**­­**A picture containing text

Description automatically generated

Information Security Classification and Handling Policy

# 1 PURPOSE AND SCOPE

## 1.1. The purpose of this policy is to establish a university-wide system of categorising information in relation to its sensitivity, confidentiality and value to the university, and to define associated rules for the handling of each category of information in order to ensure the appropriate level of security (confidentiality, integrity and availability) of that information.

## 1.2. This policy covers all information held by and on behalf of Cardiff University, including information used to support the research, teaching and administrative activities of the university. The handling rules shall apply to members of the University and to third parties handling University information.

## 1.3. Where the University holds information on behalf of another organisation with its own information classification agreement shall be reached as to which set of handling rules shall apply. This includes information held through research collaborations with other institutions and partners.

# 2. RELATIONSHIP WITH EXISTING POLICIES

## 2.1. This policy forms part of the Information Security Framework. It should be read in conjunction with the Information Security Policy and all supporting policies.

# 3. POLICY

## 3.1. All members of Cardiff University and third parties who handle information on behalf of Cardiff University have a personal responsibility for ensuring that appropriate security controls are applied in respect of the information they are handling for the University. Appropriate security controls may vary according to the classification of the information and the handling rules for the relevant category shall be followed.

## 3.2. All information held by or on behalf of Cardiff University shall be categorised according to the Information Classification Matrix (Annex 1).

## 3.3. Information shall be handled in accordance with the Information Handling Rules (Annex 2) and where information falls within more than one category, the higher level of protection shall apply in each case.

## 3.4. Where a third party, including other universities, will be responsible for handling information on behalf of Cardiff University, the third party shall be required by contract or data processing agreement to adhere to this policy prior to the sharing of that information.

## 3.5. Where the University holds information on behalf of another organisation, including other universities, with its own information classification, written agreement shall be reached as to which set of handling rules shall apply prior to the sharing of that information.

## 3.6. Breaches of this policy may be treated as a disciplinary matter dealt with under the University’s staff disciplinary policies or the Student Conduct Regulations as appropriate. Where third parties are involved breach of this policy may constitute breach of contract.

# 4. ROLES AND RESPONSIBILITIES

## 4.1. The **University Secretary**, in their role as the **Senior Information Risk Owner**, is the sponsor for this policy, and responsible for approving the need to develop or substantively amend the policy, for presenting the final draft to the approving body and for ensuring that their policy-making documents comply with, and are monitored and reviewed in line with the Cardiff University Policy for the Development of Policy-making Documents.

## 4.2. The **Senior Information Risk Owner** shall ensure that the Information Classification and associated Information Handling Rules are reviewed regularly to ensure they remain fit for purpose.

## 4.3. It shall be the responsibility of **every individual handling information** covered by this policy, to apply the appropriate handling rules to each category of information, and to seek clarification or advice from a line manager or the Compliance and Risk Team where they are unsure as to how to classify or handle information.

## 4.4. **All Line Managers are responsible for** ensuring that all local working practices, processes and procedures within their area of responsibility adhere to the handling procedures in Annex 2.

## 4.5. **Researchers** are responsible for ensuring research data is handled in accordance with this policy. In particular, researchers must ensure that:

* appropriate data sharing and processing agreements are in place for third parties handling university research data.
* precedence of information handling rules is established where the university holds research data on behalf of a third party.
* research data containing information that is private or sensitive and can be used to identify individuals is handled as confidential (C1) or highly confidential (C2) information.

## 4.6. **All members of the University** shall promptly report issues of concern in relation to the application of this policy, including alleged non-compliance, to the IT Service Desk.

# 5. DOCUMENT CONTROL

|  |  |  |
| --- | --- | --- |
| Document Name | Information Security Classification and Handling Policy | |
| UEB Policy Sponsor | University Secretary | |
| Policy Owner | Owen Hadall, Assistant Director IT Service & Operations | |
| Policy Author(s) | Owen Hadall, Assistant Director IT Service & Operations | |
| Version Number | 4.1 | |
| Equality Impact Outcome and Form Submission Date | An EIA has been conducted. The only areas of concern relate to the policy being accessible to those with visual impairments and Welsh speakers. It was noted that specific controls should be assessed as they are created or amended. | 23/01/2023 |
| Privacy Impact Assessment outcome (where applicable) | The risks to privacy and personal data arising from this policy have been assessed and found to be very low as it does require personal data to be collected for its implementation. The handling rules contained provide a framework for the storage and handling of information, and will aid safeguarding of personal and sensitive information. | 23/01/2023 |
| Approval Date | 7th March 2023 | |
| Approved By | Vice-Chancellor (UEB) | |
| Date of Implementation |  | |
| Date of Last Review | 15th January 2019 | |
| Date for Next Review | 7th March 2024 | |
| For Office Use – Keywords for search function | Information, Security, Policy, ISF, Classification, Handling, Guidance | |

|  |  |  |
| --- | --- | --- |
| **Classified C1**  **Highly Confidential** | **Classified C2**  **Confidential** | **NC**  **Non-Classified** |
| **Has the potential to cause serious damage or distress to individuals or serious damage to the University’s interests.**  This information requires signiﬁcant security controls to ensure its **confidentiality, availability** and **integrity** is safeguarded.  The information must be strictly controlled, have access limited, and protected from corruption or loss.  **Information is Classified C1 if it contains:**   * highly sensitive private information about individuals (living or deceased) and it is possible to identify those individuals, e.g. patient identifiable medical records, serious disciplinary matters, research data such as clinical trial records and genome data. * non-public information relating to business activity and has potential to seriously affect commercial interests and/or the University’s corporate reputation e.g. REF strategy. * non-public information that facilitates the protection of individuals’ personal safety or the protection of critical functions and key assets e.g. access codes for higher risk areas, University network passwords. * security sensitive research data. | **Has the potential to cause a negative impact on individuals’ or the University’s interests (but not falling into C1).**  This information requires signiﬁcant security controls to ensure its **confidentiality, availability** and **integrity** is safeguarded.  The information must be strictly controlled, have access limited, and protected from corruption or loss.  **Information is Classified C2 if it contains:**   * private information about individuals (living or deceased) and it is possible to identify those individuals, e.g. individual’s salaries, student assessment marks, research data such as research participants income and expenditure. * non-public information relating to business activity and has potential to affect financial interests and/or elements of the University’s reputation e.g. tender bids prior to award of contract, exam questions prior to use * non-public information that facilitates the protection of the University’s assets in general e.g. access codes for lower risk areas. | **Information not falling into either of the Classified categories.**  This information requires the i**ntegrity** and **availability** of information to be protected.  The information should be accessible to the University and protected from corruption or loss whilst it is required for business purposes.  **Examples of non-classified information include:**   * research data that does not include any private information about individuals or has met the bar for full anonymity. * research data containing pseudonymised private information about individuals, but decoded information and any keys used to decode must always be handled as C1 Highly Confidential information. * Information about current courses. * key information sets. * annual reports. * financial statements. * freedom of information disclosures. |

[A. GENERAL ADVICE FOR HANDLING INFORMATION 7](#_Toc150853624)

[B. ELECTRONIC/DIGITAL INFORMATION STORAGE 8](#_Toc150853625)

[University Teams and SharePoint Online file repositories for university internal use 8](#_Toc150853626)

[Shared drives (Typically S:, U:, R:\ and G:\) 8](#_Toc150853627)

[OneDrive for Business for internal university use 9](#_Toc150853628)

[Home Drive (H:\) 9](#_Toc150853629)

[Cloud file storage (Personal OneDrive, iCloud, DropBox, Google Drive, etc.) 10](#_Toc150853630)

[Research Data Store 10](#_Toc150853631)

[School/Department based servers and Network Attached Storage (NAS) 11](#_Toc150853632)

[University IT maintained databases and servers (including ARCCA) 11](#_Toc150853633)

[Small capacity devices for information storage (e.g. USB, DVD, CD, SD cards) 12](#_Toc150853634)

[Large capacity portable devices for information storage (i.e. external hard drive) 13](#_Toc150853635)

[Externally hosted and managed online data sources (not managed by University IT) 14](#_Toc150853636)

[C. ELECTRONIC/DIGITAL INFORMATION CREATION AND STORAGE 15](#_Toc150853637)

[University Desktop PC in non-public areas 15](#_Toc150853638)

[University Desktop PC in public areas (e.g. Open Access PCs) 15](#_Toc150853639)

[University owned Laptop 16](#_Toc150853640)

[University owned Smartphone or Tablet 18](#_Toc150853641)

[Personally owned Desktop PCs and Laptops 19](#_Toc150853642)

[Personally owned Smartphone or Tablet 20](#_Toc150853643)

[Audio, image, and video captures devices with onboard storage 21](#_Toc150853644)

[D. DIGITAL COLLABORATION 22](#_Toc150853645)

[Sharing content for collaboration with externals (Teams and OneDrive for Business) 22](#_Toc150853646)

[University instant messaging, i.e. Skype and Teams (including meeting chat) 23](#_Toc150853647)

[University Social Chat (Yammer) 23](#_Toc150853648)

[Other Social chat (including WhatsApp, Facebook Messenger, Slack and Discord) 23](#_Toc150853649)

[Internal only meeting recordings (from Teams and Zoom) 24](#_Toc150853650)

[Meeting recordings with externals (from Teams and Zoom) 24](#_Toc150853651)

[Generative AI (including Chat GPT and Google Bard) accessed through desktop software or the cloud 25](#_Toc150853652)

[E. ELECTRONIC TRANSMISSION 26](#_Toc150853653)

[Sending university data between university hosted email accounts 26](#_Toc150853654)

[Sending university data from a university hosted email account to an external account 26](#_Toc150853655)

[Fastfile (secure web based large file transfer) 27](#_Toc150853656)

[F. PAPER RECORDS AND OTHER RECORD STORAGE 28](#_Toc150853657)

[Paper records in restricted access university areas or in approved offsite storage 28](#_Toc150853658)

[Paper records in unrestricted access university areas 28](#_Toc150853659)

[Paper records for offsite working 29](#_Toc150853660)

[University provided Fax service 29](#_Toc150853661)

[Internal postal service 30](#_Toc150853662)

[External postal service 30](#_Toc150853663)

1. GENERAL ADVICE FOR HANDLING INFORMATION

Always aim to keep Classified Information (C1 and C2) secure within a managed environment, such as physically on the university campus or virtually in a robustly managed environment that adheres to the following handling rules.

Where this is not possible, the information must be handled in accordance with the [Remote and Mobile Working Policy](https://www.cardiff.ac.uk/__data/assets/pdf_file/0007/2466133/10_infosec_Remote_and_mobile_working_policy.pdf). Also consider whether the information can be redacted, pseudonymised, or anonymised to remove confidential or highly confidential information, thereby converting it to Non-Classified Information (NC).

Follow the requirements in the following tables to create, store and share information securely. You must follow guidance identified as ‘Required actions’.

Take extra care with master copies of information. Information should be considered to be a master file or copy of a vital record when it contains information that is relied upon by others, or it contains information that supports business processes.

Consider backup requirements in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?

Report any potential loss or unauthorised disclosure of Classified Information immediately to the IT Service Desk on ext. 11111.

Seek advice on secure disposal of equipment containing Classified Information via the IT Service Desk on ext. 11111.

Use the Confidential Waste Service for disposal of paper and small electronic media.

1. ELECTRONIC/DIGITAL INFORMATION STORAGE

| **Location and Key Features** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| --- | --- | --- | --- |
| University Teams and SharePoint Online file repositories for university internal use  Suitable for internal file sharing  University user account access permissions can be controlled  Deleted items are held for up to 90 days in a Recycle Bin, depending on user actions  High resilience and availability  For information on external sharing of SharePoint repositories, go to [Sharing content for collaboration with externals](#Sharing). | **Permitted with use of folders with access restricted to authorised recipients.** | **Permitted with use of folders with access restricted to authorised recipients.** | **Permitted.** |
| Consider:  File password protection as an additional measure for the most sensitive files. | Consider:  File password protection as an additional measure for the most sensitive files. |  |
| Shared drives (Typically S:\, U:\, R:\ and G:\)  University user account access permissions can be controlled  Backed up by University IT (90 days recovery period with University IT support)  Suitable for internal file sharing | **Permitted with use of folders with access restricted to authorised recipients.** | **Permitted with use of folders with access restricted to authorised recipients**. | **Permitted.** |
| Consider:  File password protection as an additional measure for the most sensitive files. | Consider:  File password protection as an additional measure for the most sensitive files. |  |
| OneDrive for Business for internal university use  Suitable for internal file sharing  University user account access permissions can be controlled  Deleted items are held for up to 90 days in a Recycle Bin, depending on user actions  High resilience and availability  For information on external sharing of files stored in OneDrive, go to [Sharing content for collaboration with externals](#Sharing). | **OneDrive is now the preferred storage for personal university files.** | | |
| **Permitted with use of folders with access restricted to authorised recipients.** | **Permitted with use of folders with access restricted to authorised recipients.** | **Permitted.** |
| Consider:  File password protection as an additional measure for the most sensitive files.  Does information need to be shared with colleagues – if so, move to shared storage areas.  How information you share from OneDrive will be available to others when you leave the University. | Consider:  File password protection as an additional measure for the most sensitive files  Does information need to be shared with colleagues – if so, move to shared storage areas.  How information you share from OneDrive will be available to others when you leave the University. | Consider:  Does information need to be shared with colleagues – if so, move to shared storage areas.  How information you share from OneDrive will be available to others when you leave the University. |
| Home Drive (H:\)  Not suitable for internal file sharing  User account access limited to a single University account  Backed up by University IT (90 days recovery period with University IT support) | **Home Drives have migrated to OneDrive – use OneDrive for personal file storage.**  **Only use Home Drives to save files created by software that cannot save to OneDrive.** | | |
| **Permitted.** | **Permitted.** | **Permitted.** |
| Required actions:  Do not use to store copies of master files or vital records – store these in shared storage areas. | Required actions:  Do not use to store copies of master files or vital records – store these in shared storage areas. | Required actions:  Do not use to store copies of master files or vital records – store these in shared storage areas. |
| Consider:  File password protection as an additional measure for the most sensitive files. | Consider:  File password protection as an additional measure for the most sensitive files. |  |
| Cloud file storage (Personal OneDrive, iCloud, DropBox, Google Drive, etc.)  Not suitable for internal file sharing  User account access permissions cannot be managed by the University  Information backup and resilience dependent on supplier arrangements | **Not permitted.** | **Not permitted.** | **Permitted.** |
| University business must be conducted via your university OneDrive for Business storage. | University business must be conducted via your university OneDrive for Business storage. | Required actions:  Do not use to store copies of master files or vital records – store these in university shared storage areas.  Recommended actions:  Where possible, you should always conduct university business through your university OneDrive for Business storage. |
|  |  |  |
| Research Data Store  May be suitable for internal and external file sharing  University user account access permissions can be controlled  Backed up by University IT (35 days recovery period with University IT support) | **Permitted but only grant access to those who need it.** | **Permitted but only grant access to those who need it.** | **Permitted.** |
| Consider:  File password protection as an additional measure for the most sensitive files. | Consider:  File password protection as an additional measure for the most sensitive files. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Location and Key Features** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| School/Department based servers and Network Attached Storage (NAS)  May be suitable for file storage and internal sharing  May have user account access permissions managed by University IT  Unlikely to be backed up by University IT | **Permitted for information storage or creation only where the server environment is to the standards defined by University IT for a server environment.** | **Permitted for information storage or creation only where the server environment is to the standards defined by University IT for a server environment.** | **Permitted.** |
| Required actions:  Use mechanisms to restrict access where online (web) access is required.  Seek advice from University IT on configuration, access rights, physical security of the server and backup. | Required actions:  Use mechanisms to restrict access where online (web) access is required.  Seek advice from University IT on configuration, access rights, physical security of the server and backup. | Recommended actions:  Seek advice from University IT on default access rights, physical security of the server and backup. |
| Consider:  File password protection as an additional measure for the most sensitive files.  Any requirements for data/system backup. | Consider:  Any requirements for data/system backup. | Consider:  Any requirements for data/system backup. |
| University IT maintained databases and servers (including ARCCA)  May be suitable for file sharing  University user account access permissions can be controlled  May be backed up by University IT | **Permitted.** | **Permitted.** | **Permitted.** |
| Required actions:  Seek advice from IT Services on access rights and configuration.  Use mechanisms to restrict access where online (web) access is required. | Required actions  Seek advice from IT Services on access rights and configuration.  Use mechanisms to restrict access where online (web) access is required. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Location and Key Features** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| Small capacity devices for information storage (e.g. USB, DVD, CD, SD cards)  Not suitable for file storage  No University managed access controls - user and physical access subject to local controls  Not backed up by University IT  Where this storage is used in an audio, image, or video capture device, refer to guidance for [Audio, image, and video captures devices with onboard storage](#Audio). | **Not permitted** | **Permitted but not recommended - avoid use where possible. .** | **Permitted.** |
| Use an alternative university service for information storage, such as OneDrive for Business, Teams, or the Research Data Store. | Required actions:  Consider alternative means of access instead, e.g. use secure remote connection (e.g. MyFiles, CIFS) to access files without downloading them.  Encrypt the media using a strong password (see advice on [setting strong passwords](https://intranet.cardiff.ac.uk/staff/supporting-your-work/it-support/security-and-scams/setting-a-strong-password) on the intranet) The device needs to implement FIPS 140-2 or FIPS 197 encryption standards.  Do not use to store copies of master files or vital records.  Keep the media in a lockable cabinet or drawer which is locked when unattended – this applies to on and off campus working locations.  Do not leave the media unattended at any point if you are travelling with it. | Required actions  Do not use to store copies of master files or vital records. |
|  | Consider:  Not suitable for long term storage – consider an alternative university service for information storage, such as OneDrive for Business, Teams or the Research Data Store. | Consider:  Not suitable for long term storage – consider an alternative university service for information storage, such as OneDrive for Business, Teams, or the Research Data Store. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Location and Key Features** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| Large capacity portable devices for information storage (i.e. external hard drive)  Not suitable for file storage  No University managed access controls - user and physical access subject to local controls  Not backed up by University IT  Where this storage is used in an audio, image or video capture device, refer to guidance for [Audio, image and video captures devices with onboard storage](#Audio). | **Not Permitted.** | **Permitted.** | **Permitted.** |
| Use an alternative university service for information storage, such as OneDrive for Business, Teams or the Research Data Store. | Required actions:  Encrypt the media using a strong password (see advice on [setting strong passwords](https://intranet.cardiff.ac.uk/staff/supporting-your-work/it-support/security-and-scams/setting-a-strong-password) on the intranet)  The device needs to implement FIPS 140-2 or FIPS 197 encryption standards.  Do not use to store copies of master files or vital records.  Keep the media in a lockable cabinet or drawer which is locked when unattended – this applies to on and off campus working locations.  Do not leave the media unattended at any point if you are travelling with it. | Required actions:  Do not use to store copies of master files or vital records. |
|  | Consider:  Using an alternative university service for information storage, such as OneDrive for Business, Teams or the Research Data Store. | Consider:  Using an alternative university service for information storage, such as OneDrive for Business, Teams or the Research Data Store. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Location and Key Features** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| Externally hosted and managed online data sources (not managed by University IT)  May not be suitable for information storage or sharing  User account access permissions cannot be managed by the University  Information backup and resilience dependent on supplier arrangements | **Permitted where contractual commitments to protect data and a data processing agreement are in place.** | **Permitted where contractual commitments to protect data and a data processing agreement are in place.** | **Permitted.** |
| Required actions:  Do not use to store or share information where a contract or data processing agreement is not in place.  Refer the requirement to the IT Consultation Group for advice. | Required actions:  Do not use to store or share information where a contract or data processing agreement is not in place.  Refer the requirement to the IT Consultation Group for advice. | Required actions:  Ensure appropriate commitments from the supplier to information data have been sought. |
| Consider:  Are there existing university provided solutions that can provide the same capability. | Consider:  Are there existing university provided solutions that can provide the same capability. | Consider:  Are there existing university provided solutions that can provide the same capability. |

1. ELECTRONIC/DIGITAL INFORMATION CREATION AND STORAGE

| **Device and Key Features** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| --- | --- | --- | --- |
| University Desktop PC in non-public areas  Not suitable for internal file storage  Access limited to university user accounts  Local drives are not backed up by University IT | **Permitted.** | **Permitted.** | **Permitted.** |
| Required actions:  Ensure the drive is encrypted and/or password protect files.  Ensure the screen is locked if left unattended. | Required actions:  Ensure the drive is encrypted and/or password protect files.  Ensure the screen is locked if left unattended. |  |
| Recommended actions:  Store information in university provided storage solutions, such as OneDrive for Business, Shared drive, or Teams, rather than on the local device. | Recommended actions:  Store information in university provided storage solutions, such as OneDrive, Shared drive, or Teams, rather than on the local device. | Recommended actions:  Store information in university provided storage solutions, such as OneDrive, Shared drive or Teams, rather than on the local device.  Ensure the screen is locked if left unattended. |
| Consider:  Any requirements for data backup. | Consider:  Any requirements for data backup. | Consider:  Any requirements for data backup. |
| University Desktop PC in public areas (e.g. Open Access PCs)  Not suitable for internal file sharing  Access limited to university user accounts  Local drives are not backed up by University IT | **Not permitted due to the high risk of incidental exposure.** | **Not permitted due to the high risk of incidental exposure.** | **Permitted.** |
|  |  | Recommended actions:  Store information in university provided storage solutions, such as OneDrive, Shared drive, or Teams, rather than on the local device.  Consider:  Any requirements for data backup. |

| **Device and Key Features** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| --- | --- | --- | --- |
| University owned Laptop  Not suitable for internal file sharing  Access may be limited to university user accounts, dependent on configuration  Local drives are not backed up by University IT  Continued on the next page | **Permitted.** | **Permitted.** | **Permitted.** |
| Required actions:  Ensure the device is encrypted and set to lock after a maximum of 10 minutes inactivity.  Ensure device/user accounts have a strong password.  The device needs to implement FIPS 140-2 or FIPS 197 encryption standards.  Use secure remote connection (e.g. MyFiles, CIFS, OneDrive for Business, Teams) to access files, and avoid download to the device and local storage.  Do not work on files in public areas.  Do not use to store copies of master files or vital records.  Do not leave logged in and unattended.  Do not share use of the device with non-University staff. | Required actions:  Ensure the device is encrypted and set to lock after a maximum of 10 minutes inactivity.  Ensure device/user accounts have a strong password.  The device needs to implement FIPS 140-2 or FIPS 197 encryption standards.  Use secure remote connection (e.g. MyFiles, CIFS, OneDrive for Business, Teams) to access files, and avoid download to the device and local storage.  Do not work on files in public areas.  Do not use to store copies of master files or vital records.  Do not leave logged in and unattended.  Do not share use of the device with non-University staff. | Required actions:  Do not use to store copies of master files or vital records.  Do not leave logged in and unattended.  Do not share use of the device with non-University staff. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Device and Key Features** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| **University owned Laptop (continued)** | Recommended actions:  Store created information in university provided storage solutions, such as OneDrive for Business, Shared drive, or Teams.  Consider:  Any requirements for data backup. | Recommended actions:  Store created information in university provided storage solutions, such as OneDrive for Business, Shared drive, or Teams.  Consider:  Any requirements for data backup. | Recommended actions:  Store created information in university provided storage solutions, such as OneDrive for Business, Shared drive, or Teams.  Consider:  Any requirements for data backup. |

| **Device and Key Features** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| --- | --- | --- | --- |
| University owned Smartphone or Tablet  Not suitable for internal file sharing  Access may be limited to university user accounts, dependent on configuration  Local storage is not backed up by University IT | **Permitted.** | **Permitted.** | **Permitted.** |
| Required actions:  The device must be configured to connect via Exchange Active Sync to ensure baseline security features (including timeout, password, encryption) are applied.  Services to locate device and remote wipe in case of loss/theft must be enabled.  Do not leave unattended or work on highly confidential files in public areas.  Do not share use of the device with non-University staff.  May be used for secure remote connection (e.g. MyFiles, CIFS, Teams, OneDrive for Business, SharePoint) to access files, and avoid download to the device and local storage. | Required actions:  The device must be configured to connect via Exchange Active Sync to ensure baseline security features (including timeout, password, encryption) are applied.  Services to locate device and remote wipe in case of loss/theft must be enabled.  Do not leave unattended or work on confidential files in public areas.  Do not share use of the device with non-University staff.  May be used for secure remote connection (e.g. MyFiles, CIFS, Teams, OneDrive for Business, SharePoint) to access files, and avoid download to the device and local storage. | Required actions:  Do not leave unattended in public areas.  Do not share use of the device with non-University staff. |
| Recommended actions:  Store created information in university provided storage solutions, such as OneDrive for Business, Shared drive, or Teams.  Consider:  Any requirements for data backup. | Recommended actions:  Store created information in university provided storage solutions, such as OneDrive for Business, Shared drive, or Teams.  Consider:  Any requirements for data backup. | Recommended actions:  Store created information in university provided storage solutions, such as OneDrive, Shared drive, or Teams.  Consider:  Any requirements for data backup. |
| **Device and Key Features** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| Personally owned Desktop PCs and Laptops  Not suitable for internal file sharing or storage  Access not limited to university user accounts  Local drives are not backed up by University IT | **Permitted for access and viewing of information – avoid use for information creation and do not use for storage.** | **Permitted for access and viewing of information – avoid use for information creation and do not use for storage.** | **Permitted.** |
| May be used for remote connection to access files in a private environment, with use of a VPN and if the disk is encrypted. The device needs to implement FIPS 140-2 or FIPS 197 encryption standards.  Required actions:  Clear web browser cache after read only use.  Do not leave logged in and unattended.  Do not download files to this device.  Do not store created information on the device – store on a university device or in university provided storage solutions, such as OneDrive for Business, Shared drive or Teams. | May be used for remote connection to access files in a private environment, with use of a VPN and if the disk is encrypted. The device needs to implement FIPS 140-2 or FIPS 197 encryption standards.  Required actions:  Clear web browser cache after read only use.  Do not leave logged in and unattended.  Do not download files to this device.  Do not store created information on the device – store on a university device or in university provided storage solutions, such as OneDrive for Business, Shared drive, or Teams. | Required actions:  Do not use to store copies of master files.  Do not leave logged in and unattended.  Do not store created information on the device – store on a university device or in university provided storage solutions, such as OneDrive, Shared drive or Teams. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Location and Key Features** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| Personally owned Smartphone or Tablet  Not suitable for internal file sharing  Access not limited to university user accounts  Local storage is not backed up by University IT | **Permitted for access and viewing of information – avoid use for information creation and do not use for storage.** | **Permitted for access and viewing of information – avoid use for information creation and do not use for storage.** | **Permitted, may be used for remote connection to access files.** |
| Required actions:  The device must be configured to connect via Exchange Active Sync to ensure baseline security features (including timeout, password, encryption) are applied.  Do not leave logged in and unattended.  Do not download files to this device.  Do not store created information on the device – store on a university device or in university provided storage solutions, such as OneDrive for Business, Shared drive, or Teams. | Required actions:  The device must be configured to connect via Exchange Active Sync to ensure baseline security features (including timeout, password, encryption) are applied.  Do not leave logged in and unattended.  Do not download files to this device.  Do not store created information on the device – store on a university device or in university provided storage solutions, such as OneDrive for Business, Shared drive or Teams. | Required actions:  Do not use to store copies of master files.  Do not store created information on the device – store on a university device or in university provided storage solutions, such as OneDrive for Business, Shared drive or Teams.  Do not leave logged in and unattended. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Location and Key Features** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| Audio, image, and video captures devices with onboard storage  (using DVD, CD, SD Cards, or inbuilt hard disks to store captured information)  Not suitable for file storage  Access not restricted to university users without appropriate controls  Local storage is not backed up by University IT | **Permitted for information capture and temporary storage – transfer to a university supplied storage solution as soon as possible.** | **Permitted for information capture and temporary storage – transfer to a university supplied storage solution as soon as possible.** | **Permitted.** |
| Required actions:  The device storage must be encrypted wherever possible, ideally to FIPS 140-2 or FIPS 197 encryption standards.  Where available, user accounts and passwords/pin codes should be implemented to restrict device access.  Do not download files to this device.  Transfer created information off the device as soon as possible after creation – store on university provided storage solution, such as OneDrive for Business, Research Data Store, Shared drive, or Teams.  Do not leave unattended. | Required actions:  The device storage must be encrypted wherever possible, ideally to FIPS 140-2 or FIPS 197 encryption standards.  Where available, user accounts and passwords/pin codes should be implemented to restrict device access.  Do not download files to this device.  Transfer created information off the device as soon as possible after creation – store on university provided storage solution, such as OneDrive for Business, Research Data Store, Shared drive or Teams.  Do not leave unattended. | Required actions:  Do not use to store copies of master files.  Do not store created information on the device – store in university provided storage solutions, such as OneDrive for Business, Shared drive or Teams.  Do not leave unattended. |

1. DIGITAL COLLABORATION

| **Location or Service** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| --- | --- | --- | --- |
| Sharing content for collaboration with externals (Teams and OneDrive for Business) | **Permitted if access is restricted to authorised recipients who are subject to existing information sharing agreement.** | **Permitted if access is restricted to authorised recipients who are subject to existing information sharing agreement.** | **Permitted.** |
| Required actions:  Ensure there is a named owner to manage all access.  Limit access to only the information that externals require access to.  Remove access for externals at the earliest opportunity, e.g. at the end of a research collaboration. | Required actions:  Ensure there is a named owner to manage all access.  Limit access to only the information that externals require access to.  Remove access for externals at the earliest opportunity, e.g. at the end of a research collaboration. | Required actions:  Ensure there is a named owner to manage all access.  Limit access to only the information that externals require access to.  Remove access for externals at the earliest opportunity, e.g. at the end of a research collaboration. |
| Consider:  How information you share from OneDrive for Business will be available to others when you leave the University. | Consider:  How information you share from OneDrive for Business will be available to others when you leave the University. | Consider:  How information you share from OneDrive for Business will be available to others when you leave the University. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Location or Service** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| University instant messaging, i.e. Skype and Teams (including meeting chat) | **Permitted only in chats where all participants are authorised to handle the information.** | **Permitted only in chats where all participants are authorised to handle the information** | **Permitted.** |
| Required Actions:  Exercise extreme caution when sharing information (including files) in the messaging and ensure only those who are authorised have access to the information. Where this cannot be guaranteed, identify an alternative way to share the information using secure transfer mechanisms. | Required Actions:  Exercise extreme caution when sharing information (including files) in the messaging and ensure only those who are authorised have access to the information. Where this cannot be guaranteed, identify an alternative way to share the information using secure transfer mechanisms. |  |
| University Social Chat (Yammer) | **Not permitted.**  Due to its open community nature, Yammer cannot adequately secure confidential data - use an alternative collaboration method. | **Not permitted.**  Due to its open community nature, Yammer cannot adequately secure confidential data - use an alternative collaboration method. | **Permitted.**  Required actions:  Ensure all users are aware that the platform must not be used for confidential information. |
| Other Social chat (including WhatsApp, Facebook Messenger, Slack and Discord) | **Not permitted.**  University business must be conducted via a university messaging service or use an alternative collaboration method. | **Not permitted.**  University business must be conducted via a university messaging service or use an alternative collaboration method. | **Permitted only where use is tightly regulated and controlled to avoid accidental disclosure.**  Required actions:  Ensure all users are aware that the platform must not be used for confidential information. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Location or Service** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| Internal only meeting recordings (from Teams and Zoom) | **Permitted if access is restricted to authorised recipients.** | **Permitted if access is restricted to authorised recipients.** | **Permitted.** |
| Required actions:  Teams recordings are saved to OneDrive for Business – follow the advice for [managing content on OneDrive](#OneDrive).  Zoom recordings to Zoom Cloud are not permitted for this category of data but may be captured in Panopto subject to access being restricted to meeting attendees only. | Required actions:  Teams recordings are saved to OneDrive for Business – follow the advice for [managing content on OneDrive](#OneDrive).  Zoom recordings to Zoom Cloud are not permitted for this category of data but may be captured in Panopto subject to access being restricted to meeting attendees only. |  |
| Meeting recordings with externals (from Teams and Zoom) | **Permitted if access is restricted to authorised recipients who are subject to existing information sharing agreement.** | **Permitted if access is restricted to authorised recipients who are subject to existing information sharing agreement.** | **Permitted.** |
| Required actions:  Following the guidance for [sharing content with externals.](#Sharing) | Required actions:  Following the guidance for [sharing content with externals.](#Sharing) | Required actions:  Following the guidance for [sharing content with externals.](#Sharing) |

|  |  |  |  |
| --- | --- | --- | --- |
| **Location or Service** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| Generative AI[[1]](#footnote-2) (including Chat GPT and Google Bard) accessed through desktop software or the cloud | **Generative AI platforms are a new and evolving technology that are attracting media and government attention.**  **This advice will be updated as their capabilities develop, and more information becomes available.** | | |
| **Not permitted.**  It is currently unclear where confidential information entered into generative AI platforms is processed and stored.  It is therefore not appropriate to generate or issue requests to generative AI platforms that include highly confidential information for any purpose (including for research). | **Not permitted.**  It is currently unclear where confidential information entered into generative AI platforms is processed and stored.  It is therefore not appropriate to generate or issue requests to generative AI platforms that include confidential information for any purpose (including for research). | **Permitted.**  Required actions:  Ensure that no classified information is included in any processing or action requested of the generative AI platform. |

1. ELECTRONIC TRANSMISSION

| **Transfer method** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| --- | --- | --- | --- |
| Sending university data between university hosted email accounts  **From:** @cardiff.ac.uk  **To:** @cardiff.ac.uk | **Permitted.** | **Permitted.** | **Permitted.** |
| Required action:  Mark the email as confidential. | Required action:  Mark the email as confidential. |  |
| Consider:  Whether sender or recipient may have delegated authority to others to access the account. | Consider:  Whether sender or recipient may have delegated authority to others to access the account. |  |
| Sending university data from a university hosted email account to an external account  **From:** @cardiff.ac.uk  **To:** @xxxx.xxx | **Permitted.** | **Permitted.** | **Permitted.** |
| Required actions:  Attachments must be password protected.  Mark the email as confidential.  Check the recipient identity and details - get their permission to use the destination account.  Do not auto forward to a personal email account from your university account – this is not permitted. | Required actions:  Mark the email as confidential.  Check the recipient identity and details - get their permission to use the destination account.  Do not auto forward to a personal email account from your university account – this is not permitted. | Required actions:  Do not auto forward to a personal email account from your university account – this is not permitted. |
| Consider:  Whether sender or recipient may have delegated authority to others to access the account. | Consider:  Whether sender or recipient may have delegated authority to others to access the account. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Transfer method** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| **Sending university data from one external account to another**  **From:** @xxxx.xxx  **To:** @xxxx.xxx | **Not permitted.**  University business must be conducted via your university email account. Use the university provided email service to send the message. | **Not permitted.**  University business must be conducted via your university email account. Use the university provided email service to send the message. | **Not permitted.**  University business must be conducted via your university email account. Use the university provided email service to send the message. |
| Fastfile (secure web based large file transfer)  Suitable for file sharing, especially large files and for transfer outside the University  User account access permissions can be controlled | **Permitted.** | **Permitted.** | **Permitted.** |
| Required actions:  Ensure you have confirmed the details and identity of the recipient.  Files must be password protected.  Mark the files as confidential. | Required actions:  Ensure you have confirmed the details and identity of the recipient.  Files must be password protected.  Mark the files as confidential. |  |
| Consider:  Whether sender or recipient may have delegated authority to others to access the account. | Consider:  Whether sender or recipient may have delegated authority to others to access the account. |  |

1. PAPER RECORDS AND OTHER RECORD STORAGE

|  |  |  |  |
| --- | --- | --- | --- |
| **Record Type** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| Paper records in restricted access university areas or in approved offsite storage | **Permitted.** | **Permitted.** | **Permitted.** |
| Required actions:  Store in lockable cabinet/drawer which is locked when not in active use.  Do not leave papers out unless being actively worked on. | Required actions:  Store in lockable cabinet/drawer which is locked when not in active use.  Do not leave papers out unless being actively worked on. |  |
| Consider:  Protection from fire and flood damage. | Consider:  Protection from fire and flood damage. | Consider:  Protection from fire and flood damage. |
| Paper records in unrestricted access university areas | **Not Permitted.** | **Permitted.** | **Permitted.** |
| Create as or convert to electronic documents and a use secure remote connection with a permitted device. | Required actions:  Store in lockable cabinet/drawer which is locked when not in active use.  Do not leave papers out unless being actively worked on. |  |
|  | Consider:  Creating as or convert to electronic documents and a use secure remote connection with a permitted device.  Protection from fire and flood damage. | Consider:  Protection from fire and flood damage. |
| **Record Type** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| Paper records for offsite working | **Not Permitted.** | **Permitted.** | **Permitted.** |
| Create as or convert to electronic documents and store on an appropriate university supplier storage location, accessing it using secure remote connection with a permitted device. | Required actions:  If needed to be taken off site, a backup copy must be made beforehand and stored securely onsite.  Not to be left unattended and to be locked away in secure (lockable) storage when not in use. |  |
|  | Shred documents at home or return to confidential waste on campus when the documents are no longer needed. | Consider:  A backup copy beforehand and store onsite. |
| University provided Fax service | **Permitted.** | **Permitted.** | **Permitted.** |
| Required actions:  Check the security of the receiving machine and that the recipient is at machine awaiting receipt. | Required actions:  Check the security of the receiving machine and that the recipient is at machine awaiting receipt. |  |
| Consider:  Converting the papers to an electronic format and using a secure electronic transfer method instead e.g. Fastfile. | Consider:  Converting the papers to an electronic format and using a secure electronic transfer method instead e.g. Fastfile. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Record Type** | **Classified C1**  **HIGHLY CONFIDENTIAL** | **Classified C2**  **CONFIDENTIAL** | **NC**  **NOT CLASSIFIED** |
| Internal postal service | **Permitted.** | **Permitted.** | **Permitted.** |
| Required actions:  Place papers in a sealed envelope marked confidential and with the sender details. | Required actions:  Place papers in a sealed envelope marked confidential and with the sender details. |  |
| Consider:  Hand delivering the papers.  Making a backup copy before posting. | Consider:  Hand delivering the papers.  Making a backup copy before posting. | Consider:  Making a backup copy before posting. |
| External postal service | **Permitted.** | **Permitted.** | **Permitted.** |
| Required actions:  Send via tracked and recorded delivery service, double wrapped (2 envelopes) and marked confidential. | Required actions:  Send via tracked and recorded delivery service, double wrapped (2 envelopes) and marked confidential. |  |
| Consider:  Making a backup copy before posting. | Consider:  Making a backup copy before posting. | Consider:  Making a backup copy before posting. |

1. Generative artificial intelligence or generative AI is a type of artificial intelligence (AI) system capable of generating text, images, or other media in response to prompts. Generative AI models learn the patterns and structure of their input training data, and then generate new data that has similar characteristics. (source: [Generative artificial intelligence - Wikipedia](https://en.wikipedia.org/wiki/Generative_artificial_intelligence)). [↑](#footnote-ref-2)