ADS Security Overview

Paul Young and Tim Evans

2022

Document Control Grid

Title:	ADS Security Overview
File name:	ADS_Security_Overview_v1-17
Location:	
Status:	LIVE
Version:	1.7
Last updated:	03 August 2022
Created date:	26 January 2012
Review due:	03 August 2023
Authors:	Paul Young and Tim Evans Previous contributions from Tony Austin, Ray Moore and Donna Page.
Maintained by:	Systems Manager and Deputy Director
Required Action:	N/A

1. Purpose of this document

1.0.1 This document provides signposting to the security policies provided by the University of York, alongside the specific policies and procedures to which the ADS adheres, and viewed in conjunction with specific policies outlined in:

- Information Security Risk Assessment
- Systems Overview
- Repository Operations
- Preservation Policy

- Privacy Policy
- Website Terms and Conditions
- Cookies Statement
- Accessibility Statement

2. University of York Physical Security

University of York provides a dedicated Security Service who are responsible for ensuring the physical safety of staff, students and visitors to the University. They provide a wide range of services to the whole University, including the King's Manor where the ADS offices are located. These include:

- Security.
- Technical Services – CCTV and intruder alarms.
- Access Control.
- Building Management

The University of York Security Services provide 24-hour cover, 365 days a year, which is coordinated through the Security Centre on the main Campus West, and based within the 'Porter's Lodge' at the King's Manor. Security provides a first response service for staff and students alike. Contact details for Security are:

In emergencies contact:

Call **+44(0)1904 32 3333**, or
Freephone **0800 43 3333**, or
For internal/campus phones **3333**, or
Via the 'Safe Zone' app - https://www.safezoneapp.com/

For non-emergencies contact:

Call **+44(0)1904 32 4444**, or
For internal/campus phones **4444**, or
Email security-control-room@york.ac.uk, or
Via the 'Safe Zone' app - https://www.safezoneapp.com/

The *Surveillance Policy* provides detailed information on the monitoring of University property and offices.

3. University of York IT Security

As the University of York hosts the ADS, the ADS adheres to the systems and protocols provided by its IT Services department. Discussed specifically in Section 7: ADS Systems Security below.

IT Services provide support and services according to the *Regulation 11: Use of Computing Facilities*, *Managing User Access Policy*, and monitored in accordance with the *Information Services Service Standards*. Services are coordinated through the IT Services building on the main Campus West.

Contact details for IT Services are:

In an emergency contact, York CERT (Computer Emergency Response Team):

Call **+44 (0)1904 323738**, or
Email cert@york.ac.uk

For non-emergencies contact, IT Support:

Visit Library and IT Help Desk in the JB Morrell Library
Call **+44 (0)1904 32 3838**, or
Email itsupport@york.ac.uk, or
Use the 'Knowledge Base' resource

IT Services also provide current information on recognised issues and problems and scheduled works through:

IT Services Status Board
IT Services scheduled work & events
Twitter
Facebook

3.1 System Access

As part of the University of York the ADS also adheres to the security policies and guidance outlined by its parent organisation. Security is of primary importance at multiple levels in accordance with the *Managing User Access Policy*. Details of the University of York *IT Security* policies and procedure, alongside clear guidance and support for staff to ensure the proper maintenance and security of all systems and services are available through the IT Security web pages.

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.

- Security Overview
- Accounts
- Passwords
- Two-factor authentication
- Virus & malware protection
- Content filtering software
- Managing plugins
- Network settings & firewalls
- Email security

At a minimum, access to the University network and resources is password controlled using the York Identity Manager system. In some circumstances, access to University resources may also be controlled using IP addresses. The University of York maintains a dedicated Password Policy and provides guidance on the creation and use of strong passwords, alongside the use of dedicated password managers.

3.1.2 Unsupported 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. Clear guidance on keeping your computer up-to-date, alongside the provision of information on anti-virus software (Windows Defender) and firewalls.

The use of two-factor authentication and passwords for connections to the University network from unsupported or personal devices ensures the maintenance of access security.

3.1.2.3 The provision of 'remote security' guidance, for unsupported or personal devices, ensures the maintenance of security should devices be lost or stolen.

3.1.3 Restricting physical access

The University of York also provides information on restricting physical access to supported and unsupported machines alongside personal devices connected to the network.

3.1.4 Storage media and memory sticks

The use of external media (i.e. portable drives) can be useful for storage and the transfer of data between systems; however, the University of York actively discourages their use for confidential or sensitive information. Section 3.3 Data sharing, provides detailed information on sharing data, alongside the use of cloud storage and sharing services.

3.1.5 Protecting confidential data

3.1.5.1 The University provides guidance on the appropriate sharing and storage of confidential or sensitive information or datasets, and providing support for the encryption of devices, media and files.

3.2 Data Storage

3.2.1 The University of York staff provides access to a number of services that facilitate the storage, access, and backing-up of data. These include:

- Personal filestore: A storage service that is regularly backed up. This service is part of the University's Disaster Recovery process for the central IT systems, allowing the restoration of data in the event of a catastrophic failure.
- Personal Google Drive: This gives you the ability to store files and access them from a wide variety of devices. It is also possible to share files, and folders of files, with others at the University. There may be limitations on the use of Google Drive; see the usage guidance.

- Shared Drives: There may also be limitations on the use of Shared Drives, see the usage guidance.
- Shared Filestore: For use of groups or projects where centralised access to information is necessary.

3.3 Data sharing

The University of York provides a number of data sharing services allowing the transmission of data between machines, systems and networks. These include:

- Google Drive
- University of York DropOff Service
- File transfer (SFTP and SCP)

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, outlined in the University Policy and Management Procedure: Fires Safety Arrangements. All staff must complete annual statutory basic fire safety training, with local evacuation drills carried out regularly. To facilitate the evacuation plan each department/area has dedicated fire wardens and sweepers to 'clear areas' and assist with fire evacuation. 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. The provision of dedicated personal emergency evacuation plans assist staff or visitors who cannot self-evacuate or require assistance to evacuate from University properties.

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 or 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 any associated risk.

6. ADS Offices Security

As part of the Department of Archaeology, the ADS offices are part of the King's Manor, York. 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.

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 between the hours of 7am to 7pm. 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 ADS adheres to the University of York general policies concerning members of staff who leave the organisation. 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. The provision of appropriate permissions to repository staff is on a needs basis, with levels of access relevant to each specific member of staff and their working practices. Access to these resources is also restricted through IP address, the use of encrypted passwords, and multi-factor authentication. A centralised, password management system facilitates the management of all passwords, with regular updates to all passwords, in accordance with the *Information Security Risk Assessment*.

When members of staff change roles or leave the organisation, the ADS adheres to the guidelines outlined by the University of York IT Service. Internal ADS permissions and passwords are changed, updated or removed as appropriate within the Password Management System when a member of staff leaves.

7.2 Data Storage

Repository staff, as employees of the University of York, have access to the same resources and systems as other staff, consequently they have access to:

- Personal filestore (non-sensitive data)
- Personal Google Drive (short-term, non-sensitive data)
- Shared Drives (short-term, non-sensitive data)
- Shared filestore (non-sensitive data)
- Archive data (local) storage: As outlined in the *Preservation Policy*. All data and metadata (AIP, DIP and SIPs) are stored and backed up by ADS staff on the University of York network. On this network ADS data is stored on a pair of Dell Compellent enterprise storage arrays (current capacity ~1Pb), located in two different data centres, 2 km apart. Each data centre is dedicated and purpose built, and has full UPS, fire suppression, generators and is 'lights out' and alarmed. Within each site, data is protected by being spread redundantly across multiple disks ('RAID'). Between data centres it is replicated asynchronously, with a maximum data loss of 2 hours. Data is protected against accidental deletion or ransomware via read-only snapshots (taken hourly and stored for 30 days), and additional backups to tape, which are stored for 90 days.
- 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.
- Non-networked personal storage: Data may also be stored on personal storage devices, such as memory sticks or external drives, although such storage follows guidelines provided by the University of York.
- Physical/printed documentation: The ADS runs a 'paperless office', but in rare instances, and largely as a consequence of historical practice, some documentation has been printed out. ADS Offices are locked when unoccupied or outside of office hours to ensure the correct storage of

documentation. The storage of sensitive or personal information and documents within 'lockable' filing cabinets restricts access.

When members of staff change roles, or leave the organisation, access to storage and resources is re-evaluated and, where necessary, updated or removed.

7.3 Data Sharing

7.3.1 Sharing with the ADS

Repository staff, as employees of the University of York, have access to the same file sharing services and systems as other staff, consequently they have access to:

- 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. The repository also follows the processes and protocols for checking deposition data, outlined in the Ingest Manual.
- ADS-easy: The ADS operates its own dedicated digital submission systems, ADS-easy.This service allows depositors to create metadata and upload data directly to the ADS. For security purposes, the system is isolated from data preservation and production servers. Protocols are in place to make sure that data sent through this system adheres to the guidelines set out by the University of York IT Services and the Ingest Manual.
- OASIS: OASIS is a data capture and report submission service that allows archaeological and heritage practitioners to provide information about their investigations to local Historic Environment Records (HERs) and respective National Heritage Bodies. These are preserved and added to the ADS Library.
- Google Drive
- University of York DropOff Service
- Other digital file sharing and cloud services (e.g. DropBox, OneDrive, etc.)

- File transfer (SFTP and SCP)

Where used, the ADS follows the guidelines on security provided by the University of York IT Services alongside the procedures and processes, on the deposition of data, outlined in the *Ingest Manual*.

7.3.2 Sharing with users

Repository staff, as employees of the University of York, have access to the file sharing services and systems as all other staff, and outlined in *3.3 Data sharing*.

More generally the ADS shares datasets using the following systems and resources:

- ADS website and resources: All data from the Dissemination Information Package (DIP) of each archive or dataset is accessible through the ADS website.
- Physical media: In a few circumstances, where datasets are too large for easy dissemination over the internet, they are made available 'on request' through the exchange of physical media, typically using portable media. Requests of this nature are few in preference of the sharing of data using internal and external digital exchange services. The ADS ensures compliance to the University of York IT Services security guidelines.
- Digital exchange services (internal): As outlined in section 3.3 Data sharing.
- Digital exchange services (external): External file sharing and cloud services (e.g. DropBox, OneDrive, etc.).
- OAI-PMH: The ADS provides a series of OAI-PMH targets for subsets of its collection and file-level metadata.

The access policy for ADS resources is in the *Policy and Guidance on the Deposition of Personal, Confidential and Sensitive Data* and the website Terms and Conditions. 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 Section 4: Fire Safety Procedure). All staff must undergo mandatory basic fire safety training. The provision of fire doors, alarms and appropriate evacuation signage throughout the ADS offices protects repository staff in the event of fire, whilst a dedicated fire sweeper/marshal assists all during evacuation.

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. 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 UK's Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations (2019). As employees of the University of York, all ADS staff follow the guidance provided by the University of York and all staff are required to undertake mandatory data protection training. In those circumstances where users register for services, all passwords are stored in a hashed form. The ADS provides its own dedicated Privacy Policy. 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 Deputy Director or Director.

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.