

Information Governance Safeguards for Service Suppliers

Version	5.0
Document Reference	PHC_POL_IG111
Date of Approval and Adoption	01-Dec-2023
Latest Date of next Review	01-Dec-2024

1. Purpose and Scope

This Policy outlines the Information Governance (IG) safeguards to which certain service suppliers (Service Suppliers) are subject and contains the following sections:

- **Introduction**
- **Required IG Safeguards**
Policy, Training, Hard Drive encryption, User Profiles, Passwords, Antivirus, Windows Updates, Data Deletion and Equipment disposal
- **Other required controls**
- **Required procedures**

2. Introduction

The Department has established an Information Governance (IG) program with written policies for data protection and security.

As part of its commitment to data protection and security, the Department has identified requirements, which certain “micro” service suppliers (Service Suppliers) must meet so as to demonstrate compliance with recognised security controls and privacy safeguards which are consistent with the Data Protection Legislation requirements.

- a) For the purposes of this Policy, Service Suppliers refers **only** to those which provide transcription, translation and other specified products and/or services in support of Department research.
- b) These Service Suppliers are subject to the security assessment review described in this Policy due to their limited size and/or scope of operations.

All other third parties which process Data on behalf of the Department are subject to a University third party security assessment process or Department level risk assessment, where applicable.

To request a Service Supplier be considered for review under this Policy, the Department Study/Lead, such as the Clinical Investigator (CI) and/or Principal Investigator (PI) or designee (the Department Liaison) must submit a request to the Department IG team [HERE](#) with an explanation and the basis for the request.

The Department Liaison must provide documentation showing that the Service Supplier has met the requirements of this Policy **before** entering into an agreement with the Service Supplier.

The Senior Information Governance Manager (SIGM) or designee shall coordinate a review with the Head of Administration/Finance, who serves as the Senior Information Risk Owner (SIRO) and send notice of approval or rejection with further guidance on required next steps to the requestor.

Thereafter, on an annual basis, the Department requires each Service Supplier to provide written attestation as coordinated by the Department Liaison and SIGM or designee.

3. Required IG Safeguards - Policy

The Department Liaison provides this Policy to the Service Supplier, who must acknowledge the receipt and agree to meet all of the requirements set forth therein.

4. Required IG Safeguards - Training

The designee(s) from the Service Supplier working with Data from the Department must complete the University mandated Information security and data privacy awareness training course (the Course) initially upon contract with the Department and annually thereafter.

1. To access this Course, the Department Liaison first coordinates with the Service Suppliers to submit a virtual access status (VAS) request.

VAS account holders receive virtual status only. They are ineligible to be issued a University physical ID card and do not receive access to University libraries or IT Services help. The VAS accounts are valid for up to 12 months with renewals available thereafter.

2. To initiate the VAS account request and complete the University mandated training. Refer to the steps outlined in IG204 VAS Application SOP.

5. Required IG Safeguards - Hard Drive encryption

The Service Supplier will temporarily store the Data collected from the Department on a hard drive, such as on a personal computer (PC), laptop, etc. or, if applicable, an external encrypted hard drive provided by the Department.

Consequently, the Service Supplier must certify that the hard drive where the Data collected from the Department has been properly encrypted to prevent unauthorised access.

In addition, where applicable, the Service Supplier must hold Data collected from the Department on servers based within the UK or UK recognised countries with appropriate contracts in place.

For PCs:

- i. The Department recommends the use of Microsoft Office 2016 or newer versions of the software as it meets the University's encryption security control baseline referred to as the Advanced Encryption Standard 256 bits (AES 256) encryption standard.
- ii. Hard Drive encryption can be achieved on Windows 10 professional, enterprise or Windows 8 professional using **Bitlocker**. Refer the YouTube tutorial [HERE](#) for further guidance.
- iii. For users with Windows 10 Home version, the hard drive encryption guidance is available [HERE](#).
- iv. For Macs: the File Vault feature enables encrypt the entire hard disk. Refer to for instructional videos. [HERE](#) and [HERE](#).
- v. For other devices:
Where the Data resides elsewhere, such as on a cloud-based server, the Service Supplier must provide evidence of encryption that meets the above stated requirement.

6. Required IG Safeguards - User Profiles

The Service Supplier must certify that the PC or other device on which the Data collected from the Department (e.g., digital recordings) resides is used exclusively by the individual(s) from the Service Supplier who actually performs the service for the Department. This person or persons may not share any password(s) with anyone else.

Multiple user profiles on the same PC or other device typically provide full administrator access rights. Consequently, multiple users can all access the hard drive on the PC or other device. For the duration of the Department project on which the Service Supplier works, the designated representative from the Service Supplier must demonstrate that only their profile is the one on the PC or other device(s).

7. Required IG Safeguards - Passwords

The Service Supplier must certify the deployment of password protection to all Department Data to which his/she has access. At a minimum, the University recommends:

- Unique 12-character passwords. 20 + characters are considered the best.
- Base passwords on a long memorable phrase or four random words.
- Include the use of capital letters, punctuation and/or numbers.

The Department will separately issue the Service Supplier a password for the Data to be processed by text or by phone (passwords cannot be emailed). This is used to open the file, to save on the MS Word document while working on it, and for returning the finished document.

The Department shall assign different passwords, which the Service Supplier will receive separately by text or phone for their assigned project(s).

For more information, visit the University guidance on creating strong passwords [HERE](#). Additional University password assistance, if needed, is available [HERE](#).

8. Required IG Safeguards - Antivirus

The Service Supplier must provide evidence of updated antivirus protection (e.g., Windows Defender). This includes confirmation that the Service Supplier has installed an active and current antivirus software.

The Service Supplier must also demonstrate that routine scanning occurs on the device[s], which the Service Supplier uses to perform services for the Department and that the device[s] are confirmed to be virus free.

The University also recommends the use of Malwarebytes, which is free software available [HERE](#).

9. Required IG Safeguards - Windows Updates

The Service Supplier must provide evidence that the vendor supported operating systems, such as Windows 10, Monterey, etc., and other programs used are continuously updated to the most current version.

The University recommends that Service Supplier enables the MS Windows Update feature automatically for eligible devices. This can be confirmed by checking **Settings>Update & Security> Windows Update**.

10. Required IG Safeguards - Data Deletion

The Department is required to monitor and confirm that its third-party processors, which includes Service Suppliers, (i) retain the Data provided to them for only as long as is necessary and (ii) fully delete the Data when required to do so. This includes deletion of Data from a Service Supplier's PC or other device (as well as recycle bin, where applicable).

In addition, where applicable, the Service Supplier must:

- i. delete all transcripts and/or interview recordings, including those that may still reside on a Service Supplier's PC or other device after they have finished with them;
- ii. return any external encrypted hard drive(s) to the Department and document the same in writing; and
- iii. delete all changes shown on transcripts and/or interview recordings that may still reside on a designee from a Service Supplier's PC or other device after completing the services being supplied to the Department.

The Service Supplier should retain the Data collected from the Department until the Department has confirmed that it has safely received the Service Supplier's work product.

The Service Supplier should set up the document(s) with the agreed password(s) to protect them on their PC or other device while working on them.

As specified above by the Department, the Service Supplier must - upon request, provide the Department Liaison with an email confirming deletion of the Data collected from the Department, including - but not limited to, any stored on a Service Supplier PC or other device after the return of the external encrypted hard drive, if applicable.

11. Required IG Safeguards - Equipment disposal

Before disposing of old or broken PCs or other devices, used for University Data processing, the Service Supplier must properly dispose of the device in a secure manner (e.g., securely wiped by reformatting the disk using a data destruction tool).

If the PC or other device no longer works, the Service Supplier must remove the hard drive and manually destroy it.

The Service Supplier must provide evidence of destruction upon request by the Department.

12. Other required security controls

a. Security controls

The Service Supplier must deploy other security controls, including, but not limited to, the following:

- i) Enabling of a firewall on the PC and other devices used to provide services to the Department;
- ii) Encrypting documents with password while working;
- iii) Using a modern web-browser, e.g., Chrome, Firefox, Edge or Safari;
- iv) Using only trusted USB devices that have been scanned;

- v) Downloading software from only reputable sources;
- vi) Never using pirated software;
- vii) Setting computer to lock screen after a sustained period of inactivity, e.g., 10 minutes; and
- viii) Disabling macros by default on all Microsoft Office software.

b. Encryption

The Service Supplier must deliver Data using 7-zip or another suitable encryption software.

For Mac PCs, the Department recommends use of the [Keka](#) application to open these files.

- a) 7-zip is required to encrypt the final document before transferring it back to the Department via FILR, SharePoint, MS Teams etc. rather than email. It can be downloaded [HERE](#).

Details on how to encrypt Data files using 7-zip are available [HERE](#) and by following these steps:

- i. Open the 7zip program choose the file or zipped folder you wish to encrypt;
 - ii. Press the add button (+) on the top of the 7zip program
 - iii. Add a password; and
 - iv. Press OK it will then make an encrypted copy of the file or folder with the file extension .7z.
- b) Receiving encrypted file/ folders
- i. Save the file sent via FILR, SharePoint, MS Teams, etc.;
 - ii. Open the 7zip program choose the file or folder you have been sent;
 - iii. Press the Extract button (-);
 - iv. Add the password; and
 - v. The file will then be shown in its original format. Save the file.
- c) University data sharing options
- i. The University makes SharePoint, One Drive, MS Teams, FILR, etc. available for data file sharing. The Department Liaison or designee must coordinate with the Service Supplier to arrange for the secure transfer of audio files.
 - ii. Whenever a Service Supplier has a file ready to send, such as a transcript, the Service Supplier must follow these steps:
- d) Email the Department Liaison or designee to notify the Department that the Service Supplier has a file to upload;
- e) The Service Supplier will receive an email from the Department designee, if applicable, containing a web link on which they must click to upload the file. Be sure to encrypt the file with a password; and
- f) Wait for confirmation from the Department designee that the file was safely received and then delete the file from the PC or other device.

Please do not delete the original Data received until the Department sends confirmation that it is safe to do so.

These University file sharing resources can be configured to set a time limit for files to be uploaded and downloaded.

13. Required procedures

- a. Initial and Annual Service Supplier Recertification

The Service Supplier is required to submit an attestation to the Department in which they agree to meeting the above requirements initially upon contract with the Department and annually thereafter. Refer [HERE](#) to access this template form.

The Department Liaison is responsible for collecting the required attestation and supporting documentation as outlined in the previous sections of this policies, collectively, referred to as “the Documentation”.

The Department Liaison coordinates with the SIGM or designee to review and confirm that the Documentation satisfies the requirements of this Policy initially and annually thereafter.

The Department may immediately terminate its Supplier of Service agreement whenever the terms of that agreement, including but not limited to those specified in this Policy, are not met.

b. Managing Single Sign On (SSO) account credentials

To manage the University of Oxford Single Sign On (SSO) account credentials (such as to reset the password), a Service Supplier can visit [HERE](#) or contact the University Central IT Help Desk for assistance: +44 (0)1865 612345

c. Review and processing Service Supplier Invoices

The Department Finance team has established a process for the review and processing of Service Supplier invoices.

Upon receipt of an invoice from a Service Supplier, the Finance team designee confirms whether there is (i) a Supplier of Service agreement in place with the Service Supplier and (ii) an approved Data Transfer Authorisation Request (DTAR). The DTAR might cover a single invoice or multiple invoices. Refer to IG104 Data Transfer Policy [HERE](#) for more information.

The Finance team designee asks the person submitting the invoice (the Requestor) to provide the approved DTAR tracking number and/or copy of the approved DTAR form with the assigned tracking number and required signatures.

If the Requestor is unable to provide a DTAR tracking number and/or approved DTAR form with required signatures, the Finance team designee instructs them to consult with the study/trial lead or PI (or the SIGM, if needed) for further assistance. The Finance team will not approve invoices of this kind without such documentation.

Version History

Version	Date of Approval and Adoption	Description of Changes
1.0	25-11-2019	Initial version
2.0	15-Oct-2020	Expanded and clarified applicability of this Policy to other Service Suppliers in the “Introduction” section. Moved the required VAS application and training steps to new Appendix A. Clarified responsible parties for required actions, where applicable. Clarified “Data Deletion” section
3.0	19-Oct-2021	Removal of VAS account procedures. Minor wording changes.
4.0	01-Dec-2022	Added clarification on available University data sharing resources.
5.0	01-Dec-2023	Minor editing. Removed Appendix A as it is available thru the IG resources SharePoint site.



Review History

Version	Date of Review	Reviewed By	Summary of Review and Actions
1.0	25-Nov-2019	SIRO, IT/G	Reviewed and recommended to IG Committee for adoption
2.0	15-Oct-2020	HEAD and	
3.0	19-Oct-2021	SIGM	
4.0	01-Dec-2022		
5.0	01-Dec-2023	SIRO, IT/G HEAD, SIGM and IGO	