| **Document Reference Number** | **UoG/ILS/IS/PRO 001** |
|---|---|
| Title | Procedure for Data Classification, Labelling and Handling |
| Owning Department | Information and Library Services |
| Version | 2.1 |
| Approved Date | 14/02/2024 |
| Approving Body | Information Assurance and Security Committee (IASC) |
| Review Date | 13/02/2025 |
| Classification | Public – Non-sensitive |

Version Control

| **Version** | **Last Modified** | **Last Modified By** | **Document Changes** |
|---|---|---|---|
| 2.1 | 14/02/2024 | Atif Siddique | Updated to include criminal convictions as highly sensitive information. Minor format changes. Accessibility review completed. |
| | | | |
| | | | |

**Procedure for Data Classification, Information Labelling and Handling**

## 1. Data Classification

The Data Classification Table details the university's data classification groups and the level of protection that applies to each group. The procedure supports the university Policy for Information Security & Privacy Impact Assessments and Secure Data Handling.

To determine the classification group for data, use The Data Classification and Information Labelling Flowchart.

## 2. Information Labelling

The Data Classification and Information Labelling Flowchart provides the steps for labelling documents according to the classification group of the data it holds. Use the Flowchart to label a document accordingly. Points to consider when labelling documents:

2.1.1 Information that falls under the Non-sensitive/Open Classification group does not require labelling.

2.1.2 Information that falls under the Highly Sensitive or Personal/Confidential classification groups should be handled as follows:

2.1.2.1 Paper document: **A plain sheet** should precede the front page of the document with the appropriate classification label at the top of the plain sheet, as defined below. The classification label should also be used as a header of each document page.

2.1.2.2 Digital document: Data should be stored in **restricted storage areas** as appropriate for the business need, and if practical, with the appropriate data classification label at the top of the front page of the document and in the file or folder name e.g. Special Education Needs Project [file name] – HIGHLY SENSITIVE [classification group].

2.1.3 The images below have been provided for labelling documents.

## 3. Information Handling

The Information Handling Requirements set out the expectation and steps for handing data appropriately and securely. Use the Requirements as guidance for handling data.

**4.** Exceptions to this procedure can only be granted by the university Information Assurance and Security Committee or an appropriate sub-group thereof.

**Data Classification Table**

| Classification Type | Highly Sensitive | Personal/Confidential | Non-sensitive/Open |
|---|---|---|---|
| Description | Inappropriate disclosure of such information may cause **severe damage** or distress to an individual or the University's objectives and/or reputation. | 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 organisation or other organisations e.g. a trade secret; commercially sensitive university strategy.<br>• Sensitive financial information e.g. contractual information at the time of tender.<br>• Unprotected intellectual property.<br>• Sensitive personal information e.g. race, ethnic origin, politics, religion, trade union, membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation, criminal convictions.<br>Some examples where this might occur include supplementary documents to CVs, equal opportunities forms, extenuating circumstances data, research data | • Personal information about individuals who can be identified from it. Some examples include their salary information, copies of CVs, contact details.<br>• Student information where they can be identified from it. Some examples include Banner IDs, marks, transcripts, coursework, exam scripts, images.<br>• Commercially sensitive information e.g. contractual information, or supplier information provided in confidence. | • Information which is in the public domain e.g. Policies, Academic regulations, annual financial accounts, prospectus information.<br>• Information which should be routinely disclosed e.g. some minutes of meetings. |

| | | | |
|---|---|---|---|
| | where human participants are involved.<br>• Sensitive IT information e.g. authentication details. | | |
| Level of Protection Required | • Such information requires a high level of security controls that will ensure its confidentiality and integrity is maintained at all times. It should only be shared under a very strict environment such as:<br>○ provide only hard copies to authorised individuals in face to face meetings and retrieve these copies at the end of a meeting. Where this is not possible, use email, post or hand delivery with the appropriate marking in place (refer to the data handling procedures below).<br>○ those receiving highly sensitive data must only make additional copies or edits with the originator's authority.<br>• and only on a "need-to-know" basis within the university, or external to the university, to fulfil statutory and legal requirements.<br>• It should be kept up-to-date and stored in highly restricted areas within | • 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 –know" basis within the university, or external to the university, to fulfil statutory and legal requirements.<br>• It should be kept up-to-date and stored in highly restricted areas within centrally managed shared areas or cloud storage, 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.<br>• Data should be securely wiped off electronic devices where the device has been decommissioned | • Such information should be available to university members and the general public.<br>• It should be stored on centrally managed shared areas or cloud storage areas with appropriate backup arrangements in place.<br>• It should be kept up-to-date and access to it should be limited to only to those authorised to make relevant changes to it.<br>• Disposal should follow normal file deletion or non-confidential paper record disposal procedures. |

| | | | |
|---|---|---|---|
| | centrally managed shared areas or cloud storage, 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.<br>• Data should be securely wiped off electronic devices where the device has been decommissioned, or disposal of paper records should follow confidential waste disposal procedures. Please refer to the the Policy for IT Asset Management and Disposal, Procedure for Disposal of IT Equipment and Code of Practice 6: Retention and Disposal of Records and Data. | or disposal of paper records should follow confidential waste disposal procedures. Please refer to the Policy for IT Asset Management and Disposal, Procedure for Disposal of IT Equipment and Code of Practice 6: Retention and Disposal of Records and Data. | |

**Information Handling Requirements**

| Type of Information/information asset | **Highly Sensitive** | Personal and Confidential | Non-sensitive/Open |
|---|---|---|---|
| **Paper records** | **University areas with restricted access:**<br>✓ Keep files in lockable cabinets/drawers which are locked when not in active use. | **University areas with restricted access:**<br>✓ Keep files in lockable cabinets/drawers when the office is unattended. | ✓ Permitted. Follow good records |

| | | | |
|---|---|---|---|
| | ✓ No papers left out when away from the desk.<br><br>**University areas with unrestricted access:**<br>✘ Not permitted<br><br>**Off-site working**<br>✓ At home: Should be kept away from public view and stored securely when not in use e.g. kept in lockable cabinets/drawers.<br><br>✓ Elsewhere or in transit: Not to be left unattended or in the car.<br><br>**Post**<br>✓ Must be addressed properly to a named individual, sealed and stamped with 'Private and Confidential' with a return address if not delivered.<br><br>✓ Use recorded delivery. Hand or courier delivery should also be considered where possible.<br><br>✓ It is recommended that the addressed envelope be enclosed in another sealed and properly addressed envelope.<br><br>Fax:<br>✘ Not permitted | ✓ No papers left out when away from the desk.<br><br>**University areas with unrestricted access:**<br>✘ Not permitted<br><br>**Off-site working**<br>✓ At home: Should be kept away from public view and stored securely when not in use e.g. kept in lockable cabinets/drawers.<br><br>✓ Elsewhere or in transit: Not to be left unattended or in the car.<br><br>**Post**<br>✓ Must be addressed properly to a named individual, sealed and stamped with 'Private and Confidential' with a return address if not delivered.<br><br>✓ Use recorded delivery. Hand or courier delivery should also be considered where possible.<br><br>✓ It is recommended that the addressed envelope be enclosed in another sealed and properly addressed envelope.<br><br>Fax<br>✘ Not permitted | management procedures. |

| Type of Information/information asset | **Highly Sensitive** | Personal/Confidential | Non-sensitive/Open |
|---|---|---|---|
| **Email** | | | |
| Between user@greenwich.ac.uk accounts | REQUIRED<br>✓ Only share on a "need-to-know" basis.<br>✓ If it is ad hoc or one-off document sharing, password-protect email attachments. See our information for encrypting files and folders.<br>For collaboration work, use Office 365 Teams.<br>✓ Mark email with private or confidential.<br>✓ Verify the recipient's address before you click send.<br>✓ Redact sensitive information from email messages and attachments if not relevant to all recipients particularly from email chains.<br>✓ Avoid putting Data Subject name(s) in the Subject field, where possible.<br>✘ Not permitted: Auto forwarding to personal email. | REQUIRED<br>✓ Only share on a "need-to-know" basis.<br>✓ If it is ad hoc or one-off document sharing, password-protect email attachments. See our information for encrypting files and folders.<br>For collaboration work, use Office 365 Teams.<br>✓ Mark email with private or confidential.<br>✓ Verify the recipient's address before you click send.<br>✓ Redact confidential or private information from email messages and attachments if not relevant to all recipients particularly from email chains.<br>✓ Avoid putting Data Subject name(s) in the Subject field, where possible.<br>✘ Not permitted: Auto forwarding to personal email. | ✓ Permitted |
| From user@greenwich.ac.uk to/from non-university email address: user@example.com | Only where the recipient does not have a Greenwich email account and it is necessary to use this method for a business purpose: | Only where the recipient does not have a Greenwich email account and it is necessary to use this method for a business purpose: | ✓ Permitted |

| | | | |
|---|---|---|---|
| | REQUIRED<br>✓ Be sure the recipient understands the risk involved, accepts this method, and will treat the data correctly.<br>✓ Only share on a "need-to-know" basis.<br>✓ Password-protect attachments.<br>✓ Mark email with private or confidential.<br>✓ Verify the recipient's address before you click send.<br>✓ Redact sensitive information from email messages and attachments if not relevant to all recipients particularly from email chains. | REQUIRED<br>✓ Be sure the recipient understands the risk involved, accepts this method, and will treat the data correctly.<br>✓ Only share on a "need-to-know" basis.<br>✓ Password-protect attachments.<br>✓ Mark email with private or confidential.<br>✓ Verify the recipient's address before you click send.<br>✓ Redact confidential or private information from email messages and attachments if not relevant to all recipients particularly from email chains. | |
| Between two non-university email accounts for work purposes user@example.com to user@example.com | ✗ Not permitted<br>**Only** use your @gre.ac.uk account to share. | ✗ Not permitted<br>**Only** use your @gre.ac.uk account to share. | ✗ Not permitted<br>**Only** use your @greenwich.ac.uk account to share university information. |
| **Drives** | | | |
| G drive – Personal drive | ✓ Permitted<br>You are required to use the shared drive (U) for work collaboration with team members or the university's Centrally Administered M365. | ✓ Permitted<br>You are required to use the shared drive (U) for work collaboration with team members or the university's Centrally Administered M365. | ✓ Permitted |
| U-drive – Shared drive | ✓ Store only in restricted folders on your shared drive U: (restricted folders can be | ✓ Store only in restricted folders on your shared drives – U: (restricted folders can | ✓ Permitted |

| | | | |
|---|---|---|---|
| | requested by contacting the IT Service Desk).<br>✓ 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 or on your G drive. | be requested by contacting IT Service Desk).<br>✓ 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. | |
| C drive – Local machine drive | ✘ Not permitted | ✘ Not permitted | ✘ Not permitted. University data is not permitted as the C drive is not backed up. |
| **Cloud storage** | | | |
| University Centrally Administered M365 including OneDrive for Business, Teams and SharePoint | ✓ Permitted<br>Ensure appropriate permissions are assigned to individuals only on a need to know basis, whether internal staff or external collaborators. Contact the IT Service Desk for support. | ✓ Permitted<br>Ensure appropriate permissions are assigned to individuals only on a need to know basis, whether internal staff or external collaborators. Contact the IT Service Desk for support. | ✓ Permitted |
| Non-University Administered Cloud Storage such as iCloud, Google Drive, Dropbox, personally owned OneDrive and any other cloud storage solutions | ✘ Not permitted<br>University data is not permitted for use on non-university administered or non-approved cloud platforms. | ✘ Not permitted<br>University data is not permitted for use on non-university administered or non-approved cloud platforms. | ✘ Not permitted<br>University data is not permitted for use on non-university administered or |

| | | | |
|---|---|---|---|
| | | | non-approved cloud platforms. |
| **Laptops, mobile and small storage devices** | | | |
| University-owned laptops | ✓ As of the date of the policy, all new university-owned laptops much be encrypted following the centrally agreed process.<br>✓ Permitted only where the device is centrally managed by ILS and the user does not have a local super-user account.<br>✓ Information must be password-protected and only saved temporarily on the C: drive where access to the shared drive is not possible and must be transferred immediately to the shared drive when access becomes available and deleted from the C: drive.<br>✓ Keep files away from public view when working offsite.<br>✓ Always use only issued laptops for work purposes and limit its use for personal purposes ensuring secure use. | ✓ As of the date of the policy, all new university-owned laptops much be encrypted following the centrally agreed process.<br>✓ Permitted only where the device is centrally managed by ILS and the user does not have a local super-user account.<br>✓ Information must be password-protected and only saved temporarily on the C: drive where access to the shared drive is not possible and must be transferred immediately to the shared drive when access becomes available and deleted from the C: drive.<br>✓ Keep files away from public view when working offsite.<br>✓ Always use only issued laptops for work purposes and limit its use for personal purposes ensuring secure use. | ✓ Permitted |
| University-owned mobile and portable storage devices e.g. smartphones, iPads, tablets, & USB | ✓ Permitted<br>Refer to the university's Policy for Mobile and Remote Working. | ✓ Permitted<br>Refer to the university's Policy for Mobile and Remote Working. | ✓ Permitted |

| | | | |
|---|---|---|---|
| Personal laptops, mobile devices and portable storage devices | ✘ Not permitted<br><br>In the rare case where an exception is permitted under section 4 of this document, university security controls are to be enabled on such devices.<br><br>Refer to the university's Policy for Mobile and Remote Working. | ✘ Not permitted<br><br>In the rare case where an exception is permitted under section 4 of this document, university security controls are to be enabled on such devices.<br><br>Refer to the university's Policy for Mobile and Remote Working. | ✓ Permitted |
| **Others** | | | |
| Faculty/Department-owned servers | ✓ Only permitted when the technical and governance review for servers and supporting systems is satisfactory. Please refer to the Policy for IT Asset Management and Disposal.<br><br>✓ Ensure server security and access controls align with university standards.<br><br>✓ Store only in restricted folders on the shared drive or an approved server.<br><br>✓ Password-protect files. | ✓ Only permitted when the technical and governance review for servers and supporting systems is satisfactory. Please refer to the Policy for IT Asset Management and Disposal.<br><br>✓ Ensure server security and access controls align with university standards.<br><br>✓ Store only in restricted folders on the shared drive or an approved server.<br><br>✓ Password-protect files. | ✓ Permitted |

**Data classification and Information labelling flowchart**

The flowchart provides the steps for classifying and labelling university information. Where information falls under more than one classification group, the more stringent classification group and labelling will apply.