Microsoft 365
Guidance for Use

Microsoft 365 (M365) at The University of Birmingham includes the applications OneDrive for Business (OneDrive), Teams and Forms. More M365 applications will follow and we will provide relevant guidance upon release.

The guidance for M365, Delve, OneDrive, Teams and Forms will ensure that:

- You understand the University's data storage and processing requirements;
- Personal Data is processed in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018;
- We all maintain data security, confidentiality and integrity, and save and store our data appropriately to prevent unauthorised access; and
- The University complies with all of its contractual arrangements relating to data storage and processing.

These guidelines *do not* include information on:	**Where you will find that:**
What each of the M365 applications is and what you can use them for.	The Microsoft 365 Roadmap on our Microsoft 365 Hub explains what each of the M365 applications is. Infographics available on the Hub will help you understand the purpose of each application.
Learning how to use M365.	The Microsoft 365 Hub contains a wide range of easy access training as well as links to other learning opportunities and resources.

Definitions

Data More than just numbers and factual information, this includes all information processed e.g. anything in a document or spreadsheet, text, video, audio or image files, IP address, chat files etc.

External Individuals who do not have a User Account provided by The University of Birmingham.

Personal Data Information relating to natural living persons who can be identified or who are identifiable directly from the information in question or who can be indirectly identified from that information in combination with other information.

Special Category Data Personal data that needs more protection because it is considered 'sensitive'. This additional protection is extended to data revealing racial or ethnic origin; political opinions; biometric data; data concerning health; trade union membership; religious or philosophical beliefs; genetic data; data concerning a person's sex life; and data concerning a person's sexual orientation. Similar protections are also afforded to Criminal Offence data under the Data Protection Act 2018.

Tenancy	A tenant is a term used for a Microsoft 365 organisation; our tenancy is The University of Birmingham data storage space within the overall Microsoft 365 data centres.
User	Anyone who has a User Account provided by The University of Birmingham.

Support

If you have any questions or concerns about the type of data you are processing, please contact Legal Services for advice and guidance.

Microsoft 365 Suite

This information applies to all M365 applications:

Data encryption Data stored in M365 is encrypted on Microsoft's servers and when transmitted between Microsoft's servers and the client device, ensuring that your data is protected. Data is not encrypted on any user's device unless the device is encrypted.
Data ownership The University retains full ownership of all data. Microsoft has no rights to the data.
Storage locations Data stored within M365 is primarily stored within the UK. Some services store data elsewhere within the EU such as Forms, Whiteboard, InTune and Planner, or occasionally within the US.
Data backups Data backups are not provided for users at launch. We will communicate details of backup provision as it becomes available.
Activity logs Activity and access logs are available to authorised individuals for some services and can be retrieved upon receipt of an authorised request.
Network drives Availability of existing personal and network shared drives will continue.
External collaboration M365 allows easy collaboration with external organisations. When using another organisation's tenancy, you may be subject to their governance and policies as well as our own, and you should be mindful of what data you share. When using our tenancy, externals are subject to University governance and policies as well as their own.
Use on a mobile device University M365 applications are securely accessible from mobile devices. You can find guidance in our IT Knowledge Base. Mobile app access is not possible if you access the same apps for a different organisation, e.g. NHS, which requires a similar level of security for data accessed through personal devices. Access through the web is possible.

Full mobile access to work has a risk of blurring the lines between work and personal life. Consider your wellbeing and personal security when deciding whether or how to use M365 applications from your personal mobile device.

Data restrictions
M365's security and encryption features comply with the University's security standards. The University will not impose technological restrictions on the format or types of data that can be stored on M365. You are responsible for managing the suitability of using cloud storage and M365 based on:

- Whether the M365 cloud storage platform complies with any contractual agreements regarding data storage.
- Compliance with the institutional Data Protection Policy, GDPR and the Data Protection Act 2018.
- IT policies, standards and guidance.
- Appropriate Content – ensure that content uploaded is in line with the University General Conditions of Use of Computing and Network Facilities.

Information classification
The University has three categories of information classification: Confidential, Restricted and Open. For M365 no restrictions are applied on information classification, this is in contrast to some other systems, like Contensis (internet and intranet platform), where you are not permitted to store information that has been classified as Confidential.

Personal use
You are required to use M365 only for work and work-related purposes and content. You must not use your University OneDrive account to store non work-related content, nor should you share non-work data using University M365 services.

We will not impose technical restrictions in terms of data formats and types, however:

- In accordance with our University legislation all data uploaded into the University's systems are owned/controlled by the University, not the individual.
- In certain permitted circumstances the University is required to access information for lawful purposes and has the authority to pass such data to third parties, as required by law, including for the prevention and detection of crime, the purposes of litigation, and compliance with statutory obligations, such as data protection and freedom of information etc.

Data sharing
M365 grants users the ability to share files both internally to the University and with individuals outside the University. You **must not** grant direct access to files and folders within M365 to external people / bodies and should only share files / folders with them via links.

When sharing data:

- You must ensure that the people you are sharing with have the right to access the data.
- If you grant an internal user edit rights when sharing a file with them they will be able to share that file with other internal users. If an internal user shares a file you have granted them the ability to edit to another internal user, you will receive an email to inform you that the file has been shared on.

- To share files with internal or registered external users, you should provide a link to a file.
- To share files to an external user that is not registered, you should provide a link to a file. This link will require a verification code which will be emailed to the unregistered external user when they first attempt to access the file shared with them. The code will expire after 14 days and the unregistered external user will be prompted to generate a new code on their next attempt to access the file.

When changing roles or leaving the University, users are responsible for ensuring that the ownership of any shared data they manage is transferred to another appropriate internal user. The new data owner should be granted the relevant permissions needed to manage that data prior to the original owner leaving the relevant post.

Delve

Delve allows users to provide a variety of information about themselves to anyone within the organisation. The University's Active Directory populates Delve with the data it holds on the user within Active Directory. Any additional information is entered by the user and users should be aware that by doing this they are sharing that information with all members of UoB staff and students.

Delve allows users to locate files that have been shared with them easily. It is critical that when sharing files in any M365 application the user ensures that the individuals they are sharing the files with have the right to access the data shared. Users should ensure that files are only shared with users who have the right to access the data contained within those files.

OneDrive for Business

Data storage

We allocate each user an initial 100 GB of storage in OneDrive (with the available option to request more storage space through the IT Service Desk). Do not upload data into your account that are not work related. The University has ownership of all data held in M365.

We grant authorised IT administrators access to user accounts where it is necessary for legal obligations to comply with access requests, or in the event of long-term absence.

Data synchronisation

Data can be synchronised on University devices. Data synchronisation is permitted on non-University or personal devices however you must comply with the terms of use:

- You are responsible for ensuring data stored on your personal device does not contain any personal data. Such data must remain protected within University managed and encrypted devices.
- Users must delete all University data from their personal devices once they have left the University.

Data sharing

You can share data within OneDrive both internally and with individuals outside the University. When sharing data:

- You must ensure that the people you are sharing with do have the right to access the data.
- To share files, you can provide a link to a file to anyone who is an internal user or a registered external user.
- To share files to an external user that is not registered, you can provide a link to a file. This link will require a verification code which will be emailed to the unregistered external user when they first attempt to access the file shared with them. The code will expire after 14 days and the unregistered external user will be prompted to generate a new code on their next attempt to access the file.
- You **must not** grant direct access to files and folders within OneDrive to external people / bodies.

Data access
You can view and edit files and folders online via a web browser from any device. You must delete all data downloaded on devices via web browsers from any M365 service when is no longer required.

Data retention
Data stored within OneDrive on an active account has a retention period of a maximum of 93 days after deletion.

The OneDrive recycling bin has limited capacity and therefore data may be deleted earlier than 93 days if the limit is reached (files are removed from the recycle bin starting from the oldest date of deletion).

After this retention period, the data is unrecoverable.

The data retention period for staff who leave the University is 11 months plus 30 days. Once a member of staff has left the University, the account is inaccessible to them. Only authorised IT administrators can access the data within the stated retention period. This is relatively easy within the 11 months, but is more difficult during the 30 final days as it requires third party assistance.

Microsoft Forms

Files uploaded to Forms
Any files uploaded to Forms are stored in the OneDrive of the form's owner. If a form is created as a group Form, files are stored in a SharePoint site linked to the group which owns the form.

Recording identity of submitters
By default, Forms will not capture the identity of people who complete and submit a form. If you want to capture identity information, you must enable it in your form's settings, ensuring that you inform respondents that their personal data is being captured appropriately. Resources for ensuring information is captured in accordance with Data Protection Law is found on the Legal Services Intranet page.

Forms for external use
You can create and share forms, surveys and quizzes for people external to the University to complete. You cannot share a form's editing rights or access to a form's summary responses outside the University.

Third party survey tools
Where possible, you should use Forms to develop online data capture forms or surveys rather than external third-party tools, for example Survey Monkey, FormDesk, Formstack, Lime Survey, Smart Survey in order to minimise the risk of data breach.

Embedding Video and Image files in forms
When embedding a video or image file in a form, users should ensure they comply with all University policies and standards, as well as Copyright and Intellectual Property restrictions.

Microsoft Teams

Teams and channels

- You can request the creation of a Microsoft Team through the IT Service Desk. The responsibility for data within the site sits with the primary and secondary Team owners identified in the request process.
- Team owners are responsible for managing the Team including making sure all individuals have the right to access data shared within the Team, and the conversations reflect University policies, Data Protection Law and any relevant Data Sharing Agreements and contracts.
- A SharePoint Online site is automatically created when you create a Team. Each channel within your Team corresponds to a SharePoint Online document library folder.
- Files that you share within a Teams chat are stored in your OneDrive folder. Files shared in a group chat are stored within the creator of the group chat's OneDrive, in a folder called Microsoft Teams Chat Files.
- Any files shared within a Team are automatically added to the files tab in the corresponding Team channel.
- You can invite users external to the University to join a Team. Their access is limited and they cannot create, delete or edit channels. It is important to be mindful, that once they join the Team they can see all Chats, conversations and files shared within the Team channels to which they have access, including historic Chats and information.

Chats

- As a conversation based collaboration platform, Teams offers the ability to chat with other users outside of an individual team or group.
- Your conversation history and chats are retained after you close the Teams application and are available when you next open it. They are covered by the OneDrive data storage and retention principles.
- All participants in a Teams chat can view the entire content of the chat. This includes participants who decline meeting invitations or disconnect from the meeting before it ends.
- You can delete or edit messages. All messages, including the originals, are intended as a business tool and can be searched and/or recovered in response to Freedom of Information and Subject Access requests etc.

- Whilst no technical restrictions are in place, do not send sensitive information and special category personal data via Teams chat messages.
- If you invite externals to a chat, make sure the contents of the discussion and any files are appropriate for them to access. **The external's organisation may retain a copy of the conversation on their systems.**

Meetings and calls

- Each meeting has a chat feature visible to anyone who receives an invitation to the session regardless of whether they attend. Chat guidance also applies to the chat facility during a meeting or call, including guidance about external users.
- All attendees (including one-time attendees) of a recurring meeting or series have full access to the chat of previous meetings including current and future meeting chats. While you can remove someone from a meeting chat, they will retain access to the chat history even after they are removed.
- It is important to be mindful of what information you display on your screen when presenting and sharing your screen, and who you are giving control of your screen to.
- The digital whiteboard is a useful tool for collaborating in a meeting but please note that external guests cannot see the whiteboard.
- If you invite externals to a meeting or call, make sure the contents of the discussion and any files are appropriate for them to access.

Relevant Policies and Further Reading

All staff must:

- Adhere to the University Information Security and Management Policy. You will find IT policies, standards and guidance documentation on the extensive IT policies and procedures portal.
- Complete the mandatory Information Security Awareness training and Data Protection training.
- Ensure compliance with:
  - Data formats and types: the policies apply to all data formats and types (textual, audio, video, image).
  - The immediate reporting of any loss of data, breach of Data Protection law, or "near miss" to Legal Services. To do that, submit a Data Protection Incident Reporting Form. Data Protection incidents can have a significant impact on the University and must be reported without delay.

Other relevant policies:

- Data Protection Portal
- Freedom of Information
- University of Birmingham Privacy Notices

Information Commissioner's Office (ICO) guidance on the legal basis for processing data.