Information Classification Procedure

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer
Mary Liddell
Data Protection Officer

Document control

Version history

Version	Author	Date	Comments
0.1	Andrew Clarke	28 Mar 2016	First draft
0.2	Andrew Clarke	10 Nov 2016	Amendments to handling University Confidential data
0.3	Andrew Clarke	15 Dec 2016	Update to include reference to Cloud storage (e.g. Dropbox) and Office365 – page 12
0.4	Andrew Clarke	21 Dec 2016	Revisions from Information Access Officer
1.0	Andrew Clarke	06 Apr 2017	Approved - Exec
1.1	Andrew Clarke	17 Aug 2017	Amend Mick Jenkins role to CISO; Encryption required for external communications not for internal. More email controls for UC information detailed.
1.2	Andrew Clarke	08 Oct 2019	DPO Amendment:4.2 Special Category Data always UC

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

This document requires the approval from BUL as defined in the ISMS Compliance document.

A Clarke	Mick Jenkins
Document Owner: Andrew Clarke	Document Approver: Mick Jenkins
Cyber & Information Security Manager	Chief Information Security Officer

Document Distribution

Name	Title	Version	Date of Issue

1.0 About this document

1.1 Purpose of Document

The University generates and holds a wide variety of information that must be protected against unauthorised access, disclosure, modification, or other misuse. Efficient management of such assets is also necessary in order to comply with legal and regulatory obligations such as the Data Protection Act, and to ensure efficient handling of Freedom of Information requests.

Different types of information require different security measures and hence proper classification of information assets is vital to ensuring effective information security and management. This Information Classification Policy is intended to help staff and students to determine what information can be disclosed to external parties, as well as the relative sensitivity of information that should not be disclosed outside of the University without proper authorisation.

This procedure, along with the BUL-POL-8.02 Information Classification policy, assists all members of the University to ensure that correct classification and handling methods are applied during their day-to-day activities and information is managed accordingly.

- University information assets should be made available to all those who have a legitimate need to access them;
- The integrity of information must be maintained; information must be accurate, complete, timely and consistent with other related information and events.

Please refer to BUL-GLOS-000 - SyOPs for the glossary of terms, acronyms and their definitions for the suite of BUL ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Asset Owners (as identified by the University)	• Are responsible for determining the classification of their assets • To ensure assets are correctly labelled and for any steps necessary to ensure their correct handling in line with their classification. • Are responsible for appropriate delegation to custodians
Cyber & Information Security Manager	• Is responsible for maintaining the inventory of assets and services together with their classification levels
Systems Manager	• Is responsible for technical labelling mechanisms

All Managers	• Are responsible for providing direction, as appropriate, on mail/postal services, voice mail and voice communication, fax machines, photocopiers, couriers, and sensitive documents for ensuring that these media or information types are handled in line with these requirements
All employees	• Any user of University information assets (including mobile phones, laptops and/or other peripherals) may have specific custodianship responsibilities identified in their user agreements and have a responsibility to adhere to this policy

ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A8 – Asset management
ISO 27001:2013 Conformance Control	Information Classification Objective A.8.2 - Information Classification

1.3 Scope

This policy applies to:

- All University data held on any medium, including all forms of hard copy and electronic data.
- All University Colleges, Research Institutes, Administrative and Service Departments.
- All contractors, third party suppliers and external stakeholders.

Contents:

1. Introduction

1.1 Data is one of the University's most valuable assets. It is important that the University takes appropriate care of the information it holds and uses. The classification of information forms a pivotal part of this process and is a core requirement of the University's Information Security and Data Protection policies. In addition to protection of the University's data, the use of a recognised information classification framework in line with best practice will facilitate the effective sharing of information. The guidelines set out three main classifications in ascending order of sensitivity.

- **UNCLASSIFIED**
- **PROTECT**
- **UNIVERSITY CONFIDENTIAL**

1.2 Note that UNIVERSITY CONFIDENTIAL classification may sometimes be augmented by additional '*caveats*' or '*descriptors*' as handling instructions where a limited subset of information could have more damaging consequences and requires additional measures which should be marked with additional handling instructions, for example, UNIVERSITY CONFIDENTIAL information may carry a subset of PERSONAL or BUSINESS.

1.3 Examples of a '*caveat*' or '*descriptors*' that can be used to describe handling procedures are shown at Appendix A.

2. Scope

2.1 These guidelines apply to:

- All University data held on any medium, including all forms of hard copy and electronic data.
- All University Colleges, Research Institutes, Administrative and Service Departments.
- All contractors, third party suppliers and external stakeholders.

3. Information Classification

3.1 Information created or held by the University will be classified as either:

- **UNCLASSIFIED**: These documents may have no markings or may be positively marked as **UNCLASSIFIED.** Anyone is permitted to see these documents internally or externally, the documents can be published on the University's website or made publicly available.

- **PROTECT:** Only available to a limited number of users and requires very careful protection. Documents should be clearly marked as **PROTECT**. The information should be handled with care following the guidance laid out in this document.

- **UNIVERSITY CONFIDENTIAL**: Only available to a limited number of users and requires a stringent level of security protection. These documents should be clearly marked as **UNIVERSITY CONFIDENTIAL**. The information should be handled with care following the guidance laid out in this document.

4. Applying Information Classification

4.1 The originator or nominated owner of information (data owner) is responsible for applying the correct classification. If applied correctly, the classification will ensure that only genuinely sensitive material is safeguarded / protected. The following should be considered when applying classification:

- Applying too high a classification can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of the University's business.

- Applying too low a classification may lead to damaging consequences and compromise the University's information asset.

- The compromise of aggregated or accumulated information of the same classification marking is likely to have a higher impact (particularly in relation to identifiable personal information). Generally, this will not result in higher marking but may require additional handling arrangements.

- The sensitivity of an information asset may change over time and it may be necessary to reclassify assets. If an information asset is being de-classified or the classification changed, the file should also be changed to reflect the highest marking within its contents.

4.2 When classifying a document, the criteria specified below should be used to determine the correct classification level:

PROTECT - This information is defined as any information asset where inappropriate disclosure would be likely to:

- Cause distress to individuals
- Breach undertakings to maintain the confidence of information provided by third parties
- Breach statutory restrictions on the disclosure of information
- Cause financial loss or loss of earning potential, or facilitate improper gain
- Give an unfair advantage to individuals or companies
- Prejudice the investigation, or facilitate the commission, of crime
- Disadvantage the University in commercial or policy negotiations with others.

UNIVERSITY CONFIDENTIAL - This information is defined as any information asset where inappropriate disclosure would be likely to:

- Adversely affect University relations
- Cause substantial distress to individuals
- Make it more difficult to maintain the operational effectiveness or security of the University or its partners
- Cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies
- Prejudice the investigation, or facilitate the commission, of crime
- Breach - undertakings to maintain the confidence of information provided by third parties
- Impede the effective development or operation of University policies

- Breach statutory restrictions on the disclosure of information (including the Data Protection Act or Freedom of Information Act)
- Disadvantage the University in commercial or policy negotiations with others
- Undermine the proper management of the wider university sector operations.

SPECIAL CATEGORY PERSONAL DATA

Special category data is more sensitive Personal data, so needs more protection. The list below has been taken from the Data Protection Act 2018. ANY documents or emails that include Special Category Data must be marked as UNIVERSITY CONFIDENTIAL.

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

If you require further classification on how to process Special Category Personal Data please follow the ICO link

Baseline Outcomes

- **ALL** University information must be handled with care to prevent loss or inappropriate access, and deter deliberate compromise or opportunist attack.

- Staff (from business areas and Colleges) must be trained to understand that they are responsible for securely handling information that is entrusted to them.

- Baseline classification controls **MUST** reflect commercial good practice

5. Marking Information

6.1 A limited subset of **UNIVERSITY CONFIDENTIAL** information could have more damaging consequences (for individuals, the University or external stakeholders generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the **UNIVERSITY CONFIDENTIAL** classification tier, but may attract additional measures (generally procedural) to reaffirm the "need to know" principle. In such cases where there is a clear and justifiable requirement to reaffirm the "need to know", assets should be conspicuously marked.

6. Optional Descriptors

7.1 Optional information descriptors/subsets may be used with a classification in order to describe why the information is not available to all. For example:

UNIVERSITY CONFIDENTIAL – COMMERCIAL or
UNIVERSITY CONFIDENTIAL – LEGAL

7.2 Data owners are responsible for identifying any sensitive information within this category and for putting in place appropriate business processes to ensure that it is appropriately handled, reflecting the potential impact from compromise or loss.

7.3 To support specific business requirements and compartmentalise information, the data owner may apply an optional DESCRIPTOR, alongside the **UNIVERSITY CONFIDENTIAL** classification marking, to distinguish particular types of information and indicate the need for additional common-sense precautions to limit access. **See Appendix A for a list of descriptors.**

7. Labelling

8.1 Information that is classified should be clearly marked in CAPITALS and should be visible on all pages when viewed or printed. More than one descriptor may be applied and should follow the University's information classification scheme. **For example**:

UNIVERSITY CONFIDENTIAL – COMMERCIAL

UNIVERSITY CONFIDENTIAL – LEGAL

UNIVERSITY CONFIDENTIAL – PERSONAL

8. Legal Framework

9.1 The classification of information does not exempt it from the rights of access to information under the Freedom of Information Act or Data Protection Act. For clarification on any Data Protection position, please contact the University's Information Access Officer or the Governance, Information and Legal Office. The classification scheme operates within the framework of UK law. Examples of some of the laws:

a. **Data Protection Act 1998 (DPA)**: The handling of personal data must be in compliance with the DPA. The DPA, however, contains a number of exemptions to some or all of the data protection principles and to other provisions of the DPA such as the right of access to personal data. Whilst the presence or absence of a classification marking is not in itself a deciding factor as to whether an exemption is engaged, it may be a helpful indicator that one applies.

b. **Freedom of Information Act 2000 (FOIA):** Classification markings can assist in assessing whether exemptions to the Freedom of Information Act 2000 may apply. However, it must be noted that each FOI request must be considered on its own merits and the classification in itself is not a justifiable reason for exemption. It is therefore important that staff (including contractors and third parties) who handle, or are likely to handle sensitive assets, understand fully the impact of such legislation and how it relates to their role.

c. **Public Records Act 1967.** Records selected for preservation may be retained under Section 3(4) of the 1958 Act or closed under an exemption provided by the Freedom of Information Act 2000. Decisions over retention or closure are driven by perception of residual sensitivities at the time that release is being contemplated.

9. Information Handling and Storage

10.1 When information is classed as UNIVERSITY CONFIDENTIAL or UNIVERSITY CONFIDENTIAL - DESCRIPTOR, extra care and specific procedures must be followed to ensure correct handling, storage or transmission.

10.2 Where UNIVERSITY CONFIDENTIAL / UNIVERSITY CONFIDENTIAL-DESCRIPTOR information is being sent from the University to an external source, appropriate permissions must be obtained from the data owners, and only the data that is needed should be sent. The recipients must also be made aware of their responsibilities to protect the data from loss.

10.3 When receiving data from outside the University it should be reviewed to identify if any classification has been applied and confirm that this classification is appropriate. **See Appendix B for the current guidance on information handling and storage methodology.**

Appendix A –Descriptors & Caveats

Descriptor:	
COMMERCIAL	Commercial or market sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to the University or to a commercial partner if improperly accessed
PERSONAL	Personal or sensitive personal information relating to an identifiable individual, where inappropriate access could have damaging consequences.
INVESTIGATIONS	Sensitive information relating to an investigation that requires careful disclosure and protection. Unauthorised disclosure may jeopardise an inquiry or have damaging consequences.
LEGAL	Legally sensitive information requiring enhanced security protection and controls that might, if disclosed, be prejudicial to a legal issue or have damaging consequences.
Example	UNIVERSITY CONFIDENTIAL - COMMERCIAL UNIVERSITY CONFIDENTIAL - INVESTIGATIONS
Caveats:	

Examples that may be used to describe and provide instructions on information asset handling	UNIVERSITY CONFIDENTIAL – INVESTIGATIONS Disciplinary Panel Only UNIVERSITY CONFIDENTIAL HR & Senior Management Only PROTECT Commercial Partners Only PROTECT Management Only PROTECT Planning Department Only PROTECT Executive Board Only – No Disclosure PROTECT Management in Confidence - No Disclosure PROTECT Not For External Disclosure UNIVERSITY CONFIDENTIAL – ESTATES PROJECTS UNIVERSITY CONFIDENTIAL Named Recipients Only

Appendix B – Information Handling and Storage Methodology

Unauthorised disclosure/loss or unauthorised changes to information would cause significant harm to the interest of the University by virtue of financial loss, loss of profitability, revenue and/or opportunity, embarrassment, reputational and/or brand damage. This classification applies to information which must be restricted to specified individuals or roles within Brunel University London.
The table below defines how information can be handled, transmitted, and stored for the different classification categories in use by the University– **Internal** applies for sending information within the University; **External** applies for sending information outside of the University:

	UNCLASSIFIED	**PROTECT**	**UNIVERSITY CONFIDENTIAL**
Document Marking	None	**PROTECT** at the middle top or bottom of every page	**UNIVERSITY CONFIDENTIAL** "*descriptor*" at the middle top or bottom of every page
Storage of papers	Normal	Protected by one barrier, e.g. locked cabinet or drawer. Do not leave unattended at any time	Protected by one barrier, e.g. locked cabinet or drawer. Do not leave unattended at any time
Disposal of papers	Normal	Secure waste disposal or destruction or shredding	Secure waste disposal or destruction or shredding
Electronic storage	Normal Do not leave unattended on screen - lock screen	University's network: restricted access by defined user/user groups to specific areas **Mobile working:** Minimum encryption protection on University owned mobile storage device, preferably access directly through remote network access (VPN) Do not leave unattended on screen - lock screen	University's network: restricted access by defined user/user groups to specific areas Mobile working: Minimum encryption protection on University owned mobile storage device, preferably access directly through remote network access (VPN). **Mobile devices** must have Full Disc Encryption (FDE) using complex password. Do not leave unattended on screen - lock screen

	UNCLASSIFIED	PROTECT	UNIVERSITY CONFIDENTIAL
Electronic Cloud (Internet) Storage - excluding University Office365. (e.g. Dropbox, Google Drive, Copy, Box, MS OneDrive, Sync.com, E-Box, Tresorit, owncloud, Viivio)	Normal Do not leave unattended on screen - lock screen.	Not to be stored on Cloud Storage unless University authorised Office365.	Not to be stored on Cloud Storage unless University authorised Office365.
Office 365	Normal Do not leave unattended on screen - lock screen.	University authorised OneDrive for business; Office 365 Groups; SharePoint Online; Office Apps (Word, Excel, PowerPoint, OneNote) Skype for business, Yammer, Sway and Forms not permitted Do not leave unattended on screen - lock screen.	University authorised OneDrive for business; Office 365 Groups; SharePoint Online; Office Apps (Word, Excel, PowerPoint, OneNote) Skype for business, Yammer, Sway and Forms not permitted Do not leave unattended on screen - lock screen.
Electronic backup	Backup stored in locked cabinet	Backup stored in locked cabinet	Backup stored in locked cabinet
Electronic media disposal	Normal deletion or reuse	Securely wipe then recycle or destruction if removable media	Securely wipe then recycle or destruction if removable media
Printing	Normal printing procedures	Print on a print service printer. For all other printer models, do not leave unattended on printer trays	Use the “Print and Hold” facility on Multi-Function Devices For all other printer models, do not leave unattended on printer trays

	UNCLASSIFIED	PROTECT	UNIVERSITY CONFIDENTIAL
Email	Brunel University London email	**Internal**: University email marked PROTECT in the subject **External Mail**: labelled as above, only sent to appropriate organisation, stakeholder or recipient	**Internal**: 1. University email marked **UNIVERSITY CONFIDENTIAL** in the subject line; 2. Email should be tagged with a *Confidential* sensitivity. 3. Number of addressees should be limited and only sent to those parties that have a requirement for this information. Try not to send such emails to group email addresses – send them to named individuals; 4. When forwarding or replying, consider whether *all* of the addressees need to see the entire email thread, or see the attachment. If the entire email thread is not required, delete the unneeded communications. 5. When sending an email try not to include the particular text in question within the body of the email, send the data as an attachment. **External Email**: labelled and managed as above, only sent to appropriate organisation, stakeholder or recipient When sending an email, do not include the particular text in question within the body of the email; send the data as an encrypted attachment. Email must be encrypted with a password using the recommended University compression and encrypting tool and can only be sent to the email box(es) of the identified recipient(s) and may not be copied or forwarded to individuals or roles that are not authorised to receive it
Removable and storage media (CD-ROMS, USB storage)	Normal procedures	Not to be stored on personal removable and storage media, only those provided by the University – must be encrypted to at least 256-bit AES cipher encryption	Not to be stored on personal removable and storage media, only those provided by the University – must be encrypted to at least 256-bit AES cipher encryption and FIPS-140-2 level

	UNCLASSIFIED	PROTECT	UNIVERSITY CONFIDENTIAL
Post	Internal or external mail	Internal mail or external mail – Use internal postal systems	**Internal**: Sealed envelope marked "[**UNIVERSITY CONFIDENTIAL**.] Addressee Only". Treated as current "Confidential" mail only to be opened by addressee **External**: Sealed internal envelope showing classification, **and** sealed external envelope using Royal Mail 'Recorded Signed For' service or preferably secure courier to named person, without security marking on the outside of the package, or delivery by hand
Telephone (internal, public network, mobile)	Normal use	Normal use if recipient can be identified and spoken to in person. Do not leave message on answering systems	Normal use if recipient can be identified and spoken to in person. Do not leave message on answering systems
Fax	Normal fax	If recipient is at hand: Send cover sheet first and wait for confirmation before sending	Not to be sent via fax, must be sent encrypted via email.
Public Website	Normal	To be used only if risk assessment is undertaken and the data owner approves	Not to be published on the Web

	UNCLASSIFIED	PROTECT	UNIVERSITY CONFIDENTIAL
Mobile / home / working away from office	Normal	Do not leave unattended, secure information out of sight and locked where possible Information should not be discussed in a public place where it may be overheard Not to be stored electronically on personal home computer or personal mobile device Minimum encryption protected on University mobile storage device	Do not leave unattended, secure information out of sight and locked where possible Clear desk – do not leave University Confidential data in open view; Information should not be discussed in a public place where it may be overheard Not to be stored electronically on personal home computer or personal mobile device 256-bit AES cipher encryption and FIPS-140-2 level protected on University mobile storage device

Note: Technical controls will be based on assured, commercially available products, without need for any bespoke development. Whilst these controls cannot absolutely ensure against the most sophisticated and determined threats and threats actors, they will provide for robust and effective protections that make it difficult, time consuming and expensive to illegally access the University's information assets.