security Risk Assessment[1]
- ADS Systems Overview[2]
- ADS Repository Operations[3]
- ADS Preservation Policy[4]
- ADS Privacy Policy[5]
- ADS Website Terms[6]
- ADS Cookies statement[7]

2.Security

University of York provides a dedicated Security Service who are responsible for ensuring the safety of staff, students and visitors to the University.[8] They provide a wide range of services to the whole University:

- Security
- Technical Services – CCTV and intruder alarms

[1] https://archaeologydataservice.ac.uk/advice/PolicyDocuments.xhtml#ITRisk
[2] https://archaeologydataservice.ac.uk/advice/PolicyDocuments.xhtml#Systems
[3] https://archaeologydataservice.ac.uk/advice/PolicyDocuments.xhtml#RepOp
[4] https://archaeologydataservice.ac.uk/advice/PolicyDocuments.xhtml#PresPol
[5] https://archaeologydataservice.ac.uk/advice/Privacy.xhtml
[6] https://archaeologydataservice.ac.uk/advice/WebsiteTerms.xhtml
[7] https://archaeologydataservice.ac.uk/about/Cookies.xhtml
[8] https://www.york.ac.uk/admin/security/about-us/

- Access Control
- Building Management

The University of York Security Services provide services in line with the dedicated Service Level Agreement[9], and in line with the 'Surveillance Policy'.[10]

3. University of York System Security

3.1 System Access

Security is of primary importance at multiple levels. All of the below is based on the official University of York IT Services Security.[11]

3.1.1 Centrally managed (supported) machines

System Center Endpoint Protection (SCEP) is installed and maintained on all IT Services managed office and classroom PCs. All PCs have Windows 10 installed and are regularly updated with the latest updates and patches. Managed PCs have Windows Defender (pre-installed). All managed PCs have their firewall settings configured by the University of York IT Services.

The ADS adheres to the systems and protocols provided by the University of York.

- IT Services security overview[12]
- IT Services Accounts[13] (managed by IT Services)
- IT Services anti-virus software[14]
- IT Services network settings and firewall[15]
- IT Services spam and phishing emails advice[16] and the use of malicious file-type redirection[17]
- IT Services ad-blocking software for all web browsers (uBlock Origin)[18]
- IT Services macro use (Microsoft Office) [19]
- At a minimum, access to the university network and resources is password controlled using the York Identity Manager system.[20] In some circumstances, access to university resources may also be controlled using IP address. The University of York maintain a dedicated password policy[21] and provide guidance on the creation and

[9] https://www.york.ac.uk/admin/security/service-level-agreement/v%202.0%20Section%20Service%20Level%20Agreement%20April%202014.docx, internal access only.

[10] https://www.york.ac.uk/admin/security/statistics/, internal access only.

[11] https://www.york.ac.uk/it-services/security/

[12] https://www.york.ac.uk/it-services/security/

[13] https://www.york.ac.uk/it-services/accounts/

[14] https://www.york.ac.uk/it-services/security/virus/

[15] https://www.york.ac.uk/it-services/security/network/

[16] https://www.york.ac.uk/it-services/security/spam/

[17] https://www.york.ac.uk/it-services/security/virus/#tab-4

[18] https://www.york.ac.uk/it-services/security/virus/#tab-4

[19] https://www.york.ac.uk/it-services/security/virus/#tab-4

[20] https://www.york.ac.uk/it-services/security/password/

[21] https://www.york.ac.uk/it-services/security/password/policychanges/

use of strong passwords.[22] The university provides guidance on the use of dedicated password managers.[23]

3.1.2 Unmanaged PCs and personal devices

The University of York provides clear guidance on the steps undertaken to maintain good security standards on unsupported computers and other digital devices. All users should make sure they have the same sort of protocols in place as those described for supported machines. All software is maintained and updated regularly.[24] The use of anti-virus software (Windows Defender) and firewall are mandated.[25]

3.1.3 Other measures

- All PCs should be locked when they are left unattended.[26]
- External media (i.e. portable drives and disks including those in portable computers) that are also used outside the University firewall can be a major threat to security. Infections picked up outside can be moved into the University's protective environment. It thus makes sense to scan such media coming into the University environment. This should happen automatically if your anti-virus software is set up correctly. The university provides guidance on protecting confidential information through the use of encryption[27], with further guidance on the safe sharing of data and cloud services.[28]

3.2 Data Storage

Recovery can only happen if data is backed up. Various options exist for ensuring backup,

- Personal filestore[29]: A backup service takes periodic copies of data on the various central filestores, meaning they can be restored to that point in time if needed. This service is part of the University's Disaster Recovery process for the central IT systems, allowing data to be restored in the event of a catastrophic failure.[30]

- Personal Google Drive: Google Drive gives you the ability to store files in the cloud and access them from a wide variety of devices. It is also possible to share files, and folders of files, with others.[31]

- Shared Google Drive.[32]

- Shared filestore: For use of groups or projects where centralised access to information is necessary.[33]

[22] https://www.york.ac.uk/it-services/security/password/strong/
[23] https://www.york.ac.uk/it-services/security/password/managing/
[24] https://www.york.ac.uk/it-services/security/update/
[25] https://www.york.ac.uk/it-services/security/virus/
[26] https://www.york.ac.uk/it-services/security/files/ and https://www.york.ac.uk/it-services/security/screen-lock/
[27] https://www.york.ac.uk/it-services/security/encryption/
[28] https://www.york.ac.uk/it-services/security/dropbox/
[29] https://www.york.ac.uk/it-services/filestore/
[30] https://www.york.ac.uk/it-services/services/backups/
[31] https://www.york.ac.uk/it-services/services/drive/
[32] https://www.york.ac.uk/it-services/services/drive/
[33] https://www.york.ac.uk/it-services/filestore/rented/

3.3 Data sharing

The University of York provides a number of data sharing services allowing the transmission of data.

- Google Drive[34]
- University of York DropOff Service[35]
- File transfer (SFTP and SCP)[36]

4. Fire Safety Procedure

The University of York is committed to providing a safe environment for its staff, students and visitors. Part of this safety responsibility is in its provision and management of fire safety arrangements, details outlined in the *University Policy and Management Procedure: Fires Safety Arrangements*.[37] All staff must complete annual statutory basic fire safety training,[38] with local evacuation drills carried out regularly.[39] To facilitate the evacuation plan each department/area has dedicated fire wardens and sweepers to 'clear areas' and assist with fire evacuation.[40] University properties are equipped with appropriate fire doors, alarms and signage that assist and protect staff and visitors in the event of fire and during evacuation.[41] The provision of dedicated personal emergency evacuation plans assist staff or visitors who cannot self-evacuate or require assistance to evacuate from university properties.[42]

5. Lone Working

The ADS operates during set 'core' hours (10:00 - 16:00), although staff generally work throughout the King's Manor opening hours (7:00 - 19:00). In situations where a member of staff has neither visual nor audible communication with someone else who can summon assistance in the event of an accident, illness or other emergency, for example, when the individual works outside of office hours, the ADS follows the guidance outlined by the University of York. The ADS recognises the importance of ensuring that all lone working activities are managed appropriately in order to mitigate for any associated risk.[43]

[34] https://www.york.ac.uk/it-services/services/drive/

[35] https://www.york.ac.uk/it-services/services/dropoff/

[36] https://www.york.ac.uk/it-services/services/file-transfer/

[37] https://www.york.ac.uk/admin/hsas/safetynet/Fire/fire_safety.htm, internal access only.

[38] https://www.york.ac.uk/admin/hsas/hstraining/hstraining_home.htm, internal access only.

[39] https://www.york.ac.uk/admin/hsas/safetynet/Fire/Management%20%20Procedure%20-%20Fire%20Safety%20(Evacuation%20Drills)%20(VS1.2%20-%20Mar%2017).pdf, internal access only.

[40] https://www.york.ac.uk/admin/hsas/safetynet/Fire/Management%20%20Procedure%20-%20Fire%20Safety%20(Wardens%20&%20Sweepers)%20(VS1.0%20-%20Mar%2014).pdf, internal access only.

[41] https://www.york.ac.uk/admin/hsas/safetynet/Fire/fire_safety.htm, internal access only.

[42] https://www.york.ac.uk/admin/hsas/safetynet/Fire/Management%20%20Procedure%20-%20Fire%20Safety%20(PEEP)%20(VS1.2%20-%20Aug%2016).pdf, internal access only.

[43] https://www.york.ac.uk/admin/hsas/safetynet/Lone%20Working/Management%20%20Procedure%20-%20Lone%20Working%20(VS1.8%20-%20Feb%2016).pdf, internal access only.

6. ADS Offices Security

As part of the Department of Archaeology, the ADS offices are part of the King's Manor, York.[44] As an important historic building, parts of The King's Manor are open to the public during working hours and at weekends, with access to the ADS offices restricted by key, key card and keypad security systems.[45] The University of York Security Services maintain an on-site security team who oversee access and monitor the King's Manor through a dedicated CCTV system. Outside of these office hours, access to the King's Manor is controlled by key, key card and keypad security systems, with intruder alarms, CCTV systems and routine security sweeps by Security Services. The University of York Security Services provide services in line with the dedicated Service Level Agreement[46], and in line with the 'Surveillance Policy'.[47]

The ADS adheres to the University of York general policies concerning members of staff who leave the organisation.[48] The ADS Administrator maintains an overview of physical security for the ADS offices.

7. ADS Systems Security

As part of the University of York the ADS adheres to the official policies and guidelines set out above, but at the same time takes steps to secure its own data.

7.1 Systems Access

- Systems and applications are stored and delivered on discrete independent virtual servers to improve security and reduce interdependence.
- Discrete levels of access are given to each member of ADS staff appropriate to their working needs and requirements.
- Access to systems, applications and resources is controlled via IP address.

When members of staff change roles or leave the organisation, the ADS adheres to the guidelines outlined by the University of York IT Service.[49] Access to ADS systems and resources are password controlled (for discussion of passwords see below).

7.1.1 Passwords

- The ADS maintain a Password Management System to store and encrypt all passwords.
- Unique passwords control access to all ADS systems, domains, file stores and applications.
- Passwords are subject to regular update, at a minimum annually, through the Password Management System.

[44] https://www.york.ac.uk/about/campus/landmarks/kings-manor/

[45] https://www.york.ac.uk/admin/security/access-control/, internal access only.

[46] https://www.york.ac.uk/admin/security/service-level-agreement/v%202.0%20Section%20Service%20Level%20Agreement%20April%202014.docx, internal access only.

[47] https://www.york.ac.uk/admin/security/statistics/, internal access only.

[48] https://www.york.ac.uk/admin/hr/contracts-and-appointments/leaving-the-university/resigning/

[49] https://www.york.ac.uk/it-services/accounts/staff-leavers/

- ADS staff are provided with levels of access and passwords according to the needs and requirements of their role.

In the case of staff change, the ADS follows the guidelines outlined by the University of York IT Services.[50] Internal ADS passwords are changed, updated or removed as appropriate within the Password Management System.

7.2 Data Storage

- Personal Google Drive (short-term, non-sensitive data): Google Drive gives you the ability to store files in the cloud and access them from a wide variety of devices.[51] N.B. There may be limitations on the use of Google Drive, see the usage guidance.[52]
- Personal filestore: All University of York staff are provided with their own personal filestore.[53] This drive is maintained by the University of York and is backed up as part of the wider policy.[54]
- Team Drive (short-term, non-sensitive data): Google Drive gives you the ability to store files in the cloud and access them from a wide variety of devices.[55] N.B. There may be limitations on the use of Google Drive, see the usage guidance.[56]
- Shared filestore: All ADS staff are provided with access to a networked 'backup' drive that can be mapped to individual PCs.[57] This drive is maintained by the University of York and is backed up as part of the wider policy.[58]
- Archive data (local) storage: As outlined in the *Preservation Policy* the ADS maintains multiple copies of data as part of a disaster recovery plan. All data and metadata is stored and backed up on the University of York network. Archived data is stored on a pair of Dell Compellent enterprise storage arrays located in two data centres in different locations. Each data centre is dedicated and purpose built, and has full UPS, fire suppression, generators and is 'lights out' and alarmed. Data is protected by being spread redundantly across multiple disks ('RAID'). All data is protected against accidental deletion, or 'ransomware', via read-only snapshots, taken hourly and stored for 30 days, and additional backups to tape versions, which are stored for 90 days.[59]
- Archive data (off-site) storage: All archived data is synchronised regularly from the local copy in the University of York to dedicated off-site storage provided by Amazon Web Services (AWS) and Amazon S3 Glacier.[60]
- Non-networked personal storage: Data may also be stored on personal storage devices, such as memory sticks or external drives.[61]

[50] https://www.york.ac.uk/it-services/accounts/staff-leavers/
[51] https://www.york.ac.uk/it-services/services/drive/
[52] https://www.york.ac.uk/it-services/google/policy/support/
[53] https://www.york.ac.uk/it-services/filestore/
[54] https://www.york.ac.uk/it-services/services/backups/
[55] https://www.york.ac.uk/it-services/services/drive/
[56] https://www.york.ac.uk/it-services/google/policy/support/
[57] https://www.york.ac.uk/it-services/filestore/rented/
[58] https://www.york.ac.uk/it-services/services/backups/
[59] For further discussion see the *Preservation Policy* - https://archaeologydataservice.ac.uk/advice/PolicyDocuments.xhtml#PresPol
[60] https://aws.amazon.com/glacier/
[61] https://www.york.ac.uk/it-services/filestore/

- Physical/printed documentation: The ADS run a 'paperless office', but in rare instances, largely as a consequence of historical practice, some documentation has been printed out. All documentation is stored within the ADS Offices, which are locked outside of office hours, whilst documentation containing personal information is locked in 'lockable' filing cabinets.

When members of staff change roles or leave the organisation, access to university storage is removed (see guidelines outlined by the University of York IT Service)[62] and access to the stored data, ADS systems and resources is similarly removed.

7.3 Data Sharing

7.3.1 Sharing with the ADS

- Physical media: The ADS occasionally receives data sent on a variety of physical media via the postal or courier services. On receipt of data, ADS staff follow the guidelines on security provided by the University of York IT Services.[63] At the same time the ADS follows its own protocols on checking deposition data, outlined in the *ADS Ingest Manual.*[64]
- ADS-easy and OASIS Images: The ADS operates its own dedicated digital submission system, used by ADS-easy[65] and OASIS Images services and allows depositors to create metadata and upload data directly to ADS servers. For security purposes, this system is isolated from data preservation and production servers. Protocols are in place to make sure that data sent through this system adhere to the guidelines set out by the University of York IT Services[66] and the *ADS Ingest Manual*.[67]
- OASIS: OASIS[68] is a data capture service that allows archaeological and heritage practitioners to provide information about their investigations to local Historic Environment Records (HERs) and respective National Heritage Bodies. Part of this process involves the uploading of reports into the repository. These are preserved and added to the ADS Library.[69]
- Digital exchange: Where data is exchanged outside of these systems, through Google Drive, University of York DropOff Service[70], or other digital file sharing services (e.g. DropBox, OneDrive, etc.) the ADS follows the guidelines on security provided by the University of York IT Services.[71] In each case the ADS also follows the protocols, on the deposition of data, outlined in the *ADS Ingest Manual*.[72]

[62] https://www.york.ac.uk/it-services/accounts/staff-leavers/

[63] https://www.york.ac.uk/it-services/security/

[64] https://archaeologydataservice.ac.uk/advice/PolicyDocuments.xhtml#Ingest

[65] http://archaeologydataservice.ac.uk/easy/

[66] https://www.york.ac.uk/it-services/security/

[67] https://archaeologydataservice.ac.uk/advice/PolicyDocuments.xhtml#Ingest

[68] https://oasis.ac.uk/

[69] https://archaeologydataservice.ac.uk/library/

[70] https://www.york.ac.uk/it-services/services/dropoff/

[71] https://www.york.ac.uk/it-services/security/

[72] https://archaeologydataservice.ac.uk/advice/PolicyDocuments.xhtml#Ingest

7.3.2 Sharing with users

- ADS website: All data from the Dissemination Information Package (DIP) of each archive is accessible through the ADS website. In instances where the files, or an entire dataset, is particularly large, data is available through a series of multi-zip files, see for example the *Butser Ancient Farm Project Archive 1972-2007*.[73] These files are created by ADS staff and are regularly screened. All data disseminated by the ADS is subject to guidelines outlined by the University of York IT Services.[74]
- Physical media or digital exchange: In a few circumstances, where datasets are too large for dissemination through the ADS website, these are made available 'on request' through the exchange of physical media or data exchange services.[75] In either case, compliance to the University of York IT Services security guidelines is mandated.[76]
- OAI-PMH: The ADS provides a series of OAI-PMH target for sub-sets of its collection and file-level metadata. A full list is available from the dedicated page.[77]

The access policy for ADS resources is in the Preservation Policy[78], the Sensitive Data Policy[79] and the ADS Terms and Conditions.[80] In a small number of instances, access to data may be restricted or embargoed at the request of depositors. Such restrictions are generally short term and negotiated on a case-by-case basis.

8. ADS Fire Safety

The ADS, as part of the University of York, employs the fire safety and procedures of its host institution (see above).[81] All staff must complete mandatory basic fire safety training. Fire doors, alarms and appropriate evacuation signage are provided throughout the ADS offices, with a dedicated fire sweeper/marshal to assist in the evacuation during an emergency.

9.Personal data

In all circumstances the ADS follows the regulations and guidance provided by its parent organisation, the University of York, with regard to privacy and personal data.[82] A small number of ADS services require users to register for access, e.g. OASIS, ADS-easy, etc., and hold 'personal' information about those individuals. Where personal data is necessary, the ADS recognises the importance of personal privacy and ensures that all personal data is stored in accordance with the EU's *General Data Protection Regulation* (GDPR) (2018)[83] and the UK's *Data Protection Act* (2018).[84] As employees of the University of York, all ADS staff follow the guidance provided by the University of York[85] and all staff are required to

[73] http://archaeologydataservice.ac.uk/archives/view/butser_baf_2016/downloads.cfm?archive=video
[74] https://www.york.ac.uk/it-services/security/
[75] For example, the University of York Drop-off service https://www.york.ac.uk/it-services/services/dropoff/
[76] https://www.york.ac.uk/it-services/security/
[77] https://archaeologydataservice.ac.uk/advice/OAIPMH.xhtml
[78] https://archaeologydataservice.ac.uk/advice/PolicyDocuments.xhtml#PresPol
[79] http://archaeologydataservice.ac.uk/advice/sensitiveDataPolicy.xhtml
[80] http://archaeologydataservice.ac.uk/advice/WebsiteTerms.xhtml
[81] https://www.york.ac.uk/admin/hsas/safetynet/Fire/fire_safety.htm, internal access only.
[82] https://www.york.ac.uk/about/legal-statements/#tab-4
[83] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
[84] http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
[85] https://www.york.ac.uk/records-management/dp/

undertake mandatory data protection training.[86] In those circumstances where users register for services, all passwords are stored in a hashed form. The ADS provides its own dedicated Privacy Policy.[87] This document also outlines how personal data is shared and with whom.

All documentation that exists in a 'physical' form is stored within the ADS Offices which are locked when unoccupied, or outside of office hours. Any documentation containing personal information is stored in 'lockable' filing cabinets that are only accessible on request to the ADS Administrator.

The ADS website uses cookies to improve functionality and provide analytics, although these are non-personally-identifying. The Cookies Policy provides information of those cookies used by the ADS website, and provides details on how any information is used.[88]

[86] https://www.york.ac.uk/records-management/dp/training/
[87] https://archaeologydataservice.ac.uk/advice/Privacy.xhtml
[88] http://archaeologydataservice.ac.uk/about/Cookies.xhtml