Information Handling and Classification Table

Title: Information Classification and Handling Table
Reference: IS-07a
Status: Approved
Version: 1.2
Date: March 2018
Classification: Non-Sensitive/Open

Author(s)	Head of Information Assurance
Approved by	Vice Chancellor's Advisory Group (VCAG)
Owner	Head of Information Assurance
Issue date	31st March 2018
Review date	1st June 2018

Classification Type	HIGHLY SENSITIVE	PERSONAL/CONFIDENTIAL	NON-SENSITIVE/OPEN
Description	An inappropriate disclosure of such information may cause **severe damage** or distress to an individual or the University's objectives and/or reputation	An inappropriate disclosure of such information may **negatively impact** an individual or the University's objectives and/or reputation	Such information is publicly available to everyone.
Examples	• Highly sensitive commercial information relating to the University or another organisation e.g. commercially sensitive University strategy, in year recruitment data, in year financial data, trade secret, property negotiations • Sensitive financial information e.g. contracted information at time of tender • Confidential commercial contracts • Passwords • Sensitive personal information e.g. race or ethnicity, political opinions, religious belief, trade union membership, physical or mental health, sexual orientation, information to do with offences, medical records • Disciplinary proceedings • Security information • Legally privileged information	• Personal information as defined by the Data Protection Act 1988 (see Data Protection Policy) • Student data • Databases and spreadsheets containing personal data • Data on research participants • Commercially sensitive information e.g. contractual information, or supplier information provided in confidence • Reserved committee business • Draft reports, papers, policies • Financial information not disclosed in the Financial Statements	• Information which is in the public domain e.g. policies, academic regulations, annual financial accounts, prospectus information, salary bands, staff email addresses • Information which should be routinely disclosed e.g. some minutes of meetings
Level of Protection Required	• Such information required a high level of security controls that will ensure its confidentiality and integrity are maintained at all times. It should only be shared under a very strict	• Such information requires the most suitable security controls that will ensure its confidentiality and integrity are maintained at all times with limited access only on a "need to	• Such information should be available to University members and the general public • It should be stored on centrally managed shares areas with

Classification Type	HIGHLY SENSITIVE	PERSONAL/CONFIDENTIAL	NON-SENSITIVE/OPEN
	environment • Only provide on a "need-to-know" basis within the University, or externally to fulfil statutory and legal requirements. • Provide only hard copies to authorised individuals in face-to-face meetings and retrieve these copies at the completion of any meeting. • Those receiving highly sensitive data must only make additional copies or edits with the originator's authority • Ensure data are kept up to date and stored in highly restricted areas within centrally managed shared areas or restricted physical storage areas. Access should be limited to named data owners and authorised individuals, and appropriate monitoring controls and backup arrangements put in place. University approved storage facilities should be used where third parties are responsible for data management • Data should be securely wiped off electronic devices where the device has been decommissioned, or disposal of paper records should follow Document Retention Policy guidelines	know" basis within the University, or external to the University, to fulfil statutory and legal requirements • It should be kept up to date and stored in highly restricted areas within centrally managed shared areas or restricted physical storage areas. Access should be limited to named data owners and authorised individuals, and appropriate monitoring controls and backup arrangements put in place. • University approved storage facilities should be used where third parties are responsible for data management • Data should be securely wiped off electronic devices where the device has been decommissioned and disposal of paper records should follow the requirements of the Document Retention Policy guidelines	appropriate backup arrangements in place in line with University guidance • It should be kept up to date and access to it should be limited to only those authorised to make relevant changes to it • Disposal should follow normal file deletion or non-confidential paper record disposal procedures in line with Document Retention Policy guidelines.

Classification Type	HIGHLY SENSITIVE	PERSONAL/CONFIDENTIAL	NON-SENSITIVE/OPEN

Classification Type	HIGHLY SENSITIVE	PERSONAL/CONFIDENTIAL	NON-SENSITIVE/OPEN
INFORMATION HANDLING			
Handling Paper Records	**University areas with restricted access:** ✓ Keep files in lockable cabinets/drawers which are locked when not in active use. ✓ No papers left out when not in active use or away from desk. **University areas with unrestricted access:** **X Not permitted** **Off-site working** **X Not permitted** **Post** ✓ Must be addressed properly to a named individual, sealed and stamped with	**University areas with restricted access:** ✓ Keep files in lockable cabinets/drawers which are locked when not in active use. ✓ No papers left out when not in active use or away from desk **University areas with unrestricted access:** **X Not permitted** **Off-site working** ✓ At Home: Should be kept away from public view and stored securely when not in use e.g. lockable cabinets/drawers. ✓ Elsewhere or in transit: not to be left unattended or in the car. **Post** ✓ Must be addressed properly to a named individual, sealed and stamped with	✓ Permitted. Follow good records management procedures.

Classification Type	HIGHLY SENSITIVE	PERSONAL/CONFIDENTIAL	NON-SENSITIVE/OPEN
	'Private and Confidential' with a return address if not delivered. ✓ Use recorded delivery. Hand or courier delivery should also be considered where possible. ✓ It is recommended that the addressed envelope be enclosed in another sealed and properly addressed envelope.	'Private and Confidential' with a return address if not delivered. ✓ Use recorded delivery. Hand or courier delivery should also be considered where possible. ✓ It is recommended that the addressed envelope be enclosed in another sealed and properly addressed envelope.	
Sharing information by Email *between UW email accounts* **NOTE: The use of personal email accounts for UW business is not permitted**	✓Only share on a "need to know" basis. ✓Password protect email attachments – share password separately, preferably verbally ✓ Mark email private or confidential. ✓Verify recipient's address before you click send. ✓Whenever possible redact sensitive/personal information from email messages and attachments ✓Avoid putting Data Subject name(s) in the subject field. ✓ Implement Rights Management Software	✓ Only share on a "need to know" basis. ✓ Mark email with private or confidential. ✓ Verify recipient's address before you click send. ✓Password protect email attachments – share password separately, preferably verbally. ✓ Whenever possible redact confidential or personal information from email messages and attachments. ✓ Avoid putting Data Subject name(s) in the subject field, where possible. ✓ Implement Rights Management Software	✓ Permitted

Classification Type	HIGHLY SENSITIVE	PERSONAL/CONFIDENTIAL	NON-SENSITIVE/OPEN
	when available (to be supported by IT) **X Auto forwarding to personal email accounts is not permitted.**	when available (to be supported by IT) **X Auto forwarding to personal email accounts is not permitted.**	
Sharing information by Email *between UW and external accounts* **NOTE: The use of personal email accounts for UW business is not permitted**	Only where the recipient does not have a UW email account and it is absolutely necessary to use this method for a business purpose. ✓ Be sure the recipient understands the risks involved, accepts this method, and will treat the data correctly. ✓ Only share on a "need to know" basis. ✓ Password protect attachments. Share password separately, preferably verbally ✓ Mark email as private or confidential. ✓ Verify recipient's address before you click send. ✓Whenever possible redact sensitive/personal information from email messages and attachments	Only where the recipient does not have a UW email account and it is absolutely necessary to use this method for a business purpose. ✓ Be sure the recipient understands the risks involved, accepts this method, and will treat the data correctly. ✓ Only share on a "need to know" basis. ✓ Password protect attachments. Share password separately, preferably verbally ✓ Mark email as private or confidential. ✓ Verify recipient's address before you click send. ✓ Whenever possible redact confidential or private information from email messages and attachments	✓ Permitted
Network Data Storage			

Classification Type	HIGHLY SENSITIVE	PERSONAL/CONFIDENTIAL	NON-SENSITIVE/OPEN
N drive – Personal drive	✓ Permitted Please note you are **required** to use the shared 'O' drive for collaborative work between team members.	✓ Permitted Please note you are **required** to use the shared 'O' drive for collaborative work between team members.	✓ Permitted Please note that the N drive can be used for working documents. The O drive should be used for any departmental/institutional documents such as policies, handbooks, codes of practice, marking schemes, training materials.
O drive – Shared drive	✓ Access to highly sensitive files and folders should be restricted. Requests for access to restricted folders should be submitted via the IT Service Desk. ✓ If it is not appropriate to store certain work related information on your shared drive e.g. a disciplinary process, you should consider storing it as a password protected file in a restricted folder on the N drive.	✓ Access to highly sensitive files and folders should be restricted. Requests for access to restricted folders should be submitted via the IT Service Desk. ✓If it is not appropriate to store certain work related information on your shared drive e.g. a disciplinary process, you should consider storing it as a password protected file in a restricted folder.	✓ Permitted Please note that the N drive can be used for working documents. The O drive should be used for any departmental/institutional documents such as policies, handbooks, codes of practice, marking schemes, training materials.
Local computer drives e.g. C, D, E, etc.	**X Not permitted** University data is not permitted as this is not an approved backup solution.	**X Not permitted** University data is not permitted as this is not an approved backup solution.	**X Not permitted** University data is not permitted as this is not an approved backup solution.

Classification Type	HIGHLY SENSITIVE	PERSONAL/CONFIDENTIAL	NON-SENSITIVE/OPEN
Personal (home) computers	X Not permitted	X Not permitted	✓ Permitted
Cloud Storage			
The University approved cloud storage is OneDrive for Business, part of the Microsoft Office 365 account package, which is accessed with your University staff login. Further information is available via the ICT Service Desk	✓ Permitted	✓ Permitted	✓ Permitted
Non-University Cloud Storage such as iCloud, Google Drive, Dropbox, Personal OneDrive and all similar cloud storage solutions.	X Not permitted	X Not permitted	✓ Permitted Note documents should be backed up onto the University system as soon as possible
Laptops, mobile and			

Classification Type	HIGHLY SENSITIVE	PERSONAL/CONFIDENTIAL	NON-SENSITIVE/OPEN
small storage devices			
University owned laptops.	✓ Permitted only where the device has been encrypted, is being centrally managed by IT. ✓ Keep files away from public view when working off site. ✓ Only use laptop for work purposes. Please refer to the Mobile Device Encryption table for information on what level of encryption are available on the different operating systems currently available on University owned laptops.	✓ Permitted only where the device has been encrypted, is being centrally managed by IT. ✓ Keep files away from public view when working off site. ✓ Only use laptop for work purposes. Please refer to the Mobile Device Encryption table for information on what level of encryption are available on the different operating systems currently available on University owned laptops.	✓ Permitted
University owned mobile devices, e.g. tablets, smartphones, SSDs, USB flash drives, memory cards, etc.	✓ Permitted only where the device has been encrypted and is being centrally managed by IT. ✓ Keep files away from public view when working off site. Please refer to the Mobile Device Encryption table for information on what level of encryption are available on the different operating systems currently available on University owned laptops.	✓ Permitted only where the device has been encrypted and is being centrally managed by IT. ✓ Keep files away from public view when working off site. Please refer to the Mobile Device Encryption table for information on what level of encryption are available on the different operating systems currently available on University owned laptops.	✓ Permitted But access to University emails accounts must be password or pin protected

Classification Type	HIGHLY SENSITIVE	PERSONAL/CONFIDENTIAL	NON-SENSITIVE/OPEN
	For advice on encrypting USB flash drives please contact the IT Service Desk.	For advice on encrypting USB flash drives please contact the IT Service Desk.	
University supported portable storage devices including USB sticks encrypted in accordance with University requirements	**X Not permitted**	✓Permitted only where the device has been encrypted ✓ Staff must ensure that the personal storage device is stored securely	✓ Permitted
Personal laptops, tablets and smart phones	**X Not permitted** Note: Encrypted personal mobile devices may be used to access University information using one of the following options: - UW OnedriveforBusiness - VPN - N and O drive via Webmail They may not be used for storing and transporting information in this category. Devices should be pin-protected and users should ensure that files are kept away from public view when working off site	**X Not permitted** Note: Encrypted personal mobile devices may be used to access University information using one of the following options: - UW OnedriveforBusiness - VPN - N and O drive via Webmail They may not be used for storing and transporting information in this category Devices should be pin-protected and users should ensure that files are kept away from	✓ Permitted But access to University email must be password or pin protected.

Classification Type	HIGHLY SENSITIVE	PERSONAL/CONFIDENTIAL	NON-SENSITIVE/OPEN
Dictaphones and digital recorders Recordings are not permitted without the agreement, in advance, of all parties. There may be highly sensitive/confidential meetings or hearings that a participant requests that the meeting is recorded. In these circumstances, the use must be agreed in advance by all parties and a record kept of the consent. Transcription should be carried out by a person who was present at the meeting	✓ Permitted for research purposes subject to prior approval from the relevant ethics committee This is dependent on the Dictaphone or digital recorder being securely stored. The device used must be encrypted or contain an encrypted storage card and use a means of ensuring no unauthorised access, such as pin code. Where the device allows the user to transfer the recording electronically to a secure University storage solution, this should be done as soon as possible. All information must be removed from the device once it has been transcribed. The transcription should take place as soon as possible after the recording. Transcription services may be used subject to appropriate checks including a robust confidentiality agreement and secure transfer capabilities	✓ Permitted where authorised for University purposes ✓ This is dependent on the Dictaphone or digital recorder being securely stored ✓All information must be removed from the device once it has been transcribed. The transcription should take place as soon as possible after the recording. Whenever possible use a device which can be encrypted or contains an encrypted storage card. Where the device allows the user to transfer the recording electronically to a secure University storage solution, this should be done as soon as possible. All information must be removed from the device once it has been transcribed. The transcription should take place as soon as possible after the recording Individuals need to be aware that when interviewing subjects sometimes the information disclosed may change the category to highly confidential or sensitive and additional security measures need to be put in place Transcription services may be used (see requirements of High Sensitive category)	✓ Permitted where authorised for University purposes