ISSG/14/11

Academic Services
IT Governance & Compliance

Information Handling Guidelines

Author	Revision	Date	Changes
D. Waymouth	0.2	22/02/2014	Initial Draft
D. Waymouth	1.0	18/06/2014	Approved by ISSG

Information Handling Guidelines

The handling Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference, as our information may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the information in question for example volume.

There are 4 levels of Information Classification:

- Confidential
- Restricted
- Internal
- Public

General

Some points are applicable across all the classification levels:

- Anonymise research data wherever possible, only take the data you need; and in any event do not keep data longer than required for the conduct of University business

- Do not set up your email to be automatically forwarded to an external email provider such as a personal gmail.com.

- Aim to keep Confidential and Restricted information within the University secure environment whenever possible.

- Do not leave any computing device logged in when not in use.

- Obtain any necessary permissions before sharing classified information with third parties.

- Make sure any third parties (including contractors) permitted to handle restricted or confidential data are required to take appropriate security measures. Similarly, respect any additional third party rules relating to data that has been shared with the University for example, by the NHS.

- Delete information from portable devices when it is no longer required

	Public	Internal	Restricted	Confidential
	The availability and accuracy of this data is more important.	Limited availability and integrity of this data is more important.	The integrity and confidentiality of this data is more important	The integrity and confidentiality of this data is more important
Marking	Identify UoE as the source.	All unmarked documentation will be considered for internal use only.	Mark as “UoE Restricted”	Mark as “UoE Confidential”
Access	Widely available. Unrestricted dissemination via electronic or hard copy. Dissemination must not violate any applicable laws or regulations. Information should be identifiable as from the UoE. Permissions to modify may be limited to authorised persons and procedures in place to ensure that information is kept up to date.	Dissemination only to members of the University of Exeter or organisations and individuals authorised by UoE. Where shared with a 3rd party, only authorised personnel at the 3rd party are allowed to have access to the information. Permissions to modify will be limited to authorised persons (e.g. author or authoring department).	Dissemination and amendments limited to authorised personnel only. Version control should be adopted. All access failures are logged.	Dissemination and access strictly controlled by the information owner, limited to very few authorised individuals and all access logged. Version control must be used.
Storage	Stored on centrally managed facilities backed up e.g. centrally managed file store and UoE web pages. Appropriate 3rd party storage where the data cannot be amended, avoid	Stored on University facilities with UoE authentication required backed up on a 24hr basis. Appropriate 3rd party storage with access restrictions and encryption	Stored on managed servers (patching, AV/filtering and appropriate configuration), controlled access with restrictions to authorised individuals, backed up on a 24hr basis.	Stored on managed servers (patching, AV/filtering and appropriate configuration), controlled access with restrictions to authorised individuals, backed up on a 24hr basis.

	storing the master copy. Paper documents may be available in receptions, library or other public buildings.	capability Avoid storing the master copy of documents on 3rd party/cloud services. Paper documents should only be available in University premises not open to the public. *Example:* Stored on web pages secured by UoE Single sign on (SSO) Hosted on 3rd party server with authentication handled by UoE SSO, access restrictions, regularly patched with security configuration and measures to prevent unauthorised access.	Consider using encryption and password protection for specific files 3rd party storage should have University specific encryption capability and access controls Paper documents must not be left unattended on desks or printers and stored in locked rooms or cupboards *Example:* Shared N: drive with folders set up for the specified individuals. College server managed to the same level as Exeter IT, seek advice from your CDO on default access rights and services, physical security and backup.	Consider using encryption and password protection for specific files. Paper documents must not be left unattended on desks or printers and stored in locked rooms or cupboards *Example:* Shared N: drive with folders set up for the specified individuals. Using a password to protect the file. Exeter IT managed database servers, with restricted access and data encryption.
PCs	Accessible from University cluster PCs and stored on U drive or personal cloud storage.	Accessible from University cluster PCs and stored on U drive. College PCs must be patched, consider where the data is stored alongside the physical security of the device when not in use.	Accessible from University PCs in private spaces eg. offices. Full disk encryption should be arranged in case of theft.	Accessible from University PCs in private spaces eg. offices. Full disk encryption should be arranged in case of theft.

Laptops	Data may be accessed and stored on personal and University laptops	Data may be accessed and stored on personal and University laptops with a supported and patched operating system. Up to date antivirus must be installed. Access to the laptop must be authenticated by password or similar. Data should be encrypted, if possible. Consider your backup *Example:* Personal laptop with most recent or last release of Windows, which is patched, has an antivirus product and folder based encryption for University data.	Data may be accessed and stored on laptops with a supported & patched operating system, endpoint protection and full disk encryption. AES128 is considered the minimum acceptable encryption algorithm. Endpoint protection means up to date antivirus and firewall. *Example:* University managed laptop with BitLocker enabled. iMac with a supported version of OSX, patched and Filevault 2	Data stored centrally on servers only. Do not download files to the device if at all possible. Data is accessed from laptops but not created or stored on them. *Example:* Accessed over VPN from University managed laptop with BitLocker enabled
Mobile devices (tablet or smartphone) or portable media	Data can be accessed and stored on mobile devices and portable media	Data may be accessed and stored on mobile devices and portable media where access must be authenticated by PIN, password or similar. Data should be encrypted. *Example:* Kingston DataTraveler Locker+ G2 USB stick iPad with PIN code enabled	Data may be stored on mobile devices where access is authenticated with a PIN, data wipe is enabled and has full disk encryption. Portable media with whole device encryption. AES128 is considered the minimum acceptable encryption algorithm. Do not store the master copy of a document	Data stored centrally on servers only. Data is accessed from mobile devices but not stored on them. Do not download data to portable device or media if at all possible.

			Example: Kingston DataTraveler Locker+ G2 USB stick, with a strong passcode iPad with PIN code enabled & wipe after 10 PIN entry failures. Keep in a locked drawer when not in use	
Transmission & collaboration	Via web, email, appropriate third party storage or printed copy.	Via internal email, UoE intranet, College or departmental intranets, shared folders on centrally managed file servers, appropriate 3rd party storage and printed copy. If sent via the internet, the data must be encrypted eg https on a web site, or 7-zip in email.	When emailing restricted information to other members of the University, always use their @exeter.ac.uk email address. Double-check that you have used the right address before sending the email. Use encryption if sending restricted information outside the University electronically and request a delivery receipt. The authentication process and the sensitive data must be secured in transit eg. https for web access. Any distributed documents (electronic or paper) to be	Only transmitted via email where absolutely necessary. Where transmitted via email, both the transmission and the content must be encrypted. Double-check that you have used the right address before sending the email. Use the University email system if possible: @exeter.ac.uk A delivery receipt must be requested. Shared folders on centrally managed file servers can be used. Printed copies to be delivered by hand directly to the recipient. Appropriate 3rd party

			marked as 'UoE Restricted' and the intended recipients clearly indicated. Use shared folders on centrally managed servers with specific access controls Remote access via VPN from known computers, not public computers. Appropriate 3rd party sharing tools can be used provided encryption and other appropriate security controls are in place. Seek assistance from IT G&C where needed.	sharing tools can be used provided encryption and other appropriate security controls are in place, information owners are advised to seek advice from ITC&G in advance of using third party storage for this information class.
Disposal	Staff must follow the procedures for the disposal of old equipment	Staff must follow the procedures for the disposal of old equipment and confidential non-paper waste (eg CDs and USB sticks).	Staff must follow the procedures for the disposal of old equipment and confidential non-paper waste (eg CDs and USB sticks). Confidential waste must be disposed of as follows: www.exeter.ac.uk/media/level1/academicserviceswebsite/it/recordsmanagementservice/The_Dos_and_Donts.docx	Staff must follow the procedures for the disposal of old equipment and confidential non-paper waste (eg CDs and USB sticks). Confidential waste must be disposed of as follows: www.exeter.ac.uk/media/level1/academicserviceswebsite/it/recordsmanagementservice/The_Dos_and_Donts.docx
Telephony & conversation		Take care of who may be around you when discussing University	This type of information should not be discussed in open plan areas of the	This type of information should not be discussed by telephone or in open

		business, especially in a public place or on public transport.	University. If discussed on conference calls it must be explained to attendees that the information is of a confidential nature and not for discussion with anyone outside of the distribution list.	plan offices. If disclosed during conference calls, all participants must be verified. It must be explained to attendees that the information is of a confidential nature and not for discussion with anyone outside of the distribution list.
Example Security measures		Webpages protected by UoE single sign-on Use of https or sftp for electronic transmission across the internet. If secure remote access is not possible, data may only be moved from the University on encrypted media for secure storage at another location. Use of 7zip for storage outside of the University systems Printed copies to be kept in secure location	Webpages protected by UoE single sign-on and access is restricted to specific teams or departments. Consider security by encryption at all times. Encrypt the data on any portable media or mobile device: http://as.exeter.ac.uk/it/infosec/encryptionforlaptops Printed copies to be kept in a secure cabinet Use of https, ssh or sftp for electronic transmission. Encrypt the file prior to transmission so that it is secure where ever it is stored even temporarily on the remote system. Use of 7zip, GPG or	Document secured by encryption at all times eg proprietary encryption in database tables, 7zip on shared folders, whole disk encryption. Printed copies to be kept in a secure cabinet Use secure protocols such as https, ssh or sftp for electronic transmission. No caching of data in browsers. No access from public computers eg airports or cluster PCs Remote access, not storage, from managed, encrypted devices

			s/MIME for encryption in email. Remote access using VPN from known devices	