



## IT Services Policy

---

### ITS1390B-Dropbox use by Exception Policy

Prepared by Kemi Odukoya and Lisa Francis

<b>Last Review Date:</b>	<b>22/01/2024</b>	<b>Next Review Date:</b>	<b>Policy has been approved</b>
--------------------------	-------------------	--------------------------	---------------------------------

<b>Reviewers:</b>	<b>IGG (Information Governance Group)</b>
-------------------	---

As per approvers and distribution list

**Policy Owner: Anne Parry**

<b>Name/Position</b>	Anne Parry- Faculty Director of Operations
----------------------	--

**Revision History**

<b>Version</b>	<b>Description</b>	<b>Author</b>	<b>Date</b>
1	Initial version	Kemi Odukoya	24/04/23
2	Update	Valerie Olatunji	01/09/23
3	Update	Kemi Odukoya	16/10/23
4	Review and update	Rupa Dey	22/11/23
5	Review and update	Lorna Ireland	27/11/23
6	Review and update	Natalie McCloskey, Anne Parry, Rupa Dey	01/12/23

**Authorisation:**

<b>Name / Position</b>	Rachel Bence, Chief Information Officer, IT Services
<b>Signature</b>	<b>Rachel Bence</b>
<b>Date</b>	<b>16-Feb-2024</b>

APPROVALS

Name	Title	Date of issue	Version
Anne Parry	Faculty Director of Operations (FDO), S&E	22/01/2024	V1.0
Natalie McCloskey	Deputy FDO, FMD	22/01/2024	V1.0
Lorna Ireland	Deputy FDO, H&SS	22/01/2024	V1.0
Jo Young	Deputy FDO, S&E	22/01/2024	V1.0
Rupa Dey	Deputy Chief Information Officer	22/01/2024	V1.0
Tom King	Assistant Director, ITS Research	22/01/2024	V1.0
Sade Giwa	Programme Manager	22/01/2024	V1.0
Geoffrey Providence	Head Of Hybrid Platforms	22/01/2024	V1.0
Shelim Miah	Risk and Governance Manager	22/01/2024	V1.0
Tim Passe	IT Security	22/01/2024	V1.0

## Contents

Contents.....	4
<b>1. Policy Statement.....</b>	<b>5</b>
<b>2. Dropbox Managed Solution Implementation Objectives .....</b>	<b>5</b>
<b>3. Coverage and Scope .....</b>	<b>6</b>
<b>4. Policy Detail .....</b>	<b>6</b>
<b>Do's.....</b>	<b>6</b>
<b>Don'ts.....</b>	<b>7</b>
<b>5. Dropbox Approval Process and Procedure .....</b>	<b>8</b>
<b>6. Roles and Responsibilities.....</b>	<b>9</b>
6.1 End User .....	9
6.2 Line Manager .....	9
6.3 School/Institute Managers.....	10
6.4 Faculty Director of Operations (FDO).....	10
6.5 IT Services .....	10
<b>7. Compliance and Enforcement.....</b>	<b>10</b>
<b>8. Policy Review .....</b>	<b>11</b>
<b>9. Exceptions.....</b>	<b>11</b>
<b>10. Related Documents .....</b>	<b>12</b>
<b>11. References .....</b>	<b>12</b>
<b>12. Terminology .....</b>	<b>12</b>
<b>13. Appendix A - Definitions .....</b>	<b>13</b>
<b>14. Appendix B: Email Confirmation of Acceptance .....</b>	<b>13</b>
<b>15. Distribution.....</b>	<b>14</b>

## 1. Policy Statement

This Policy outlines the appropriate use of Dropbox for institutional file sharing and storage purposes within Queen Mary University of London. This Policy aims to establish a secure and controlled approach to Dropbox use within the university; ensuring that it is employed judiciously, primarily for external research collaboration and in strict accordance with established information governance standards.

## 2. Dropbox Managed Solution Implementation Objectives

The primary objective of this policy is to develop a governance framework that:

- **Establishes clear criteria**, as well as processes and procedures for the use of Dropbox at Queen Mary University of London.
- **Ensures data security and compliance with cybersecurity standards**; in line with the University's internal policies such as Information Classification Policy (DG09).
- **Identifies and captures all unmanaged Dropbox accounts within the Queen Mary domain**. This involves migrating eligible personal or individual accounts to QMUL managed accounts. Non-eligible users, based on the governance model, will need to move their data to alternative managed secure solutions, for example, Data Safe Haven, SharePoint etc.

This initiative is driven by the current lack of oversight and visibility regarding the type and security of data stored on Dropbox, please refer to the business case. The anticipated benefits of a governance framework are to ensure greater transparency, research protection and GDPR compliance. This strategic alignment is pertinent to Queen Mary University of London's research and innovation goals.

Queen Mary University of London aims to implement robust account management practices, including the implementation of Multi-Factor Authentication (MFA), for all Dropbox users within the QMUL domain. This objective is motivated by security and data protection. By ensuring proper account management and security measures, QMUL aims to enhance the protection of data stored on Dropbox. The anticipated benefits include:

- Improved security measures.
- Reducing the risk of data breaches and cyberattacks, which in turn provide a more secure environment for both end-users and stakeholders.

By reducing the number of unmanaged Dropbox accounts, QMUL can mitigate potential security risks associated with these and ensure that Dropbox use aligns with the university's policies and standards. This objective is imperative to ensure compliance with established policies and standards.

### 3. Coverage and Scope

- 3.1 This policy applies to all employees, Queen Mary University of London affiliates, agency employees, contractors, third parties, undergraduate and postgraduate research students (hereby referred to as 'employees'), who are provided with access to Queen Mary University of London IT accounts, with the intention or permission to use Dropbox within the Queen Mary University of London domain.
- 3.2 This policy covers all locations, including remote workers and overseas campuses.
- 3.3 This policy covers the use of IT accounts owned and issued by Queen Mary University of London.
- 3.4 The use of personal devices and accessing information from third-party devices, in reference to Queen Mary University of London.
- 3.5 This policy covers all forms of Dropbox use for Queen Mary University of London information in all forms, when it is created, collected, processed, shared, stored, or destroyed.

### 4. Policy Detail

#### Do's

- 4.1 All of Dropbox capabilities are locally funded (Schools and PS Functions), we have established this policy mandating quarterly reviews of the Dropbox enterprise solution within each faculty area.  
  
These reviews facilitate our ability to ascertain the adherence of Dropbox Enterprise solution users to policy guidelines and to accurately reconcile charges incurred from Dropbox services.
- 4.2 To uphold adherence to Queen Mary University of London's policy guidelines regarding the use of digital platforms and tools, all users are mandated to complete an assessment form for Dropbox usage.
- 4.3 Dropbox use at Queen Mary University of London shall be within a secure managed service under the university's enterprise licensing.
- 4.4 Dropbox use shall be limited to file share and storage for official business activities only; in situations where existing secured managed solutions such as OneDrive and SharePoint for Business (ODFB) cannot be used.
- 4.5 OneDrive and SharePoint for Business remains the primary and preferred file share and storage solution at and shall be used for all internal collaborations within the Queen Mary University of London's community.
- 4.6 Dropbox licences shall be issued only if a user is not able to conduct external collaborative research using QMUL's existing authorised secure solutions i.e. SharePoint/OneDrive.

- 4.7 In addition to satisfying the criteria listed above, users shall receive a prerequisite approval from their respective line managers, School/Institute Managers and Faculty Directors of Operations (FDO), before a Dropbox licence is granted.
- 4.8 Dropbox users, within the secure managed enterprise solution, shall be required to provide a relevant budget code.
- 4.9 Dropbox users shall ensure that files stored on Dropbox are directly related to institutional activities and do not violate any applicable laws, regulations, or institutional policies, e.g. GDPR.
- 4.10 Dropbox users shall reports any suspicious activity immediately to the Information Security Team.
- 4.11 Dropbox shall be used in accordance with the Information Governance policies.  
<https://www.its.qmul.ac.uk/governance/policies/>
- 4.12 Dropbox users shall ensure that files stored on Dropbox are directly related to institutional activities and do not violate any applicable laws, regulations, or institutional policies, e.g. GDPR.
- 4.13 When an employee or contractor leaves the institution, or no longer requires access to Dropbox, their account shall be promptly deactivated to prevent unauthorised access to institutional files.
- 4.14 IT Services reserve the right to monitor Dropbox usage for compliance with this policy.  
[ITS Policy Dropbox Use by Exception v1.0.docx](#)
- 4.15 Failure to comply with this policy may result in disciplinary actions, including account suspension or termination.
- 4.16 This policy will be reviewed and updated annually, to ensure its effectiveness and relevance.
- 4.17 Dropbox users within Queen Mary University of London must acknowledge and comply with this policy.
- 4.18 Users accessing their personal Dropbox accounts are required to utilise them solely for personal use and are prohibited from storing any institutional data within these accounts.

## Don'ts

- 4.18 Persons who do not meet these criteria should not use Dropbox for any business purposes.
- 4.19 In addition, Queen Mary University of London employees shall not use personal Dropbox accounts for official business and academic purposes.
- 4.20 Dropbox shall not be used for internal file sharing; but only for sharing files externally, with known official collaborators, related to institutional activities.

- 4.21 It is essential to emphasize that merely asserting the historical or widespread internal Dropbox use or deeming the use of existing secure and managed alternatives as inconvenient, shall not suffice as a valid ground for Dropbox use at Queen Mary University of London.

## 5. Dropbox Approval Process and Procedure

- 5.1 End-users seeking to obtain a Dropbox managed account shall adhere to a standardised procedure. This process commences with the user's deliberate decision to opt for a Dropbox managed license. Subsequently, a formal approval process shall be followed.
- 5.2 Users requesting a Dropbox account are required to submit a request for approval to the respective line manager, School/Institute Manager and FDO. Dropbox licences shall only be issued after approvals have been granted at all required levels.
- 5.3 The line manager will assess the request to determine its alignment with departmental requirements, the user's role and in line with the stipulated criteria for Dropbox use at QMUL.

The line manager's approval or denial of the request will be communicated to the user for license allocation or rejection. If approved, this shall be forwarded to School/Institute Manager and then to the FDO.

The FDO will assess the request in line with its alignment with the faculty requirement considering the stipulated criteria for Dropbox use at QMUL for final approval or rejection.

Users in the Central Professional Services Directorate who may require a licence for official work are requested to seek approvals from their respective line managers, Head of department and then, the Chief Information Officer.

- 5.4 Users are encouraged to provide detailed justifications and explanations in their license allocation requests to facilitate the line managers/SM/FDOs decision. Requests that fall short shall regrettably face rejection.
- 5.5 In cases where a line manager or School Manager denies a license request, the user may appeal the decision following QMUL's established appeals processes.
- 5.6 Line managers, School Managers and FDOs (Faculty Director of Operations) shall refer to the stated Dropbox criteria to ensure that approvals are granted only when these criteria are unduly met.
- 5.7 Following the prerequisite approvals, requests for Dropbox licences shall be submitted to the IT Service Desk via email or using the self-service portal. [Log on | Ivanti \(qmul.ac.uk\)](#)



## 6. Roles and Responsibilities

### 6.1 End User

- Users are responsible for initiating license allocation requests for Dropbox within the managed solution. They are required to provide accurate and complete information in their requests for approvals.

Users are advised to continue to use existing managed and secure storage platforms such as *OneDrive for Business*, *Apocrita (ITS Research Storage)* and *Data Safe Haven (FMD)*. If you need further guidance on these storage platforms, contact the IT Research Facilitator at [its-research-consultants@qmul.ac.uk](mailto:its-research-consultants@qmul.ac.uk) to assist you in using a suitable storage/sharing platform for your data.

The end-user of the Dropbox account shall ensure that all the data is stored/shared according to Queen Mary University of London's Information Classification Policy, and appropriate controls are in place as defined by it. There is to be compliance adherence to the Information Storage Matrix in DG09.

<https://www.its.qmul.ac.uk/governance/policies/>

- Furthermore, researchers are reminded to ensure that they adhere to any specific condition set by the data owner for processing and storing data for individual research projects (i.e. as defined by data management plans/research protocol).

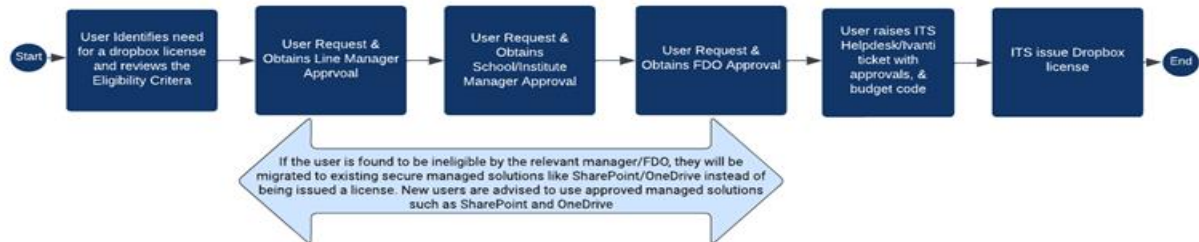
In all cases, personal identifiable information (PII) should not be held on a Dropbox account without a detailed assessment of the risks involved. This can be undertaken by the ITS Research Facilitators, ITS Information Security team and/or Barts Cancer Institute IT staff.

- **Incident Reporting** -Any security-related, theft or data loss incidents shall be raised immediately with the ITS Service Desk. Live Chat: [ITS Live Chat - IT Services \(qmul.ac.uk\)](#)  
Phone: +44 20 7882 8888 or [servicedesk@qmul.ac.uk](mailto:servicedesk@qmul.ac.uk). In addition, the Records & Information Compliance Manager should also be informed at [p.smallcombe@qmul.ac.uk](mailto:p.smallcombe@qmul.ac.uk)

### 6.2 Line Manager

- Line managers are responsible for the initial review of user requests for Dropbox licences promptly. Requests shall be reviewed in alignment with departmental needs and considering the established criteria for Dropbox use at Queen Mary University of London.
- Line managers are expected to approach these requests with the understanding that the university has invested heavily in safe, managed, and secure file share and storage solutions.

### DROPBOX APPROVAL FLOW



**If at any point the user is found to be ineligible to use Dropbox by their Manager/FDO, a license will not be issued and the user will be migrated on to existing secure managed solutions such as SharePoint /OneDrive**

#### 6.3 School/Institute Managers

- Where appropriate, School/Institute Managers are responsible for the second line review of user requests for Dropbox licences promptly. Requests shall be reviewed in alignment with departmental/School needs, availability of fundings and considering the established criteria for Dropbox use at Queen Mary University of London.
- School/Institute managers are expected to approach these requests with the understanding that QM has invested heavily in safe, managed, and secure file share and storage solutions; as well as the heightened risks and associated costs and cost-effective delivery of research and other critical School/Institute activities.

#### 6.4 Faculty Director of Operations (FDO)

- FDOs serve as the third level of approval for Dropbox licences. FDOs are responsible for reviewing user requests for Dropbox licences promptly. Requests shall be reviewed only after line manager approvals. Requests shall be reviewed considering the established criteria for Dropbox use at Queen Mary University of London.
- FDOs are expected to approach these requests with the understanding that the university has invested heavily in safe, managed, and secure file share and storage solutions; as well as the heightened risks and costs associated with Dropbox use.

#### 6.5 IT Services

- IT Services are responsible for monitoring compliance, implementing approved license allocation requests, and maintaining accurate records of licenses issued.

### 7. Compliance and Enforcement

- The designated local Dropbox Admin license holders are tasked with managing user accounts within each faculty area., including creating, modifying, and removing accounts as needed.

They ensure that access privileges are appropriately assigned based on user roles and responsibilities.

- The responsibilities of Dropbox Admin License holders include conducting quarterly review of Dropbox usage within their respective areas. These reviews serve the dual-purpose of upholding compliance with the Use by Exception policy across faculty areas and ensuring the accuracy of associated Dropbox license costs from a financial standpoint.
- Failure to comply with this policy may result in license allocation delays, or other appropriate disciplinary actions in accordance with organisational policies.

Compliance with the policies and procedures, laid down in this document, will be monitored by IT Services and Dropbox licences within the Queen Mary University of London's managed solution shall be audited quarterly.

The Head of Platforms, IT Services, in conjunction with the Assistant Director, Research is responsible for the monitoring, revision and updating of this document.

Users are expected to be truthful and provide accurate information in all cases relating to this policy. Dropbox shall be used in accordance with the Information Governance policies. <https://www.qmul.ac.uk/governance-and-legal-services/policy/>

IT Services staff may remedy any discrepancies or advise users on the best practice. As with all agreed university policies, wilful contravention of this IT policy can be considered a disciplinary offence that can be reported to senior staff within the School, Institute or Department and/or lead to the revoking of the license or other standard disciplinary measures.

Please find link to policies below:

[QMUL Discipline and Policy Procedure](#)

[QMUL Policies and Procedures](#)

## 8. Policy Review

This policy will be reviewed annually to ensure its effectiveness and relevance to revisions organisational needs. Any necessary updates or will be made by IT Services.

## 9. Exceptions

This policy is effective from dates as per stated at the beginning of the policy. In the event of any exceptions that are not addressed by this policy, the matter will be first referred to the appropriate Faculty Relationship Manager for advice and guidance.

## 10. Related Documents

Information Security policies can be found at  
<https://www.its.qmul.ac.uk/governance/policies/>

Other related policies can be found at

[Policy zone - Directorate of Governance and Legal Services \(qmul.ac.uk\)](https://www.qmul.ac.uk/governance-and-legal-services/)

Overarching Policies can be found on the QMUL Policy Zone page under “Information and IT-related policies and procedures” at:

<https://www.qmul.ac.uk/governance-and-legal-services/policy/>

## 11. References

DG09 – Information Classification Policy

All users of services provided by QMUL ITS must abide by the ITS Policies and Standard Operating Procedures (SOPs) that can be found at:

<http://www.its.qmul.ac.uk/governance/policies/index.html>.

## 12. Terminology

The following terms will be used throughout the policy:

- Shall; is used to state a mandatory requirement of this policy.
- Should; is used to state a recommended requirement of this policy.
- Dropbox refers to the file share and storage solution provided under the trademark Dropbox.
- External organisations refer to entities outside of Queen Mary University of London with which users interact or collaborate for various official purposes.

### 13. Appendix A- Definitions

Term	Meaning
Owner, End-user, You/your	All these terms are used interchangeably to mean the end-user/owner. The principal user who requested the Dropbox account
Dropbox account	An account where data is stored, shared, and managed by Dropbox™
DMP (Data management plan)	Data Management Plan used widely by various funding bodies EPSRC/UKRI
ODfB (OneDrive and SharePoint for Business)	QM’s SharePoint and OneDrive for Business (data storage platform) <a href="https://www.its.qmul.ac.uk/services/service-catalogue-items/communication-and-collaboration/email-and-collaboration-services/file-sharing/">https://www.its.qmul.ac.uk/services/service-catalogue-items/communication-and-collaboration/email-and-collaboration-services/file-sharing/</a>
Apocrita	ITS Research storage platform attached to the Apocrita HPC (High Performance Computing) service.

### 14. Appendix B: Email Confirmation of Acceptance

You should add the text below to your email request for a Dropbox account. By sending the text below (*Italic*) you accept your responsibility and obligations outlined in this policy document and other reference documents therein.

*I acknowledge and agree to comply with the proper use of Dropbox to conduct University work as detailed in the Dropbox policy document and other documents listed in the reference section of the document and agree to the terms and conditions therein.*

*I will engage in any audit or review of my Dropbox account and understand that failure to show compliance with this policy may lead to my right to have my Dropbox license being suspended or revoked.*

## 15. Distribution

Name	Title	Date of issue	Version
Rupa Dey	Deputy Chief Information Officer	20/02/2023	V0.1
Sade Giwa	IT Programme Manager	20/02/2023	V0.1
Tom King	AD, ITS Research	20/02/2023	V0.1
Geoffrey Providence	Head Of Hybrid Platforms	20/02/2023	V0.1
Shelim Miah	Risk and Governance Manager	20/02/2023	V0.1
SMT (Senior Management Team)	Members of the Senior Management Team	20/02/2023	V0.1
Tim Passe	Head of Information Security	20/02/2023	V0.1
Matthew Trump	Information Security Manager	20/02/2023	V0.1
Paul Smallcombe	Records & Information Compliance Manager	20/02/2023	V0.1
Skender Osmani	Head Of Client Devices & Audio Visual	20/02/2023	V0.1
Roshan Hewavitarne	Head of Operations and Service Management	20/02/2023	V0.1
Beth Prescott	Faculty Relationship Manager, FMD	20/02/2023	V0.1
Phillip Goodfellow	FRM S&E	20/02/2023	V0.1
Sophia Eglin	Faculty Relationship Manager, HSS	20/02/2023	V0.1
Agnieszka Jankowska	Head of Change and Student Experience	20/02/2023	V0.1