Part A: Handling Methods based on Information Classification

Classification	Public	Non Sensitive	Restricted	Confidential
Risk Level	None - confidentiality is of no particular significance to this information	Low - inappropriate disclosure would have minimum significance	Medium – inappropriate disclosure could adversely affect the University's reputation or operations, substantial distress to individuals or breach statutory restrictions on disclosure of information; likely financial or legal penalties	High - inappropriate disclosure could cause significant damage to the University's reputation or operations, great distress to individuals, pose a danger to personal safety or to life or impede the investigation or facilitate the commission of serious crime; substantial financial or legal penalties
Types of Information	* Term and closed dates * Academic staff and G9 or above with a public facing role * Job adverts (excluding internal only positions) * Press releases * Faculty names codes and addresses * Programme, unit and school/department names * HESA subject and fee status codes * Staff publications * Salary bands / grades of individual job roles * Strategies, policies and procedures * Organisational and departments structures * Annual report and financial statements * Agendas and minutes of University committees and working groups (minus any reserved business) * Patented intellectual property * Prospectus, programme and course information * Open content on the website * Flyers and publicity leaflets	* Student Names and email addresses * Staff Work Contact Details (incl job titles) * Academic Staff Qualifications and Publication Details * List of student or staff names and ID number * Internal only University policies, processes and guidelines * Non-private calendar entries * Internal only job adverts * Internal staff communications * Normal Calendar entries * Individual student exam timetables * Research proposals prior to award	* Exact staff salary details * Staff/student personal details including: Individual's name home addresses, contact details, age and passport or NI number, dates of birth (DoB) * Emergency contact / next of kin details * Staff/student photographs unless consent for publication provided by individual * CCTV footage * Student admission/registration details * Student assessment marks/ comments * Prospective Students' contact details * Information relating to supply or procurement of goods/services prior to approved publication * Non-public data that relates to business activity and has potential to affect financial interests and/or elements of the University's reputation e.g. tender bids prior to	* Any identifiable medical details (relating to physical or mental health) * Racial or ethnic origin of an individual * Sexuality or sexual life of an individual * Criminal activity or alleged criminal activity relating to an individual * Religious beliefs of an individual * Trade union membership * Bank account/payment card details * Commercially sensitive information * Legally privileged information * Intellectual property that is under development and subject to patent * Any information subject to a confidentiality agreement * Research data containing identifiable information * Research data that is 'owned' by a third party * Staff/student passwords * Any information subject to or obtained under the Official Secrets Act * Data contains highly sensitive private information about living

	* Anonymised information * Information on individuals made public with their consent including on social media sites or departmental websites * Research publications and research datasets cleared for publication		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. * UCAS forms	individuals and it is possible to identify those individuals' e.g. Medical records, serious disciplinary matters. * Non-public data relates 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. * References for staff or students * 'Trade' secrets, intellectual property intended for commercialisation
General Handling Methods	Some contact details are associated with specific job roles and responsibilities only and should not be released to the public without consent.	• Such information may be shared with peers and partner organizations within the sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within community. This information may not generally be released outside of the community. Specific legal or other reasons may require wider release. • It should be stored on centrally managed shares areas with appropriate backup arrangements in place in line with University guidance • It should be kept up to date and access to it should be limited to only those authorised to make relevant changes to it • Disposal should follow normal file deletion or non-confidential paper record disposal procedures in line with Document Retention Policy guidelines.	• Restricted information may generally only be shared with members of BU, and with others who need to know the information for a legitimate reason, for example to perform a contract with BU or prevent harm. This type of information requires the most suitable security controls that will ensure the appropriate distribution and maintain the information's integrity. • It should be kept up to date and stored in restricted areas within centrally managed shared areas or restricted physical storage areas. • Access should be limited to 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	• Such information may not be shared with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. It should only be shared under a very strict environment. • Only provide on a "need-to-know" basis within the University, or externally to fulfil statutory and legal requirements. • Ensure data is kept up to date and stored in highly restricted areas within centrally managed shared areas or restricted physical storage areas. Access should be limited to named data owners and authorised individuals, and appropriate monitoring controls and backup arrangements put in place. University approved storage facilities should be used where third parties are responsible for data management

			• Data should be securely wiped off electronic devices where the device has been decommissioned and disposal of paper records should follow the requirements of the Document Retention Policy guidelines	• Data should be securely wiped off electronic devices where the device has been decommissioned, or disposal of paper records should follow Document Retention Policy guidelines Any created documents (electronic or paper) must be marked as "**Confidential**" and the intended recipients clearly indicated; if marking is not possible "**Confidential**" must be included in the document header or use a file naming convention e.g. xxxxx-Confidential.doc. Printed copies to be delivered in sealed envelopes marked "**Confidential**"

Part B: Handling Methods based on Type and Storage Methods

ONLINE COLLABORATIVE SPACES AND CLOUD STORAGE				
	Public	Non Sensitive	Restricted	Confidential
BU-provided Office 365	OK to use for this type of information	OK to use for this type of information	OK to use for this type of information if restricted to authorised recipients	OK to use for this type of information only where specifically set up for this level of security with restricted recipients
External "Cloud" storage/file sync provider. Non University contract (e.g. individually set up Dropbox account, personal Office 365 subscriptions, personal OneDrive account)	Can be stored in any public cloud, including personal and corporate accounts.	Do not use to store master copy	Use University solutions (e.g. Office 365)	Use University solutions (e.g. Office 365)

EMAIL AND FILE TRANSFER				
	Public	Non Sensitive	Restricted	Confidential
Sending from BU hosted email account to same **From: @bmth.ac.uk** **To: @bmth.ac.uk**	OK to use for this type of information	OK to use for this type of information	Marked **Restricted** and double check recipient	Marked **Confidential** and double check recipient
Sending from BU hosted email account to an external account **From: @bmth.ac.uk** **To: @xxx.xxx**	OK to use for this type of information	OK to use for this type of information **Auto forward to a personal email account from your BU account not permitted**	Marked **Restricted** and double check recipient **Auto forward to a personal email account from your BU account not permitted** Ensure email or attachments (that which contains the restricted information) is encrypted	Marked **Confidential** and double check recipient **Auto forward to a personal email account from your BU account not permitted** Ensure email or attachments (that which contains the restricted information) is encrypted
Sending from externally provided personal email (e.g. Hotmail, Gmail, etc.) **From: @xxx.com** **To: @xxx.xxx**	University business **must** be conducted via your university email account only. Use university provided alternative to send message instead	University business **must** be conducted via your university email account only. Use university provided alternative to send message instead	University business **must** be conducted via your university email account only. Use university provided alternative to send message instead	University business **must** be conducted via your university email account only. Use university provided alternative to send message instead
Sending a personal email from BU hosted email account	In line with the Electronic Communications policy personal use of business email should be **clearly labelled as personal** and will be subject to the terms of the Acceptable Use Policy and the Code of Practice – Use of Communication Facilities (C7 – Section 3.3)			

File Transfer	OK to use for this type of information	OK to use for this type of information	As password protected attachment, marked **Restricted** and double check recipient Consider whether sender or recipient may have delegated authority to others to access the account	Only as password protected attachment, marked **Confidential** and double check recipient Consider whether sender or recipient may have delegated authority to others to access the account

SAVING AND STORING FILES				
	Public	Non Sensitive	Restricted	Confidential
University desktop PC drives **In non-public areas:** **Controlled access** **Not a shared space** **Not centrally backed up**	OK to use for this type of information	Lock screen when unattended **No storage or creation permitted on device** Consider any backup requirements	Lock screen when unattended **No storage or creation permitted on device** Consider any backup requirements	Lock screen when unattended **No storage or creation permitted on device** Consider any backup requirements
University desktop PC drives **In public areas (e.g. OAC):** **Not controlled access** **Not a shared space** **Not centrally backed up**	OK to use for this type of information	Lock screen when unattended **No storage or creation permitted on device** Consider any backup requirements	High risk of incidental disclosure **Do not use for this type of information** Use university desktop PC in non-public area	High risk of incidental disclosure **Do not use for this type of information** Use university desktop PC in non-public area
Personally owned desktop PC drives	OK to use for this type of information	**No master copy storage permitted** May be used for remote connection to access files via secure means e.g. VPN/VMware View. Do not leave logged in and unattended Created documents must be saved on university network or university owned device	**No storage or creation permitted on device** May be used for read only remote connection to access files if used in a private environment. Encrypt drive. Do not download files to device. Do not leave logged in and unattended. Clear browser cache after read only use.	**No storage or creation permitted on device** May be used for read only remote connection to access files if used in a private environment. Encrypt drive. Do not download files to device. Do not leave logged in and unattended. Clear browser cache after read only use.

University owned laptop	OK to use for this type of information	Do not use to store master copy of vital records Do not leave logged in and unattended Do not share use of device with non-university staff Consider any backup requirements	Encrypt device - use strong password with maximum of 10 minutes' inactivity until device locks Use secure remote connection (e.g. View) to access files and avoid download or storage Do not use to store master copy of vital records Do not work on files in public areas Do not leave logged in and unattended Do not share use of device with non-university staff Consider any back up requirements	Encrypt device - use strong password with maximum of 10 minutes' inactivity until device locks Use secure remote connection (e.g. View) to access files and avoid download or storage Do not use to store master copy of vital records Do not work on files in public areas Do not leave logged in and unattended Do not share use of device with non-university staff Consider any back up requirements
University owned smartphone or tablet	OK to use for this type of information	**No master copy storage permitted** Do not leave device unattended in public areas Do not share use of device with non-university staff Consider any back up requirements	**No storage permitted locally on device** Device must be configured to connect via Exchange Active Sync to ensure baseline security features (timeout, password, encryption) are applied Service to locate device and remote wipe in case of loss/theft to be enabled Do not leave device unattended in public areas Do not share use of device with non-university staff May be used for secure remote connection (e.g. View) to access files but do not work on restricted files in public areas Consider any back up requirements	**No storage permitted locally on device** Device must be configured to connect via Exchange Active Sync to ensure baseline security features (timeout, password, encryption) are applied Service to locate device and remote wipe in case of loss/theft to be enabled Do not leave device unattended in public areas Do not share use of device with non-university staff May be used for secure remote connection (e.g. View) to access files but do not work on confidential files in public areas Consider any back up requirements
Personally owned laptop	OK to use for this type of information	**No master copy storage permitted** May be used via secure remote connection to access files. Do not leave device unattended in public areas Do not share use of device with non-university staff Consider any back up requirements	**No storage or creation permitted on device** May be used for read only remote connection to access files if used in a private environment. Encrypt drive. Do not download files to device.	**No storage or creation permitted on device** May be used for read only remote connection to access files if used in a private environment. Encrypt drive. Do not download files to device. Do not leave logged in and unattended.

			Do not leave logged in and unattended. Clear browser cache after read only use.	Clear browser cache after read only use.
Personally owned smartphone or tablet	OK to use for this type of information	**No master copy storage permitted** May be used via secure remote connection to access files. Do not leave logged in and unattended Created documents must be saved on university network or university owned device Do not leave device unattended in public areas Do not share use of device with non-university staff Consider any back up requirements	**No storage permitted locally on device** Device must be configured to connect via Exchange Active Sync to ensure baseline security features (timeout, password, encryption) are applied Service to locate device and remote wipe in case of loss/theft to be enabled Do not leave device unattended in public areas Do not share use of device with non-university staff May be used for secure remote connection (e.g. View) to access files but do not work on restricted files in public areas Consider any back up requirements	**No storage permitted locally on device** Device must be configured to connect via Exchange Active Sync to ensure baseline security features (timeout, password, encryption) are applied Service to locate device and remote wipe in case of loss/theft to be enabled Do not leave device unattended in public areas Do not share use of device with non-university staff May be used for secure remote connection (e.g. View) to access files but do not work on confidential files in public areas Consider any back up requirements
Networked storage I:	No restrictions	OK to use for this type of information	Use restricted access folders to protect files Consider file password protection for most sensitive files	Use restricted access folders and consider password protecting files
Networked storage H:	No restrictions	Consider - does information need to be shared with colleagues - if so enable folder sharing or move to shared drive	Consider file password protection for most sensitive files Does information need to be shared with colleagues - if so enable folder sharing or move to shared drive	Consider file password protection for most sensitive files Does information need to be shared with colleagues - if so enable folder sharing or move to shared drive

Small capacity portable storage devices e.g. USB, CD	OK to use for this type of information	Not suitable for long term storage Do not use to store master copy	**No permanent storage permitted on device** **Short term storage permitted in line with Research Ethics approval** Encrypt media - strong passcode Keep in lockable cabinet/drawer which is locked when unattended	**No permanent storage permitted on device** **Short term storage permitted in line with Research Ethics approval** Encrypt media - strong passcode Keep in lockable cabinet/drawer which is locked when unattended
Large capacity portable storage devices e.g. external hard drive	OK to use for this type of information	Do not use to store master copy	**No permanent storage permitted on device** **Short term storage permitted in line with Research Ethics approval** Encrypt media - strong passcode Keep in lockable cabinet/drawer which is locked when unattended	**No permanent storage permitted on device** **Short term storage permitted in line with Research Ethics approval** Encrypt media - strong passcode Keep in lockable cabinet/drawer which is locked when unattended
Faculty/Department based server not managed by IT Services	OK to use for this type of information	Consider any backup requirements	**Seek advice from IT Services on default access rights, physical security of server and back up** No storage or creation permitted unless server environment is equivalent to IT Services server environment If yes then required to use restricted access mechanisms where online access is shared Consider any backup requirements	**Seek advice from IT Services on default access rights, physical security of server and back up** No storage or creation permitted unless server environment is equivalent to IT Services server environment If yes then required to use restricted access mechanisms where online access is shared Consider password protection for most sensitive files Consider any backup requirements
Other IT Services maintained service e.g. database	OK to use for this type of information	OK to use for this type of information Consider making a backup copy before posting	Seek advice from IT Services on default access rights, Use restricted access mechanisms where online access is shared	Seek advice from IT Services on default access rights, Use restricted access mechanisms where online access is shared

STORING PAPER RECORDS				
	Public	Non Sensitive	Restricted	Confidential
Paper copies	OK to use for this type of information	OK in restricted access university areas OK in unrestricted access university areas Offsite working - consider making a backup copy before taking off site	Consider - protection from fire and flood damage. Do not take in to public areas. In restricted access university areas store in lockable cabinet/drawer that is locked when office is unattended. No restricted papers left out when desk unattended. Offsite working - If needed to be taken off site a backup copy must be made beforehand.	Consider - protection from fire and flood damage. Do not take in to public areas. In restricted access university areas store in lockable cabinet/drawer that is locked when office is unattended. No restricted papers left out when desk unattended. Offsite working - If needed to be taken off site a backup copy must be made beforehand. Alternative - create as/convert to electronic documents and use secure remote connection with permitted device Presumption is that confidential papers are not taken offsite.
Printing or copying	Unrestricted	Unrestricted	Unrestricted	Any created documents must be marked as " **Confidential**" Printed copies to be delivered in sealed envelopes marked "**Confidential**"