|  |  |  |  |
| --- | --- | --- | --- |
| **Classification Type** | **RESTRICTED** | **PRIVATE** | **PUBLIC** |
| **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  • Sensitive personal information e.g. race or ethnicity, political opinions, religious/philosophical beliefs, trade union membership, genetic or biometric data, health data, data concerning an individual’s sex life or sexual orientation, information relating to criminal offences.  • Disciplinary proceedings.  • Information where a legal or regulatory requirement may exist that requires for it to be classified as restricted. | • Personal information as defined by the Data Protection Act 1998 and GDPR (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 requires that stringent security controls are in place to maintain its confidentiality and integrity. | • Such information requires the most suitable security controls are in place in order to maintain its confidentiality and integrity. | • Such information should be available to University members and the general public  • It should be stored on centrally managed shared areas with |

|  |  |  |  |
| --- | --- | --- | --- |
| **Classification Type** | **RESTRICTED** | **PRIVATE** | **PUBLIC** |
|  | • 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 data owner’s authority.   * Ensure data is kept up to date and stored in restricted areas within centrally managed shared areas or restricted physical storage areas. * 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 changed ownership, been decommissioned, or disposal of paper records should follow the Disposal Policy. | • Access limited on a “need to  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 Disposal Policy | appropriate backup arrangements in place in line with University guidance  • It should be kept up to date and modified only by authorised personnel. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Classification Type** | **RESTRICTED** | **PRIVATE** | **PUBLIC** |
| **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 ‘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 ‘Private and Confidential’ with a return | * Permitted. Follow good records management procedures. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Classification Type** | **RESTRICTED** | **PRIVATE** | **PUBLIC** |
|  | * 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. | 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 USW  email accounts  **NOTE: The use of personal email accounts for USW 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.   **X Auto forwarding to personal email**  **accounts is not permitted.** | * 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.   **X Auto forwarding to personal email accounts is not permitted.** | * Permitted |

|  |  |  |  |
| --- | --- | --- | --- |
| **Classification Type** | **RESTRICTED** | **PRIVATE** | **PUBLIC** |
| **Sharing information**  **by Email between USW**  **and external accounts**  **NOTE: The use of personal email accounts for USW business is not permitted** | Only where the recipient does not have a  USW 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  USW 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 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Classification Type** | **RESTRICTED** | **PRIVATE** | **PUBLIC** |
| **DATA STORAGE** | | | |
| N drive – Personal  drive | * Permitted | * Permitted | * Permitted   Please note that the N drive can be used for working documents. The Shared O drive should be used for any departmental/institutional documents such as policies, handbooks, codes of practice, marking schemes, training materials. |
| S 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. | * Access to highly sensitive files and   folders should be restricted. Requests  for access to restricted folders should be submitted via the IT Service Desk. | * Permitted |
| Local computer drives | **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** | **RESTRICTED** | **PRIVATE** | **PUBLIC** |
| 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. | * 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** | **RESTRICTED** | **PRIVATE** | **PUBLIC** |
| **LAPTOPS, MOBILES 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. | * 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. | * Permitted |
| University owned  mobile devices, e.g. tablets, smartphones.. | * 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. | * 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. | * Permitted |

|  |  |  |  |
| --- | --- | --- | --- |
| **Classification Type** | **RESTRICTED** | **PRIVATE** | **PUBLIC** |
| Personally owned laptops | **X No storage permitted**   * May be used for read only remote connection to view files if used in a private environment. Encrypt drive. * Clear browser cache after read only use. * Do not leave logged in and unattended. * Back up on the device must be encrypted. | **X No storage permitted**   * May be used for read only remote connection to view files if used in a private environment. Encrypt drive. * Clear browser cache after read only use. * Do not leave logged in and unattended. * Back up on the device must be encrypted. | **X No master copy storage permitted** |
| Personally owned Smartphone or tablet | **X Avoid storage or creation of confidential information on device.**   * Device must be configured to connect via Exchange Active Sync to ensure baseline security features (timeout, password, encryption) are applied. * Back up on the device must be encrypted. | **X Avoid storage or creation of confidential**  **information on device.**   * Device must be configured to connect via Exchange Active Sync to ensure baseline security features (timeout, password, encryption) are applied. * Back up on the device must be encrypted. | **X No master copy storage permitted** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Classification Type** | **RESTRICTED** | **PRIVATE** | **PUBLIC** |
| Large Capacity Storage device (external hard drive) | **X Do not use to store master copy**   * Avoid use where possible. * Consider alternative means of access   instead e.g. Sharepoint.   * Encrypt device using a strong password. * Keep in lockable cabinet/drawer which is locked when unattended | **X Do not use to store master copy**   * Avoid use where possible. * Consider alternative means of access   instead e.g. Sharepoint.   * Encrypt device using a strong password. * Keep in lockable cabinet/drawer which is locked when unattended. | **X Do not use to store master copy.** |
| Dictaphones and digital recorders | **X Not permitted** | * 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. | * Permitted where authorised for   University purposes |
| Small capacity portable storage devices (USB and CD) | **X Do not use to store master copy.**   * Avoid use where possible. * Consider alternative means of access   instead e.g. Sharepoint.   * Encrypt device using a strong password. * Keep in lockable cabinet/drawer which is locked when unattended | **X Do not use to store master copy.**   * Avoid use where possible. * Consider alternative means of access   instead e.g. Sharepoint.   * Encrypt device using a strong password. * Keep in lockable cabinet/drawer which is locked when unattended | **X Do not use to store master copy.** |