Leicester Cancer Research Centre

Working Off Campus – Data Security and Information Governance Policy

Introduction

This document is created to provide local Centre based context to the Data Security and Information Governance policies of the University of Leicester as they apply to work which takes place "off-campus". It should be read in that context and if there is any doubt reference should be made to those documents.

"Off-campus" means outside of building space owned/controlled by the University of Leicester. Within the Centre many staff will have occasion to work in NHS owned rooms/spaces. These should generally be regarded as "off-campus" though in multiple cases Ethernet links have been established which allow the use of secure UoL managed desktop devices in these areas. Laptop users connecting their devices to the Eduroam network are effectively operating "off-campus" when doing so.

The policy and instructions within this document apply to all staff, associates and students (research and taught) within the Leicester Cancer Research Centre and a copy will be made available as part of the normal induction procedures within the Centre.

Information classification

The University of Leicester's Information Assurance Service (IAS) has created a data classification model. The details of that model are set out on their web pages (https://www2.le.ac.uk/offices/ias/university-data-classification). All members of the Centre are expected to have a basic understanding of this classification and should review these webpages as part of their study of this document. In the policy that follows "Public", "Unrestricted", "Restricted" and "Highly Restricted" are used as defined by IAS.

Policy

This policy sets out general guidance applicable in the majority of situations. Following the GDPR coming into force in May 2018 any research project which involves the collection of significant amounts of personal data will have a Data Privacy Impact Assessment (DPIA) and its associated risk assessment. That documentation may set more stringent requirements for data handling in which case the requirements established by the DPIA will override this general guidance.

1. Digital Data

Digital data broadly covers any and all material prepared using and accessed by a computing device, this includes the records of communications such as emails, IM logs, Skype recordings. Within the University our systems are configured to store all such material on central file stores rather than the devices used to access them. Since the overwhelming majority of the University's operations depend on such files, anyone working off campus needs to have access to this material. This can be achieved by either physically transporting a copy of the digital data on a suitable storage device or by setting up remote access.

Where this can be arranged secure access to the on-site file stores is always preferred over physically transporting material.

i) VPN access – the University has set up a system allowing secure encrypted communication between a remote Internet connected computer and our internal

systems. This is only available on University owned, managed Windows based laptops. These computers provide access equivalent to that of an on campus desktop computer with the user having full access to everything they would see on campus. Any member of staff of grade 7 or above is eligible for such a laptop. In keeping with the University policy of only supplying one computing device per staff member from central funds users will be expected to use them both on-campus (with a docking station) and off campus.

Please note there are no circumstances in which anyone but the registered user is allowed to access a University laptop, they are provided for the sole use of the Centre member. Do not allow family/friends access.

ii) Access via MyFiles – this UoL system allows an off campus user access to their personal file store (Z: drive) and those parts of the Research File Store (R: drive) which are configured to allow this access. Since the majority of the Centre generated research files fall into the Restricted category which requires enhanced R: security these will not be available off campus by this method. Since early June 2018 the University has determined that all departmental administration files (X: drive) are Restricted and removed all MyFiles access to that file store.

Centre staff and students must not use their personal z: drive file store to hold data which is properly categorised as "Restricted" or above in the University data classification model to allow them to access it off campus using MyFiles.

The Centre will do its best to provide any senior member of staff who needs to work off campus with a secure encrypted laptop with VPN access to perform this work. Of necessity the long term use of a laptop will involve the replacement of the user's desktop with a laptop docking station as University rules specify that only one computing device will be provided to each staff member.

The Centre has (1/2 TBD) laptops which will provide off campus VPN access available for short term loan to centre members who need this facility.

{*apart from current provision I am expecting to receive 6 new laptops from the College replacement budget which can be allocated as required, these loan machines will need to come from that allocation}*

iii) OneDrive – the University provides all staff and students with access to a OneDrive for business account. Any UOL computer can be used to store files therein. Files stored in OneDrive can be accessed from any Internet connected computer and worked on using the browser based Office365 tools. It is possible to use the inbuilt collaborative tools to allow others with a UoL account to see and edit files stored on your OneDrive to facilitate shared working. Please be aware that files with an IAS classification of "Restricted" or above must not be placed in a OneDrive folder. You must not synchronise your OneDrive folder with any non-University owned device unless it meets the requirements set out in section v) below.
Further details: https://www2.le.ac.uk/offices/itservices/ithelp/my-computer/office-365/onedrive

iv) Use of personally owned computers/tablets etc.

Access to the MyFiles system and the files in a user's z: drive and any unrestricted R: drive folders is permitted from a personally owned device. This permission is granted on the basis that users will only use it to access material which does not meet the University's data classification status of Restricted or above. Accessing that material on a personally owned device is not allowed and will potentially leave the user facing University disciplinary sanctions and personal liability for any data security breach or data loss caused.

Users should be very aware that any device which is set up in such a manner that it automatically connects to University file stores (i.e. without a password entry on each access) will be storing a copy of their password(s). These password stores are only as secure as the device storing them. On a normal unencrypted Windows/Mac machine accessing such material is trivial for a knowledgeable user. If you use such a device do not allow it to store your University passwords. If you do so, anyone who has access to the device either as a friend or possibly a thief will then have access to everything in your UoL accounts.

As time permits the Centre's IT manager will provide advice on securing personal devices on the understanding that this is on a best efforts basis and ultimately responsibility for the device and its security remains with the owner.

v) Transporting data on portable devices

While on site a user may choose to copy digital files to which they have access to a portable device to allow them to access the files off site. The devices involved could be a laptop or tablet, a flash memory device such as a memory stick or less often a hard disk. With memory sticks or hard drives the use of unencrypted devices is strongly discouraged. If the material concerned falls into the IAS "Restricted" category then devices with strong encryption (at least AES 256bit standard) must be used. If the material is "highly restricted" then the whole device must meet the FIPS 140-2 standard. Copying restricted data to an unencrypted storage device will be regarded as a disciplinary offence.

Where the device concerned is a laptop/tablet or phone University data may only be copied to such a device where there is appropriate security/encryption. For material with a Restricted classification appropriate security will require:
Windows: Bitlocker or equivalent encryption requiring both TPM and PIN identification, an active device firewall and active, up to date Antivirus/malware software
Apple: FileVault encryption, an active device firewall and active, up to date Antivirus/malware software

If you are in any doubt as to the suitability of your devices do not use them until you have sought appropriate advice and received permission to do so.

2. Printed/photographic records

While it is uncommon for Centre staff to remove printed records from University premises to use them for working at home you should be aware that data protection regulation does cover such records in the same way as it does digital records. Loss of such material can have very serious consequences and must be guarded against.

If any member of the Centre needs to remove paper records off campus and these contain restricted material – as for example any records of, or material related to actual or potential

staff or students of the centre; they should as a minimum ensure they have provided a comprehensive list of the material concerned to the Centre's Ops Manager before its removal.

3. Loss of Data

If any member of the centre has any reason to believe that they have lost possession of any computer or any data digital or printed which is the property of the Centre/UoL they must report this loss immediately to both the Centre's IT officer and the Centre's Operations manager. Failure to make such a report promptly will be regarded as a serious disciplinary breach