ONLINE ETHICS CHECKLIST

Keeping your Information Secure – An example

Example of how to treat data which includes collecting identifiable medical details (relating to physical or mental health) – **Type of Information**

- This information should be treated as confidential (classification) and the risk is high (**risk** of inappropriate disclosure could cause great distress to an individual and significant damage to BU's reputation)
- Sharing this information should be restricted or included as part of a data sharing agreement; data kept up to date and stored in restricted areas, access limited and securely destroyed (as appropriate) – if retaining for research, safeguards must be applied.

Handling guidelines

- *Online Collaborative spaces and cloud storage* would be BU-provided Office 365 only where specifically set up for this level of security with restricted recipients
- *Email and File Transfer*
  - From: @bmth.ac.uk to @bmth.ac.uk – marked confidential and double check recipient
  - From: @bmth.ac.uk to @xxx.xxx – marked confidential and double check recipient (attachments encrypted) – note auto forward to a personal email account from your BU account **NOT PERMITTED**
  - From @xxx.com (hotmail, gmail) to @xxx.xxx **NOT PERMITTED**. University business must be conducted via your university email account.
  - 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 – Only as password protected attachment marked strictly confidential and double check recipient.

Saving and Storing Files (see Information Classification Types for details about using smartphone, I drive etc):

- *BU desktop PC drives in non-public areas* (e.g. staff centre) – lock screen when unattended, consider appropriate backup but no storage or creation permitted on device.
- *BU desktop PC drives in public areas* (e.g. Open Access Centre) – high risk of incidental disclosure (use university desktop PC on non-public area). Do not use for this type of information
- *Personally owned desktop PC drive* – No storage or creation permitted on device. May be used for read only remove 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.
- *BU owned laptop* – encrypt device, use secure remote connection 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 back up requirements

Storing paper files:

- do not take in to public areas, kept in lock filing cabinet in a lockable office (when left unattended), do not leave out on your desk
- Working off site – if needed to be taken off site, back up 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.
- If printing documents should be marked confidential. Printed copies should be sealed in envelopes marked 'confidential'.