INFORMATION SECURITY PROCEDURE

INTRODUCTION

This procedure was originally created from JISC guidance on 'Developing an Information Security Policy'. It has been updated from the more detailed guidance in the UCISA Information Security Toolkit that, in turn, is based upon the industry standard ISO 27001.

Computer and information systems underpin all the University's activities, and are essential to the delivery of the University's strategic objectives.

UWS recognises the need for its staff, students and visitors to have access to the information they require in order to carry out their work and recognises the role of information security in enabling this.

Security of information must therefore be an integral part of the University's management structure in order to maintain continuity of its business, legal compliance and adhere to the University's own regulations and policies.

This procedure supersedes any written or oral policy previously issued concerning Information Security in the University.

1. SCOPE OF PROCEDURE

This procedure applies to the use of all UWS information systems by all UWS staff, students, their agents and visitors. It also includes data extracted from any system, whether in electronic or paper based format.

This procedure defines the framework within which information security will be managed across UWS. It demonstrates management direction and support for information security throughout UWS. It should be read in conjunction with the following documents which are available on the University's website:

- IT Acceptable Use Statement
- IT Password Management Procedure
- Data Protection Code of Practice
- Records Management Protocol
- Data Classification Schedule

This procedure defines roles and responsibilities with respect to data security and to make explicit the institution's attitude to any actions that threaten the security of information assets. The concept of 'ownership' of information systems, procedures and data is core to this procedure.

2. STATEMENT

UWS is committed to protecting the security of its information and information systems. It is the University's policy that the information it manages shall be appropriately secured to protect against breaches of confidentiality, failures of integrity or interruptions to the availability of that information. It shall ensure appropriate legal, regulatory and contractual compliance.

2.1. Network Security

Protective systems must be implemented to ensure the security of the network that carries information both internally and externally. These systems will include, but

not limited to, email filtering, web filtering, anti-virus, anti-malware, anti-spyware and firewalls.

All incoming and outgoing email and its attachments, internet access and downloads will be monitored and controlled in a manner that (where possible) detects and eliminates security threats. All file storage and transfer may be monitored to identify active or potential threats to sensitive data.

Adequate safeguards must be established so that disruption to the University is minimised in the event of critical information systems becoming unavailable due to network issues. Network security standards and procedures will be updated as often as is necessary to measure and maintain their effectiveness.

2.2. User Identification and Passwords

All staff and students using UWS information systems and services will be individually identifiable by the use of a unique user ID. All those with a user ID must comply with the Password Management Procedure. Multi-Factor Authentication is required on all UWS M365 accounts

2.3. Encryption and Mobile Devices

Sensitive/Special Category data relating to identifiable individuals and sensitive information require encryption to prevent unauthorised access. This applies particularly when the information is being transported outside the institution (e.g. on laptops or other mobile devices). Cloud storage using Microsoft OneDrive is a preferred alternative to portable storage devices. See Cloud Storage Protocol and Data Classification Schedule for more information.

Any person carrying University information of a personal or otherwise sensitive nature on portable or mobile devices, whether the device is University owned or otherwise, must take additional precautions to avoid loss of or unauthorised access to the information.

In such circumstances, all portable and mobile devices must utilise encryption software in addition to password-protected access to the device. Where personal or sensitive information is regularly accessed on mobile devices off-campus, consideration should be given to other ways of working (e.g. VPN access). Mobile devices must have at least the PIN access control function enabled at all times and allow remote deletion of emails in the case of loss or theft.

University owned mobile devices must not be lent to family or friends for any reason.

2.4. Remote Access

Web browser access will be provided to UWS owned systems that sit outside the institutional firewall (e.g. public web and M365 email access). Remote access to systems inside the firewall will only be provided via a secure Virtual Private Network (VPN) connection or similarly encrypted channel.

VPN access for those staff that require the facility will be provided, subject to conditions being met regarding the device to be used to connect to the network, whether a UWS device or a personal one.

2.5. Ownership of Information

Information security is a shared responsibility for all members of the institution. UWS systems alone cannot provide the level of security required and there is an obligation on every individual to behave responsibly.

Each information system must have a 'business owner' who can establish and specify the level of security required for the information contained within the system as well as take responsibility for the quality and quantity of the information held.

2.6. Access Control

Control of access to data and access to online services is part of the information security process. Least privilege access is the over-arching basis on which access should be granted. Where individual access to a system should be controlled, this will be managed through Active Directory. Where access to the system is allowed but certain restrictions apply within the system, this will be controlled by the relevant application. Appropriate levels of access must be defined by the information system 'business owner' (see above). Access to information held on shared network drives will be defined by the nominal 'owner' of this data. This will normally be a Dean of School or Head of Department or member of the Senior Management team.

2.7. Online or 'Cloud' Storage

Online or 'cloud' storage of UWS information must comply with the Data Protection Act 2018. To this end, disability, financial or health data relating to identifiable individuals must not be stored in online or 'cloud' systems. Other personally identifiable data may be stored on cloud. Where there are uncertainties, prior approval from IT or Data Protection may be sought. Due diligence should be applied to sensitive business information in terms of the security risks to storing online or in the 'cloud'. It is the responsibility of every individual who uses these external facilities to ensure compliance with this procedure for online or 'cloud' storage. If in doubt, seek guidance from IT.

2.8. Social Media

Social media is defined as any online interactive communication tool that encourages participation and exchanges. Common examples include; Twitter, Facebook, YouTube, Skype, Instagram, Pinterest, and LinkedIn.

Staff must ensure that when using social media, no personal, identifiable data related to another individual is posted without their explicit consent to ensure compliance with the Data Protection Act 2018.

Staff will not post any images, photographs, videos, text, etc. via social media sites without appropriate permission from the rights holders.

Staff must consider carefully any communications posted on social media that directly or indirectly represent the University. Professional responsibilities apply regardless of the medium being used. All social media communications that might affect the University's reputation, whether made either in a private or professional capacity, must comply with relevant University policies that address staff conduct.

2.9. Email

All emails sent from or received by the institution are University property and should be treated as such. Forwarding of University emails, containing information

relating to identifiable individuals or sensitive information to another email account without a good business reason is in contravention of this procedure and the Data Protection Act, if special category data.

Staff leaving the institution may create an Out-of-Office message advising of new contact details. This will be made available for a maximum of 90 days following the leaving date. The message needs to be created by the relevant individual and must be in place prior to the leaving date. User accounts are deleted 90 days from leaving date from which point data relating to that account is no longer recoverable.

2.10. Electronic Extracts and Paper-Based Reports

Personal data extracted from any Information System in electronic format, such as Excel, or paper-based reports must comply with the Data Protection Act 2018. To this end, information relating to identifiable individuals must be secured against unauthorised access, as should sensitive business information. This may be password protecting electronic extracts and storing them in a private area, while keeping paper-based reports locked away.

Sensitive information or personal data must be destroyed in accordance with the UWS Record Management Protocol and Data Protection Code of Practice.

2.11. Data Archiving and Retention

Data archiving and retention must comply with the Records Management Protocol.

2.12. Backup and Disaster Recovery

All information held on UWS networked information systems will be backed up as agreed with business owners.

3. PROCEDURE

3.1. Information Technology (IT) Responsibilities

The Director of Information Services is ultimately responsible for the maintenance of this procedure and for compliance within UWS.

IT are responsible for reviewing this procedure on a regular basis and submit any amendments that may be necessary. They will provide clear direction, visible support and promote information security through appropriate commitment and adequate resourcing.

The Information Security Manager is responsible for provision of advice and guidance regarding the implementation of this procedure.

3.2. Staff and Student Responsibilities

It is the responsibility of all line managers across UWS to implement this procedure within their area of responsibility and to ensure that all staff and students for which they are responsible are:

1) made fully aware of the procedure.

2) given appropriate support and resources to comply.

It is the responsibility of each member of UWS staff, students and visitors to adhere to this procedure.

IT should be contacted for guidance when necessary.

3.3. Jisc Acceptable Use

All staff and students must also abide by the conditions for Acceptable Use of the Jisc Network. These have been defined by JISC and apply to all connected sites. Further guidance is available from IT.

3.4. IT Security Incidents

It is a requirement that all information or cyber security incidents, or other suspected breaches of this procedure are reported to the IT Helpdesk as soon as possible so that appropriate measures may be taken to lessen the impact of the breach.

Data breaches that involve personal data should be reported to the University's Data Protection Officer in line with the procedure on Personal Data Breaches.

Security breaches will be recorded and reported on a regular basis.

3.5. Compliance

Regular audits of individual computer equipment and storage devices will be conducted in order to monitor the effectiveness of this procedure. Under circumstances where a breach of the University's Information Security Procedure is suspected, the University reserves the right to inspect the email delivered to and/or sent by an individual and the individual's electronic audit trail throughout our information systems, in accordance with the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPA).

There are risks to the University arising from 'vicarious liability' for its employees' activities. Individual staff and students have a responsibility to ensure that they comply with this procedure and the associated legislation, standards, protocols and procedures.

Failure to comply with any aspect of this procedure will be dealt with in accordance with the Procedure for Student Discipline or employee Disciplinary Procedure. Where there is a suspected breach of the procedure by an individual, their computer-based services may be suspended.

Procedure Author - IT Security and Customer Support Manager

Procedure Owner - Director of Information Services

Parent Policy Statement – Information Services Policy Statement

Public Access or Staff Only Access - Public

Version – v3 – March 2022

Changes and Reason for Changes - JISC name change, readability improved, hyperlinks added.