1. Who is this guidance for?

Researchers consulting material held in archives may want to view, and photograph, sensitive material that is ordinarily closed to public access. An application to view this data can be made under section 33 of the Data Protection Act (DPA). Section 33 of the DPA is designed to enable those engaged in historical or other research to consult material that may otherwise be restricted. Archives should be able to provide information about the process involved in applying to view restricted material, and researchers should familiarise themselves with the archives’ rules and regulations. It is important to note that archives are under no obligation to allow researchers to photograph restricted material. This guidance is designed for researchers who have obtained permission, from the relevant data controller, to view and/or photograph sensitive archival material.

2. Steps to take prior to visiting the archives

It is important to allow plenty of time for requests to view material with restricted access to be processed by archives (at least a month, sometimes longer). Please also allow 30 days for your CUREC 1A research ethics application (if applicable).

Depending on the material being requested, archives may need to approach external data depositors before granting access to restricted material. This can explain why researchers may find that certain restricted collections are made available for consultation more quickly than others. It is important to be aware that some archives require researchers to provide references as part of their application process.

If researchers wish to photograph restricted material it is important to disclose this as part of any section 33 application. Archives are likely to have their own policies about whether they permit photographing of restricted material. When applying to view and photograph restricted material it is important to detail how safely these photographs will be stored once they have been taken. If an archive has decided not to allow researchers to photograph restricted material it may be still be possible to view the material and take notes.
3. How to handle the data when at the archives

For the purposes of your research ethics application (usually via a CUREC 1A application), when photographing restricted material, it is important that no identifying data is captured. Similarly, when taking written notes relating to restricted material it is important not to make notes of any names or other personal identifiers.

Before taking photographs, it may be necessary to conceal certain parts of the documents to ensure that personal details are not photographed. If this is necessary, it is important to ensure that the process of concealing personal details does not damage the documents. Researchers should consult the relevant archivists about the most appropriate way of concealment.

4. How to handle the data once you have left the archive

Once restricted materials have been photographed, or associated notes have been taken, researchers have a responsibility to ensure that photographs are stored, and transferred between devices, as securely as possible. Photographs, and any accompanying notes, must be kept confidential, and must not be shared with others. Please only use encrypted devices, such as encrypted USB sticks, smartphones, cameras and laptops. The number of devices on which such data is stored should be kept to a minimum.

Although researchers may want to take photographs on their (encrypted and password-protected) smart phones, it is important that the data is not uploaded to devices, such as laptops and PCs, through third-party software such as iCloud or DropBox. This is because the University of Oxford has no control over how third parties handle this data.

In order to minimize the risk of data being inadvertently shared with third parties, researchers wishing to transfer photographs between devices – irrespective of whether they were taken on a digital camera or a smart phone – will need to download the photographs directly to the device. It is important that the device on which the photographs are stored is encrypted.

Researchers using computers provided by the University of Oxford are encouraged to contact their faculty IT Support Staff who can ensure that their machine is covered by Whole Disk Encryption. For researchers using a private computer there are other available solutions like Bitlocker (Windows), Filevault (OSX), or Truecrypt. Further details about encrypting devices can be found at http://researchdata.ox.ac.uk/home/managing-your-data-at-oxford/storage-and-backup/ and http://help.it.ox.ac.uk/wde/index.

Finally, it is important to ensure that any photographs taken of restricted archival material are securely backed up using the University’s HFS backup service. Backing up data can
Central University Research Ethics Committee (CUREC)

Best Practice Guidance 14_Version 1.0

Title: Consulting and/or photographing archival material (e.g. with restricted access)

Protect researchers against the accidental loss of data, corruption, hardware and operating system crashes. Backing up University work-related data on a regular basis helps mitigate this issue by allowing researchers to restore a previous version if necessary. Further details about backing up devices can be found here:

http://help.it.ox.ac.uk/hfs/help/registration.

Further information

- CUREC application process: www.admin.ox.ac.uk/curec/apply/
- Oxford Information Security website: www.infosec.ox.ac.uk
  - How to encrypt laptops and other devices: www.infosec.ox.ac.uk/protect-devices
  - How to secure mobile devices: www.infosec.ox.ac.uk/want/mobile
- Oxford IT Services: how to register for Oxford’s HFS backup service: http://help.it.ox.ac.uk/hfs/help/registration
- Oxford University research data website: http://researchdata.ox.ac.uk/
- University of Exeter guidance on encrypted cameras and audio recording devices: https://as.exeter.ac.uk/it/infosec/tips/recordingdevices/