INFORMATION CLASSIFICATION AND HANDLING MATRIX (Version 2 February 2021)

Category	Public/Open	Internal Use	Sensitive	Protected
Risk	None	Low	Medium	High
Criteria	No need for confidentiality or restrictions. May be shared with or viewed by members of the public.	Some limited restrictions in place in relation to the handling of information. Information may be accessed by authenticated Sussex users such as staff, students and associates using a secure log on.	Protection of information and confidentiality is required. Loss or unauthorised disclosure of information could, for example: -Constitute a personal data breach; -Cause harm to individuals; -Compromise integrity or breach trust or a contract; or -Prejudice the University's commercial interests.	Highest level of protection required. Loss or unauthorised disclosure of the information could, for example: -Prejudice security or the prevention and detection of crime; -Cause significant harm to individuals or have a serious impact on them; -Seriously impact University operations or damage University reputation.
Examples. Please note, this is <u>not</u> an exhaustive list	Information published on the University website, including professional contact details. Information disclosable under the Freedom of Information Act.	Internal correspondence, emails and some internal communications. Committee papers. Internal reports and working group papers.	Personal data (other than that published on the University's website). Information exempt from disclosure under the Freedom of Information Act.	Large data sets of personal data (>1000 records). Personal data defined as 'special category data' under data protection legislation.

	Promotional materials, such as Prospectus and recruitment information. Public lectures/seminars. University policies and procedures, guidance and FAQs.	Course and module related material. Recordings of teaching activities and meetings. Except where the above also contain Sensitive or Protected information and then the higher classification shall be applied.	Commercially or financially valuable information. Student coursework and examinations. General research data held by academic staff. Financial data such as card holder data.	Research data specifically covered by patent or legal agreement. Information protected by clauses in commercial contracts. Information relating to criminal activity, investigations or convictions. Highly sensitive business or financial information.
Protective markings	None required	All information must be clearly and visibly marked according to its classification. This should include the classification in the email subject line or on the outside of documents, folders, storage solutions etc, or in the meeting invitation.		
Availability on the University's website	All Public/Open information can be made available via the University's publicly accessible webpages.	Information should only be available on the website via authenticated secure access, for example, requiring a Sussex user log on.		Information should not be available via the website.
Access controls	None – information is publicly available	Available to relevant University staff, students and associates, Electronic access requires authentication.	Available only to specifically authorised University staff, students or associates, who require access to the information. Information should only be accessible to authenticated	Access is controlled and restricted to a small number of University staff, based on management approval. Information should only be accessible to authenticated users and limited by role

			users and limited by role specific access controls. Multi-factor authentication must be used wherever possible. Hard copy information must be kept in locked cabinets / secure offices or in dedicated on-site archival rooms or offsite storage with an approved archival company.	specific access controls. Multi-factor authentication must be used wherever possible. Information must not be processed on personal devices. Hard copy information must be kept in locked cabinets / secure offices or in dedicated on-site archival rooms or offsite storage with an approved archival company.
Storage	Information may be stored on publicly accessible University webpages and in publicly available papers, brochures etc.	Information must be stored in University backed up personal or shared network spaces with access restricted as necessary. Information may also be stored on other University devices (such as laptops of mobile media) and personal devices, if appropriate information security measures are in place.	Information must be stored in University provided resources or services with access restricted to those with a right to access the information (e.g. folder permissions). Information may be stored on other University managed devices (such as laptops or mobile media) if appropriate information security measures are in place, such as software, encryption and password protection.	Information must be stored in University provided resources or services with access restricted to only those with a valid right to access the information (e.g. folder permissions). Information should only be stored on other University managed devices (such as laptops or mobile media) on a temporary basis and only if encrypted and password

			Information may be stored on personal devices on a temporary basis but only if information security arrangements are in place, including appropriate software, encryption and password protection, and in compliance with the Bring Your Own Device Policy.	protected, taking care to avoid loss or theft. Restricted information must not be stored on personal devices.
Transfer	Information may be transferred freely, internally and publicly.	Information may be emailed internally (i.e. to University of Sussex email addresses) without additional measures in place. Any external transfer of information should be with the use of appropriate password protection.	Information should be shared wherever possible by sharing its storage location and only granting access to intended recipients. Information may be emailed internally (i.e. to University of Sussex email addresses) without additional measures in place. Any external transfer of information should be with the use of appropriate password protection and encryption.	Information must only be transferred (by email or otherwise) with appropriate password protection and encryption in place.
Disposal	Recycling for paper. Out of date information should be removed from the University webpages.	Information should be disposed of securely, for example, confidential waste disposal, secure shredding or IT Services deletion of information from IT equipment, servers etc. in accordance with the University's Records Management policy and Master Records Retention Schedule.		