Information Classification and Handling Policy

Version number	IG-ICHT-002
Date of Approval	11-07-2022
Approved by	UEB
Effective from	11-07-2022
Policy Officer	Information Governance Officer
Department	Information Assurance
Review Date	11-07-2025
Last Reviewed	N/A
Equality Impact Assessment	18-07-2022
Accessibility checked	18-07-2022

1. Purpose and Scope

1.1 This Policy sets out the framework for how data is classified and how it should be handled safely in accordance with that classification. This is to ensure compliance with data protection legislation and other legal and contractual obligations.

There are 3 classifications of data defined in this Policy: highly sensitive data, data which is deemed personal or confidential, and non-sensitive or open data.

This Policy outlines the definition of each data category in the classification table and provides examples.

Depending on the data classification, this Policy details how data must be stored, shared, and disposed of securely.

1.2 This Policy applies to all items of data that are processed through the University of Worcester ('the University') and its subsidiaries as further outlined below:

i) All those with access to University information systems, including staff, students, visitors and contractors.
ii) All data or information held in print or in electronic formats by the University including documents, spreadsheets and other paper and electronic data, images and video.
iii) All systems attached to University computer or telephone networks and any systems supplied by the University.
iv) All information processed by the University relating to its operational activities, regardless of whether the information is processed electronically or in paper form, including all communications sent to or from the University and any University information held on systems external to the University's network.
v) All University owned and personal Mobile Computing Devices being used to access the University's Information systems as well as University owned non-mobile computers. Non-mobile devices, such as personally owned desktop computers that are used outside University premises to access University information are also within the scope of this Policy.
vi) All external third parties that provide services to the University in respect of information processing facilities and business activities.

All staff and others processing data on the University's behalf must read and comply with it. Breaches of this Policy may lead to disciplinary action or other appropriate action being taken.

2. Related Policy and Guidance documents

This Policy should be read in conjunction with the following:

Document Name	Revision	Owner
IT Regulations	2.7	Chief Information Officer
University Data Protection Policy	1.0	University Secretary
IT Hardware Policy	1.2	Deputy Director of IT
IT Software Policy	1.1	Deputy Director of IT
IT Email Policy	1.0	Deputy Director of IT
User Account and Password Policy	1.1	Cyber Security Service Manager
Vulnerability and Patch Management Policy	1.2	Cyber Security Service Manager
Bring Your Own Device	1.0	Cyber Security Service Manager
Information Security Policy	1.1	Cyber Security Service Manager

In addition, further information about records and document management is available here.
For a list of legal definitions please refer to the Data Protection Policy.

3. Information Classification and Handling

Information is a fundamental University asset, required for the effective operation of the University and the services it offers, including teaching, learning and research; and administrative, management and commercial activities. The correct classification of information is important to help ensure the prevention of information leaks and to minimise the impact of such breaches if they do occur. As well as being good practice, it helps to ensure that the University remains compliant with Data Protection legislation, Freedom of Information regulations and other regulatory requirements. To ensure that University information can be both accessed, used and shared effectively, and also protected from inappropriate access, use or sharing, the following information management principles will apply:

i) Information is an Asset: Information is an asset that has value to the University and must be managed accordingly.
ii) Information is Shared: Users have access to the information necessary to carry out their duties; therefore, information is shared where permissible and appropriate.
iii) Information is Secure: Information is protected from unauthorised use and disclosure. In addition to traditional aspects of information security, such as the data protection legislation, this includes protection of sensitive and commercial information.
iv) Information is Responsibly Managed: All members of the University community have responsibility for ensuring the secure and appropriate use of information assets.

To support the operation of the above principles this Policy has been developed to ensure that all members of the University community understand the ways in which different kinds of information and data should be handled accordingly to their sensitivity.

3.1 Information Classification and Categories

3.1.1 Information classification is based on the level of sensitivity and the impact on the University, or an individual should that information be disclosed, altered, lost or destroyed without authorisation. The classification of all information into different categories ensures that individuals who have a legitimate reason to access a piece of information are able to do so, while at the same time ensuring that information is protected from those who have no right to access the information. The classification will guide the appropriate security and technical controls required.

3.1.2 All information owned, used, created or maintained within the University should be categorised into one of the following three categories:

- Non-Sensitive/Open
- Personal/Confidential
- Highly Sensitive

Where data contains personal information which relates to an identifiable living individual, it will always be categorised as 'Personal/Confidential' as a minimum. If the personal data contains any special category data (please see the definition below at 3.1.4) it will always be categorised as 'highly sensitive'. Only information which does not contain any personal data will be classified as 'Non-Sensitive/Open'.

3.1.3 It is important to note that one piece of information may have different classifications throughout its lifecycle; for instance, commercially sensitive information may become less sensitive over time. Where one set of information contains a range of information, such as a database, the highest classification must be applied to the whole set of information.

3.1.4 The University has a Policy which relates specifically to the processing of Special Category Data. 'Special Category Personal Data' is defined as information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person data concerning health, sex life or sexual orientation. This data is given the greatest protections under law, and we may only process it when strict conditions are met. All Special Category data shall be categorised as 'Highly Sensitive'.

4. Classification and Handling Table

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 • Special Category Data e.g., race or ethnicity, political opinions, religious belief, trade union membership, physical or mental health, sexual orientation, medical records, genetic or biometric data • Disciplinary proceedings • Security information • Legally privileged information	• Other personal information as defined by the UK GDPR (which does not fall in the 'Special Category' Data defined in the Highly Sensitive column). This includes personal identifiers such as name, identification number, contact details, location data and online identifiers such as IP addresses and cookie identifiers • • All further data relating to students • 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	• 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. • Where hard copy data is shared with individuals in face-to-face meetings, retrieve and securely dispose at the end of the meeting. Those receiving highly sensitive data must only make additional copies or edits with the originator's authority • Consideration should be given during online meetings whether it is appropriate to 'share your screen' when this is displaying Highly Sensitive information. This should only be done if essential and all attendees must ensure the data is kept confidential. This should not be done during recorded meetings where the recordings are due to be published/widely circulated. • Ensure data is kept up to date and hard copy records are stored in highly restricted areas within centrally managed shared areas or restricted physical storage areas subject to access control. • Data can be stored off-site using the University's approved secure storage provider.	know" basis within the University, or external to the University, to fulfil statutory and legal requirements Consideration should be given during online meetings whether it is appropriate to 'share your screen' when this is displaying Personal/Confidential information. This should only be done if essential and all attendees must ensure the data is kept confidential. This should not be done during recorded meetings where the recordings are due to be published/widely circulated. • Data should be kept up to date and hard copy records are stored in highly restricted areas within centrally managed shared areas or restricted physical storage areas subject to access control. • Data can be stored off-site in the University's approved secure storage provider. Further guidance is available from infoassurance@worc.ac.uk • Data should be securely deleted from 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
	• Data should be securely deleted from electronic devices where the device has been decommissioned, or disposal of paper records should follow Document Retention Policy guidelines.		

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 'Private and Confidential' with a return address if not delivered.	**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
	Use recorded delivery. Hand or courier delivery should also be considered where possible.	'Private and Confidential' with a return address if not delivered. Use recorded delivery. Hand or courier delivery should also be considered where possible.	
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 content 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
SharePoint and O drive	✓ Access to highly sensitive files and folders should be restricted. Requests for access to restricted folders on the O Drive 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 an access restricted folder on SharePoint.	✓ Access to highly sensitive files and folders should be restricted. Requests for access to restricted folders on the O drive 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 SharePoint.	✓ Permitted Whilst the O drive can be used for any departmental/institutional documents such as policies, handbooks, codes of practice, marking schemes, training materials. Staff should now be taking steps to migrate data across to SharePoint in accordance with IT guidance.
Local computer drives	**X Not permitted** Storage of University data to local computer drives is not permitted as this is not an approved backup solution.	**X Not permitted** Storage of University data to local computer drives is not permitted as this is not an approved backup solution.	**X Not permitted** Storage of University data to local computer drives 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**	**X Not 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

Classification Type	HIGHLY SENSITIVE	PERSONAL/CONFIDENTIAL	NON-SENSITIVE/OPEN
Laptops, mobile and 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	**X Not permitted**	**X Not permitted**	✓ 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/SharePoint - O drive via Webmail - Windows Virtual Desktop (WVD) 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/SharePoint - O drive via Webmail - Windows Virtual Desktop (WVD) 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