

Privacy Impact Assessment

Worked example for Office 365

Contents

[1 Introduction to the worked example 2](#_Toc513036684)

[2 Office 365 – Privacy Impact Assessment 3](#_Toc513036685)

[3 Step One – Identify the need for a Privacy Impact Assessment 4](#_Toc513036686)

[3 Step Two – Describe the information flows 5](#_Toc513036687)

[3.1 Current email information flow 6](#_Toc513036688)

[3.2 Proposed email information flow 6](#_Toc513036689)

[3.3 Student email, calendar etc. 7](#_Toc513036690)

[3.4 SharePoint Online 7](#_Toc513036691)

[3.5 OneDrive for Business 7](#_Toc513036692)

[3.6 Skype for Business 7](#_Toc513036693)

[3.7 Yammer 8](#_Toc513036694)

[3.8 Forms 8](#_Toc513036695)

[3.9 Azure AD 8](#_Toc513036696)

[3.10 Significant differences 8](#_Toc513036697)

[4 Step Three – Identify the privacy and related risks 10](#_Toc513036698)

[5 Step Four – Identify privacy solutions 18](#_Toc513036699)

[6 Step Five – Sign off and record the PIA outcomes 18](#_Toc513036700)

[7 Step Six – Integrate the outcomes into the project plan 28](#_Toc513036701)

[8 Consultation 31](#_Toc513036702)

[9 Annexe – Further information on Office 365 components 32](#_Toc513036703)

[10 Acknowledgements 33](#_Toc513036704)

[11 Copyright, disclaimer and availability 33](#_Toc513036705)

# Introduction to the worked example

The following pages show a worked example of a Privacy Impact Assessment for provision of Office 365 to staff at the fictional University of Edgestow. It is intended to illustrate the guidance in the UCISA Privacy Impact Assessment Toolkit[[1]](#footnote-1).

As well as giving some useful information on the privacy aspects of Office 365, it represents a complex example as there will be many types of information involved and many different use cases.

**Scenario**

The example assumes that Office 365 is already used by undergraduate students and taught Master’s students, and that research Master’s students, postgraduate students and staff are currently using on-site Exchange for email and calendaring. A number of unofficial file sharing services are known to be in use amongst students and staff.

The University is research intensive, and undertakes research in some sensitive areas such as peace studies, climate change, medicine and criminality.

**Disclaimer**

The product information presented is thought to be correct at the time of going to print, but you should check that it is still current, as new features are added to Office 365 at frequent intervals.

**It is also important to note that the use cases and the solutions identified may not be applicable to your institution. In the example Privacy Impact Assessment (PIA), solutions include turning of Yammer and Sway, and consideration of implementing a hybrid Exchange approach. These are not recommendations of UCISA, Microsoft or the Information Commissioner’s Office – they are just how the University of Edgestow decided to address some of the privacy risks identified. There is no implication that the solutions listed in the example are in any way the ‘correct’ solutions.**

Many of the risks identified in the PIA are applicable beyond the Office 365 project. In some cases, Edgestow has decided to constrain the solutions to stay within the scope of the project. In other cases (for example RISK 020, adequacy of existing policies, or RISK 023, the use of Forms) the solutions chosen involve a wider review of practice in the university. You will have to decide for yourself the best approach to suit your project and institution.

**The example is intended to help with your Privacy Impact Assessment; not to substitute for it.**

# Office 365 – Privacy Impact Assessment

This document records the outcome of a Privacy Impact Assessment for deployment of Office 365 to staff at the University of Edgestow.

It follows the approach recommended by the UCISA Privacy Impact Assessment Toolkit[[2]](#footnote-2) and the Information Commissioner’s Office Code of Practice[[3]](#footnote-3).

Office 365 is a ‘hosted’ suite of productivity and collaboration tools and is provided by Microsoft to its UK higher education customers from its datacentres in Europe (currently Dublin and Amsterdam, but with the possibility of moving to UK datacentres in the future).

The University is planning the implementation of Office 365 for staff from September 2018.

The Office 365 platform includes an ever-growing range of facilities, currently including:

* Exchange (email, calendaring, to-do lists etc.)
* SharePoint (team sites, document storage)
* OneDrive for Business (a personal file storage space with the ability to share files and folders)
* Online Office Applications (web based versions of Word, Excel etc.)
* Skype for Business (teleconferencing and videoconferencing)
* Video (video file management, storage and delivery)
* Yammer (social networking for the organisation)
* Sway (digital storytelling)
* Delve (searching across Office 365)
* Flow (process and task automation across apps and services)
* Forms (creation of quizzes, surveys, questionnaires, registrations etc.)
* Planner (tools to organise teamwork)
* Project (project management)
* PowerApps (building custom Apps)
* Dynamics 365 (Customer Relationship Management and Enterprise Resource Planning)

More information about each of these elements of Office 365 is given in the Annexe.

Office 365 also provides users with the right to download and use the Microsoft Office suite (Word, Excel, PowerPoint etc.) on up to five devices.

Undergraduate and taught Master’s students[[4]](#footnote-4) at the University already have access to many Office 365 facilities, whilst staff currently use it only for downloading the Office suite.

The University is currently considering extending the use of Office 365 email, calendaring and to-do lists to staff, research Master’s and postgraduate students[[5]](#footnote-5). This would replace the current staff email system (on-premise Exchange).

In future, some of the other Office 365 facilities could be rolled out to staff and students.

The proposed change involves the processing of staff emails, calendar information, contact lists, tasks, notes, documents, conversations etc. in Office 365.

It is highly likely that some staff emails and documents will contain personal information, or other confidential information.

The data centres involved in the provision of the Office 365 service are located within the European Economic Area (EEA), and most data[[6]](#footnote-6) are never stored outside the EEA. However, the data may be remotely accessed (but not stored) outside the EEA under certain well-defined circumstances. The Data Processor (Microsoft) is subject to US laws that could impinge on its handling of University data.

Furthermore, the Office 365 suite introduces new functionality that could, for example, make the inappropriate sharing of information easier, or allow the gathering of data (such as presence information) that was not previously possible.

Microsoft has ISO 27001[[7]](#footnote-7) and ISO 27018[[8]](#footnote-8) accreditation for the Office 365 service, is a signatory to the Privacy Shield framework[[9]](#footnote-9) and has written the EU Data Protection model clauses into its agreement with the University.

Nevertheless, there are foreseeable privacy risks to be assessed before proceeding with the proposed implementation.

A Privacy Impact Assessment (PIA) represents a well-structured approach to identifying the risks involved and any measures necessary to mitigate those risks. More information about the PIA process is available from the Information Commissioners Office[[10]](#footnote-10).

# 3 Step One – Identify the need for a Privacy Impact Assessment

**Will the project involve the collection of new information about individuals?** *There is a high likelihood that Office 365 could be used by individuals to gather personal data through the Forms feature for example.*

**Will the project compel individuals to provide information about themselves?** *No*

**Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?** *Because the service is hosted outside the UK by an American company, this would require further investigation, so impossible to say no at this stage.*

**Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?** *No*

**Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.** *No*

**Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?** *No*

**Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.** *It is possible that due to the nature of University services or research, information of this nature could be handled within Office 365.*

**Will the project require you to contact individuals in ways which they may find intrusive?** *No*

**Will the project introduce new facilities that might be used by individuals in the institution to gather, process, analyse or share personal information in ways that would previously have required specialist support?** *Yes, Office 365 offers the potential for file sharing with individuals outside the University and an online forms facility that could be used to gather personal data.*

**Will the project involve the processing of personal data by third parties (this would include all cloud based services)?** *Yes, Microsoft will be providing the data processing facility.*

**Will the project expose personal data to elevated levels of security risks?** *Yes, the facility will encourage the use of mobile devices and involve data transmission over the internet.*

**Are stakeholders likely to have privacy concerns about the project?** *Possibly; given the current political climate at least some groups in the University are likely to be concerned about the potential for external access to University information.*

Based on the above information, it has been decided that a complete Privacy Impact Assessment is required.

# Step Two – Describe the information flows

Staff at the University use Microsoft Exchange as the mail service. This runs on servers located on site and managed by University staff.

In general, email is managed entirely by the senders and recipients. The sender creates and sends the email, typically storing the original in a mail folder. Senders and recipients can then manage (store, answer, forward or delete) their copy of the email and any attachments.

The University may need to search across mailboxes to answer valid requests under Data Protection or Freedom of Information legislation, or in response to specific and suitably authorised requests from law enforcement agencies. The University deletes mailboxes and their content within three months of a user leaving.

Email is a store-and-forward technology, so copies of the email and any attachments will be stored temporarily (i.e. until it has been successfully forwarded) on any mail servers that it passes through between the sender and recipients, as well as ‘permanently’ in the sender’s and recipients’ mailboxes and potentially on any devices used to access those mailboxes. These mail servers (the sender’s, the recipient’s and the intermediaries) will also keep ‘metadata’ about the email, typically the sender, recipient(s), date and time, and subject. The length of time that metadata is retained varies according to the policies of and legal constraints on the organisation operating the mail server, but typically would be at least 90 days.

The content of email messages will be highly variable in nature, but it must be assumed that there is the potential for at least some emails to contain unencrypted private, sensitive or confidential information, even though University policy prohibits this. For example, external users sending confidential information by email *to* the University need not comply with the University policy, and may have sent confidential information unencrypted. A copy of this would remain in the recipient’s mailbox. Calendar information, tasks and notes are mostly handled within the host system, and could contain sensitive information. An exception to this would be a calendar appointment or invitation sent to or received from an external user, and this would be handled in a very similar way to email, and has the same potential to contain sensitive information.

## Current email information flow

The following diagram is a highly-simplified view of how email is handled by the existing system:

External email server

Off campus

University staff email users

intranet

University email server



External email user



Internet  
(may or may not be encrypted)

Internet (may or may not be encrypted)

On campus

1

2

3

4

Figure 1 Current Staff Email System

The content of emails is stored on the University mail server and on the correspondent’s mail server.

The following analysis of how email is transmitted assumes that the user has not taken any special steps to encrypt the email or attachments. The content of emails traverses the University’s internal network (1) from on‑campus users to the mail server. If the user is off campus, it must traverse the internet to reach the University email server, and this may be in an unencrypted form (2). If the correspondent is external, the message traverses the internet between the University email server and the external email server (3). Depending on the capabilities of the external email server, this may be encrypted or unencrypted. How the email traverses between the external email server and the recipient (4) is also beyond the University’s control, and should be assumed to be unencrypted and over the internet.

Note that when email is sent from one internal user on campus to another internal user on campus, this is handled entirely by the University email service, and the data never leaves the University.

## Proposed email information flow

With the proposed email system, all email is stored in the Microsoft Cloud, and traverses the internet (1 and 2) even if the sender and receiver are both internal.

Off campus

Microsoft Cloud



External email user



Staff email users

External email server



Internet

Internet (encrypted)

Internet (encrypted)

On campus

1

2

3

4

Figure 2 Proposed Staff Email System

Email being sent to or received from the email servers used by external correspondents (3 and 4) traverses the internet in exactly the same way as it would if the University were using an internally hosted mail service.

## Student email, calendar etc.

Students are already using Office 365 email, calendaring etc. These information flows are as described above, and will not be affected by the proposed changes.

## SharePoint Online

SharePoint Online is a cloud hosted service offering a number of facilities, including:

* individual and group document storage;
* internal and external websites; and
* forms and workflows.

Access to the information held in SharePoint online is generally via a web browser, mobile app or other Office 365 aware applications such as Office 2010 and later. In all cases, access over the internet uses encryption. The data is stored encrypted on Microsoft’s servers.

Access to the information in SharePoint is controlled by a fine-grained access control scheme that only allows individuals and groups with the relevant permissions to read or change the material. It is possible to set up the permissions on individual documents so that they are accessible to users outside the University who have a Microsoft account (for example a personal Hotmail or Outlook.com account or an Office 365 account with another organisation).

## OneDrive for Business

OneDrive for Business is a cloud based facility for individual file storage. It is implemented using the same underlying technology as the document storage facilities within SharePoint Online, but with the focus on individual use rather than departmental or enterprise-wide use.

There are facilities to access the files directly through Office 2010 (and later) applications, through a web interface and through a synchronisation application that allows copies to be maintained on a PC, Apple or mobile device.

Files in OneDrive for Business can be shared with other Office 365 users and with users outside the University.

The encryption of the data in transit and at rest on the servers, and the granularity of access control is the same as for SharePoint Online.

It is also worth noting that the unofficial use of other similar facilities, especially Google Drive and DropBox, is thought to be widespread among students and staff.

## Skype for Business

Skype for Business provides communication facilities including:

* audio conferencing;
* telephony integration;
* video conferencing;
* instant messaging; and
* presence management.

All communications through Skype for Business are encrypted in transit, other than those ‘breaking out’ into the telephone network. External users can be invited to take part in Skype conversations, but the digital communications are still encrypted. Skype for Business calls are all set up through the Office 365 server, but once they are set up only calls involving more than two participants are routed through the Office 365 server. Calls between just two Skype for Business participants are routed directly from one to the other, so if they are both situated on the University network, the traffic does not leave the University network.

Presence information (i.e. whether a user is busy, available, away from desk etc.) is gathered by Office 365 from a variety of sources including:

* appointments;
* the particular client being used;
* keyboard activity and timeouts; and
* direct user choice.

The resulting status information is made available by the user to others under a fine-grained access control scheme, and is visible in Skype for Business and increasingly throughout other relevant Office 365 components. For example, if you add an address to the circulation of an email, some Office 365 components will display the recipients’ current presence status.

## Yammer

Yammer is an enterprise social network tool, and is available free to Universities as part of the Office 365 suite. The communications channels it offers are very similar if not identical (from the functional and privacy perspectives) to those offered by other elements of Office 365, in particular email and chat. However, unlike most other Office 365 elements, Yammer is hosted on USA based servers.

## Forms

Microsoft Forms is a new part of Office 365 Education that allows staff and students to quickly and easily create custom quizzes, surveys, questionnaires, registrations etc. When you create a form, you can invite others to respond to it using any web browser, even on mobile devices. As results are submitted, you can use built-in analytics to evaluate responses. Form data, such as quiz results, can be easily exported to Excel for additional analysis or grading.

The information gathered using Forms is stored on the Microsoft cloud servers in the USA.

## Azure AD

Active Directory is the Microsoft technology used to store information about ‘things’ that Microsoft operating systems and software needs to know about to function properly. These things could be people, computers, storage areas or printers etc. In the case of people, Active Directory (or AD) is where your login name, access rights and password checking information is stored.

To use Office 365, there needs to be a cloud-based version of AD, known as Azure AD, which is kept synchronised with the on-premises AD. While it is not necessary to have all the information in the on-premises AD duplicated in Azure AD, there is inevitably some personal information stored in Azure AD, and therefore in the Microsoft Cloud in the EEA.

## Significant differences

The significant technical differences between the current systems and the full adoption of Office 365 are as follows:

* Staff mailboxes containing sent and received emails and their attachments will be stored on Microsoft’s servers in the EEA rather than on the University’s;
* Calendar information, contact lists, notes, tasks and any attachments will be stored on Microsoft’s servers in the EEA rather than on the University’s;
* Data associated with Yammer, Forms and Sway will be stored on Microsoft’s servers in the USA rather than on the University’s;
* Microsoft’s mail servers will gather and retain metadata on all incoming, internal and outgoing emails, calendar events and other communications;
* Even internal emails, calendar events, contacts, tasks and notes sent and retrieved by users on campus will traverse the Internet between the University and Microsoft’s servers;
* Skype for Business calls involving more than two participants will traverse the Internet between the University and Microsoft’s servers even if they are all on the University network;
* Cross-mailbox search facilities are those provided wholly by Office 365 rather than those provided by the current on-site staff email system and the Office 365 student email system;
* SharePoint, OneDrive for Business and other Office 365 components offer the potential for documents to be shared outside the University under the control of individual users;
* Office 365 has the potential to gather presence information (i.e. when someone is at their PC, on leave, busy, offsite etc.) that could be used for purposes other than presence management in Office 365;
* Azure Active Directory needs to be used to provide the Office 365 service - this is itself a cloud based facility, and it may contain some personal information about the users; and
* Managing the retention of data may be subject to constraints imposed by the design of the Microsoft services in addition to University policies and practice.

The regulatory differences between the proposed and current systems are as follows:

* Law enforcement agencies might approach Microsoft rather than the University for data relating to individuals’ use of email, calendaring, SharePoint, Yammer, Skype etc.;
* Personal data contained in emails, calendar events, SharePoint documents and lists, Skype conversations and Yammer activity are being processed by a third-party Data Processor (Microsoft) on behalf of the Data Controller (the University);
* Personal data contained in emails, calendar events, contact lists, tasks, notes, SharePoint documents and lists, Skype conversations may be remotely accessed (but not stored) temporarily by Microsoft in data centres outside the EEA for fault-finding and in other well defined circumstances; and
* Personal data stored in Sway, Forms and Yammer is stored in the USA.

# Step Three – Identify the privacy and related risks

“Table 1 - Privacy risks and their explanation” lists the potential privacy risks identified from the changes to the information flows outlined above, and provides an explanation for each one, describing how the risk arises. “Table 2 – Impact of privacy risks” examines the potential impacts should these risks materialise.

Note that this list includes all the identified risks, rather than just those that are likely to require addressing. **Solutions for all these risks are identified later in this document.**

Table 1 - Privacy risks and their explanation

| Risk ID | Title | Explanation |
| --- | --- | --- |
| RISK 001 | Personal data handled outside EEA | The University is required to ensure that all processing of personal data for which it is responsible is carried out in accordance with the *Data Protection Act* *or GDPR.* If we use Office 365, which is run by Microsoft and based in datacentres outside the UK, how can the University be sure that all data processing complies with the current legislation? |
| RISK 002 | Unauthorised access to Office 365 content by Microsoft | Because University information (emails, calendar events, documents, files, contacts etc.) would be stored in Office 365 on the Microsoft servers rather than on University servers, the risk of agencies outside the University being able to access it without permission may be increased in comparison with the current arrangements. |
| RISK 003 | Access to Office 365 content by UK authorities |
| RISK 004 | Access to Office 365 content by foreign authorities |
| RISK 005 | Unauthorised access to Office 365 content by third parties |
| RISK 006 | ‘External’ communications may be intercepted in transit | Agencies outside the University might be able to intercept and record, use, disclose, corrupt or block the content of communications (email, meeting invitations, Skype etc.) between University users who are on campus and people off campus (whether University users or external users). |
| RISK 007 | ‘Internal’ communication content may be intercepted by Microsoft in transit | Because most communications (email, meeting invitations, Skype for Business calls between more than two participants etc.) in Office 365 between users goes via the Microsoft servers, the communication leaves the University campus even if all participants are University users connected to the University network. This introduces the risk of interception while the messages are traversing networks that are not under the University’s control.  The access could be used to intercept and record, use, disclose, corrupt or block University communication.  The agencies doing this could be:  • Microsoft themselves;  • UK government, law enforcement agencies or intelligence services;  • foreign government agencies; or  • other agencies, such as ‘hackers’, terrorist organisations or organised crime syndicates. |
| RISK 008 | ‘Internal’ communication content may be intercepted by UK authorities in transit |
| RISK 009 | ‘Internal’ communication content may be intercepted by foreign authorities in transit |
| RISK 010 | ‘Internal’ communication content may be intercepted by third parties in transit |
| RISK 011 | Gathering of metadata on communications by Microsoft | Because most communications (email, meeting invitations, Skype for Business calls between more than two participants etc.) in Office 365 between users goes via the Microsoft servers, the communication leaves the University campus even if all participants are University users connected to the University network. Each of the operators of the networks between the ‘senders’ and ‘recipients’ will maintain a log of the communication. This will contain information such as the network addresses of the computers involved in the communication, the date and time and some basic information about the nature of the communication, although not the detailed content. Individually, this ‘metadata’ is of little use, but when large amounts of metadata are combined there is the potential for patterns to emerge that can reveal a great deal of potentially sensitive information. The security of these logs of communications metadata is dependent on the measures put in place by each of the network operators, and is beyond the control of the University.  The agencies who might attempt to gain access to communications metadata could be:   * Microsoft themselves; * UK government, law enforcement agencies or intelligence services; * foreign government agencies; or * other agencies, such as the network operators themselves, ‘hackers’, terrorist organisations or organised crime syndicates.   Note that this applies even to Skype for Business calls between two on-site users; although the calls do not leave the University network, they will be initially set up by the Office 365 servers, and summary information will be collected by Office 365. |
| RISK 012 | Gathering of metadata on communications by UK authorities |
| RISK 013 | Gathering of metadata on communications by foreign authorities |
| RISK 014 | Gathering of metadata on communications by third parties |
| RISK 015 | Data may be accidentally disclosed, lost or corrupted | The use of Office 365 would allow the storage of large amounts of University information on systems operated by Microsoft, and located away from the University campus. It is possible that the likelihood of accidental information disclosure, loss or corruption on Office 365 might be higher than the corresponding likelihood with the current arrangements. |
| RISK 016 | Search facilities may be inadequate to fulfil Subject Access and/or FoI Requests | The University needs to be able to search efficiently across emails and documents to satisfy Data Protection Subject Access Requests and Freedom of Information Enquiries. Arrangements are in place for the current email and file storage systems, but there is a risk that the equivalent facilities in Office 365 may not be adequate. |
| RISK 017 | Presence information gathered by Office 365 may be used for unauthorised purposes | Office 365 detects information about individuals’ availability from several sources, including diary commitments, the client used to access Office 365, keyboard activity and whether or not they are logged in. This presence information can be used to let other users know the best channels to use for contact. There is a risk that information gathered for this purpose, which reveals a great deal about location and activity over time, could be used for unauthorised purposes. |
| RISK 018 | Documents containing personal information may be inappropriately shared outside the University accidentally | Office 365 allows users to easily share information with people within and beyond the University – it is after all a collaboration tool. There is a risk that the ease with which this can be done could lead to information being shared inappropriately, for example the ‘wrong’ document being shared, a document being shared with the ‘wrong’ user, or sharing with a particular user being left enabled after there is no longer any need. |
| RISK 019 | Personal data might be retained longer than necessary | Microsoft has its own mechanisms for the backup and archive of information within Office 365, and these are not under the control of the University. There is a risk that personal information is retained longer than necessary. |
| RISK 020 | Existing policies may not be adequate | The University’s existing policies around information governance and information security may be based in part on the assumption that personal or sensitive data is generally processed within the University. The introduction of Office 365 could make some of these policies out of date. For example, existing policies might prohibit the storage of University data on external servers. |
| RISK 021 | Personal Information might be inappropriately disclosed through the external directory service | To use Office 365, it is necessary to have some user account details held in Azure Active Directory. This is a cloud based service that holds identity and access information for other Microsoft cloud based services including Office 365. By having these details in the cloud, it is possible that they could be disclosed to third parties. |
| RISK 022 | The introduction of new Office 365 components and integrated apps could lead to the inappropriate sharing of personal data | Microsoft introduce new components of Office 365 at frequent intervals. For example, the “Staff Hub” was introduced on 12th January 2017. Very often, these new components are switched ‘on’ by default, so users may be able to see and use them before the organisation has had chance to evaluate any privacy issues they may introduce.  Similarly, third parties can write applications that integrate tightly with Office 365, and are available through the Office Store. These third-party apps could also introduce new privacy issues. For example, if a new app requests access to your contacts list, and you agree to this, contact details for other people theoretically become available to whoever hosts the third-party app. These third parties may well be outside the EEA. |
| RISK 023 | The use of Microsoft Forms could lead people to supply personal information without understanding how it is processed | Microsoft Forms allows people to easily create questionnaires, surveys, registrations etc. These can be deployed to people outside the University, and the information gathered is stored in Microsoft Office 365 on servers in the USA. People submitting information might assume that it is being sent directly to the University, and therefore not be aware of exactly how and where it is being stored and processed. |
| RISK 024 | Failure to meet confidentiality requirements of research grants | Some research grants may make stipulations about the location of the associated information. There is a risk that the use of Office 365 may contravene these requirements. |

Table 1 - Privacy risks and their explanation

Table 2 - Impact of privacy risks

| Risk ID and Title | Impact on individuals | Compliance impact | Impact on institution |
| --- | --- | --- | --- |
| RISK 001 - Personal data handled outside EEA | Personal data contained in emails, calendar, contacts, documents etc. may not be protected by acceptable data protection legislation. | Organisation might be in breach of *Data Protection Act 1998* principle 8 *GDPR* articles 45, 46, 49. | Reputational damage, possible fines, possible cost of complying with ICO notices/audits. |
| RISK 002 - Unauthorised access to Office 365 content by Microsoft | Personal, sensitive or confidential information may be used for unauthorised purposes, disclosed inappropriately, corrupted, made unavailable or lost. | Organisation might be in breach of *Data Protection Act 1998* principle 7 *GDPR* article 24. | Reputational damage, possible fines, possible cost of complying with ICO notices/audits.  University information may be used for unauthorised purposes, disclosed inappropriately, corrupted, made unavailable or lost.  Potential loss of intellectual property.  Potential disruption to operations. |
| RISK 003 - Access to Office 365 content by UK authorities |
| RISK 004 - Access to Office 365 content by foreign authorities |
| RISK 005 - Unauthorised access to Office 365 content by third parties |
| RISK 006 – ‘External’ communications may be intercepted in transit | Personal communications may be recorded, used for unauthorised purposes, disclosed, corrupted or blocked. | Organisation might be in breach of *Data Protection Act 1998* principle 7 *GDPR* article 24. | Reputational damage, possible fines, possible cost of complying with ICO notices/audits.  University communications may be recorded, used for unauthorised purposes, disclosed, corrupted or blocked.  Potential loss of intellectual property.  Potential disruption to operations. |
| RISK 007 - ‘Internal’ communication content may be intercepted by Microsoft in transit |
| RISK 008 – ‘Internal’ communication content may be intercepted by UK authorities in transit |
| RISK 009 – ‘Internal’ communication content may be intercepted by foreign authorities in transit |
| RISK 010 – ‘Internal’ communication content may be intercepted by third parties in transit |
| RISK 011 - Gathering of metadata on communications by Microsoft | Party may build up a detailed picture of an individual’s activities and contacts. | Organisation might be in breach of *Data Protection Act 1998* principle 7 *GDPR* article 24. | Reputational damage, possible fines, possible cost of complying with ICO notices/audits. |
| RISK 012 - Gathering of metadata on communications by UK authorities |
| RISK 013 - Gathering of metadata on communications by foreign authorities |
| RISK 014 - Gathering of metadata on communications by third parties |
| RISK 015 - Data may be accidentally disclosed, lost or corrupted | Personal, sensitive or confidential information held in emails, contacts, tasks, calendar or notes may be shared inappropriately, corrupted or lost. | Organisation might be in breach of *Data Protection Act 1998* principle 7 *GDPR* article 24. | Reputational damage, possible fines, possible cost of complying with ICO notices/audits.  University information may be used for unauthorised purposes, disclosed inappropriately, corrupted, made unavailable or lost.  Potential loss of intellectual property.  Potential disruption to operations. |
| RISK 016 - Search facilities may be inadequate to fulfil Subject Access and/or FoI Requests |  | Unable to fulfil requests under *DPA/GDPR*, FoI or lawful requests from law enforcement. | Reputational damage, possible fines, possible cost of complying with ICO notices/audits, cost of implementing alternative approaches. |
| RISK 017 - Presence information gathered by Office 365 may be used for unauthorised purposes | Information on location, working patterns etc. may be gathered and used inappropriately. | Organisation might be in breach of *Data Protection Act 1998* principle 2 *GDPR* article 5. | Reputational damage, possible fines, possible cost of complying with ICO notices/audits, staff may decline to use the facility. |
| RISK 018 - Documents containing personal information may be inappropriately shared outside the University accidentally | Personal, sensitive or confidential information, messages and documents may be disclosed inappropriately. | Organisation might be in breach of *Data Protection Act 1998* principle 7 *GDPR* article 24. | Reputational damage, possible fines, possible cost of complying with ICO notices/audits.  Potential loss of intellectual property. |
| RISK 019 - Personal data might be retained longer than necessary | Personal information may be retained longer than necessary. | Organisation might be in breach of *Data Protection Act 1998* principle 5 *GDPR* article 5, 17. | Reputational damage, possible fines, possible cost of complying with ICO notices/audits. |
| RISK 020 – Existing policies may not be adequate | Individuals may not follow the appropriate procedures or take appropriate precautions when using Office 365, meaning that personal, sensitive or confidential information messages and documents may be disclosed inappropriately or that full advantage of Office 365 cannot be taken. | Organisation might be in breach of *Data Protection Act 1998* principle 7 (The “appropriate organisational measures” mentioned in the Act includes having relevant policies), *GDPR* article 24. | Reputational damage, possible fines, possible cost of complying with ICO notices/audits.  Organisation may not see the full benefit of deploying Office 365 because staff are not permitted to use it fully. |
| RISK 021 – Personal Information might be inappropriately disclosed through the external directory service | Personal, sensitive or confidential information held in Azure Active Directory may be shared inappropriately. | Organisation might be in breach of *Data Protection Act 1998* principle 7 *GDPR* article 24. | Reputational damage, possible fines, possible cost of complying with ICO notices/audits.  University information may be used for unauthorised purposes, disclosed inappropriately, corrupted, made unavailable or lost. |
| RISK 022 – The introduction of new Office 365 components and integrated apps could lead to the inappropriate sharing of personal data | Personal, sensitive or confidential information held in emails, contacts, tasks, calendar or notes may be shared inappropriately, corrupted or lost.  Personal data contained in emails, calendar, contacts, documents etc. may not be protected by acceptable data protection legislation. | Organisation might be in breach of *Data Protection Act 1998* principle 7 *GDPR* article 24.  Organisation might be in breach of *Data Protection Act 1998* principle 8 *GDPR* articles 45, 46, 49. | Reputational damage, possible fines, possible cost of complying with ICO notices/audits.  University information may be used for unauthorised purposes or disclosed inappropriately. |
| RISK 023 – The use of Microsoft Forms could lead people to supply personal information without understanding how it is processed | Personal information may be processed in a manner that differs from the respondents’ expectations. | Organisation might be in breach of *Data Protection Act 1998* principle 2, 8, *GDPR* article 5, 45,46,49 . | Reputational damage, possible fines, possible cost of complying with ICO notices/audits. |
| RISK 024 - Failure to meet confidentiality requirements of research grants |  |  | Loss of research contracts / income, reputational damage. |

Table 2 - Impact of privacy risks

# Step Four – Identify privacy solutions

This step involves examining each of the risks identified in Step Three and identifying solutions that will bring the residual risk to a level where the University can accept it.

In some cases, these solutions are inherent in Office 365, and no further actions are required. In other cases, further action will be required and these will need to be integrated back into the project plan (see Step Six).

To avoid repetition, the information for Steps Four and Five have been consolidated into “Table 3 - Risks, solutions, and acceptance”. Columns one two three and four of this table record the outcomes of Step Four. For convenience in Step Six, column three records whether there are any actions required to implement the solutions identified.

# Step Five – Sign off and record the PIA outcomes

Whether the solution to a privacy risk involves taking additional action or not, the University needs to formally consider the risk and the proposed solution, and satisfy itself that the residual risk had indeed been reduced to an acceptable level.

Step Five records the formal acceptance of the residual risks by appropriate people on behalf of the University.

Column five of “Table 3 Risks, solutions, and acceptance” records the outcomes of Step Five.

Table 3 - Risks, solutions, and acceptance

| Risk ID and Title | Solution(s) | Action required | Result: Is risk eliminated, reduced or accepted? | Approved by |
| --- | --- | --- | --- | --- |
| RISK 001 - Personal data handled outside EEA | For applications other than Yammer, Forms and Sway, data will be stored and processed within the EEA, other than temporary processing for exceptional technical purposes.  This exceptional processing:   * Can only be instigated in response to an issue formally logged by the University; * Involves Microsoft engineers in the USA remotely accessing University data for the purposes of resolving the issue; * May involve these engineers temporarily copying data to other servers in the same data centre (still in the EEA); * Does not involve the data being stored at rest outside the EEA at any point; * Requires specific authorisation for each occasion; * Is subject to an audit trail; and * Is subject to secure processes for data destruction of any temporary copies of the data in the EEA once the issue is resolved.   Microsoft has incorporated EU Data Protection Model clauses into the agreement with the University, and is a signatory to the Privacy Shield Framework. This means that the use of Office 365 is compatible with *DPA* Principle 8 and *GDPR* article 46. The Office 365 service is certified to ISO 27001 (Information Security Management Systems) and ISO 27018 (Cloud processing of personal data). The results of the regular independent audits of Microsoft’s compliance with these standards are available to the University. | None for EEA hosted applications  Turn off Yammer and Sway. (See RISK 0023 for Forms)  Keep hosting location for Office 365 applications under review[[11]](#footnote-11). | The risk is reduced to a level where it is accepted, and eliminated for Yammer and Sway. | CIO and DPO |
| RISK 002 - Unauthorised access to Office 365 content by Microsoft | Microsoft are contractually bound to use the data only to provide the Office 365 service, and for no other purpose other than lawful requests from government agencies (the latter are covered by other identified risks). Data access by Microsoft is restricted to very specific circumstances and is subject to an audit trail. | None | The risk is reduced to a level where it is accepted. | CIO and DPO |
| RISK 003 - Access to Office 365 content by UK authorities  and  RISK 004 - Access to Office 365 content by foreign authorities | Microsoft will attempt to direct all lawful requests for data from government authorities to the customer, or failing that to inform the customer that such requests have been made. This is part of Microsoft’s Privacy statement, a part of the Office 365 contract.  Microsoft regularly publishes figures on the total numbers of government requests[[12]](#footnote-12) although this does not distinguish between corporate and consumer accounts[[13]](#footnote-13).  The on-site systems would be subject to the same potential lawful requests, and although the organisation would be aware of the requests, the individual might not be made aware of any such requests or resulting disclosures. However, the involvement of the University in processing the request could help avoid misunderstandings arising from the nature of the material involved in certain research areas.  For cases where the offsite storage of email would not be acceptable, the University should consider a hybrid Exchange solution. This allows nominated users’ email, to be stored on-site, while retaining the full functionality of Office 365. Anyone requiring their mailbox to be located on premise could request this but they would still need to be aware that any email messages sent to collaborators who do not have mailboxes on the University on premise installation of Microsoft Exchange could mean that the data goes outside of the EEA. The University should also investigate a ‘bring your own key[[14]](#footnote-14)’ approach that would negate Microsoft’s ability to access any customer data (though with implications for cost, functionality and support). | Issue a policy statement prohibiting the storage on Office 365 of particularly sensitive material.  Consider implementing a hybrid Exchange solution allowing the on-site storage of some mailboxes, or a ‘bring your own key’ approach.  Continue to provide onsite data storage facilities. | The risk is reduced to a level where it is accepted. | CIO and DPO |
| RISK 005 - Unauthorised access to Office 365 content by third parties | Microsoft have implemented a multi layered approach to security complying with ISO 27001 and ISO 27018. Their compliance with these standards is independently audited at least annually. The results of these audits are available to customers[[15]](#footnote-15). The likelihood of unauthorised access to Office 365 content by virtue of a compromise of Microsoft’s security is very small compared with the likelihood of unauthorised access by virtue of a compromise at the client end (for example, weak or shared passwords, PCs left logged in and unattended, PCs infected with malware, loss of mobile devices), and is almost certainly less than the likelihood of a breach of the security of the University’s servers and network. | Periodically review the independent audit of Microsoft data centre security. | The risk is reduced to a level where it is accepted. | CIO and DPO |
| RISK 006 – ‘External’ communications may be intercepted in transit | In the case of email, there is a significant risk of confidential information being accessed in transit or after receipt depending on the security of the networks, servers and clients once the message leaves Office 365. However, this is no different than the situation with an on-site email system. The University’s existing policy cautions against sending high risk personal data or sensitive information to external users by email. | None | The risk is no different to that currently accepted. | CIO and DPO |
| RISK 007 - ‘Internal’ communication content may be intercepted by Microsoft in transit | Microsoft are contractually bound to use the data only to provide the Office 365 service, and for no other purpose other than lawful requests from government agencies (the latter are covered by other identified risks). Data access by Microsoft is restricted to very specific circumstances and is subject to an audit trail. | None | The risk is reduced to a level where it is accepted. | CIO and DPO |
| RISK 008 – ‘Internal’ communication content may be intercepted by UK authorities in transit  RISK 009 – ‘Internal’ communication content may be intercepted by foreign authorities in transit  RISK 010 – ‘Internal’ communication content may be intercepted by third parties in transit | Email in transit between two University users, both on the University network, is nevertheless routed through the Microsoft servers.  However, it can be strongly encrypted.  Microsoft have a direct connection to Janet, so the only networks involved in the exchange are the University network, Janet and the Microsoft network. If either the sender or recipient are off the University network, this would be covered by RISK 006 even if one or both are University users. | Enforce the use of strong encryption between email clients and the Office 365 mail service. | The risk is reduced to a level where it is accepted. | CIO and DPO |
| RISK 011 - Gathering of metadata on communications by Microsoft | Microsoft are contractually bound to use the customer data, including metadata, to provide the Office 365 service, and for no other purpose other than lawful requests from government agencies (the latter are covered by RISK 012 and RISK 013). | None | The risk is reduced to a level where it is accepted. | CIO and DPO |
| RISK 012 - Gathering of metadata on communications by UK authorities  RISK 013 - Gathering of metadata on communications by foreign authorities | Communications between Office 365 clients and the Office 365 server are encrypted by SSL / TLS. Therefore, the only metadata that can be collected indicates that a client communicated with Office 365. No information about the recipient, subject etc. can be gathered at this stage. Microsoft have a direct connection to Janet, so for on-campus users the only networks involved are the University network, Janet and Microsoft’s network. For users off campus, the risk is no different to that for the use of the current systems.  Metadata about emails (typically the message subject, sender’s and recipient’s email addresses, date and time message was sent and arrived etc.) will be held on the Microsoft mail servers and the recipients’ mail servers. See also the assessment for RISK 003.  Communication using Skype for Business is all encrypted using SSL/TLS, and if the communication is between two internal users, it does not leave the home network (although initial call set-up is performed via the Office 365 servers). Even for external communication, the metadata captured would reveal only that a connection took place, and very little about the nature of the communication.  The recorded metadata is subject to lawful requests for access from UK authorities (as is email sent using the University’s internal systems). The only difference is that for internal communications, the request would necessarily have to be processed by University staff when University systems are used, whereas if Office 365 is used, the processing of the request could in theory not involve any University staff. | None | The risk is reduced to a level where it is accepted. | CIO and DPO |
| RISK 014 - Gathering of metadata on communications by third parties | Communications between Office 365 clients and the Office 365 server is encrypted by SSL / TLS. Therefore, the only metadata that can be collected indicates that a client communicated with Office 365. No information about the recipient, subject etc. can be gathered at this stage. Microsoft have a direct connection to Janet, so for on-campus users the only networks involved are the University network, Janet and Microsoft’s network. For users off campus, the risk is no different to that for the use of the current systems.  Metadata about emails (typically the message subject, sender’s and recipient’s email addresses, date and time message was sent and arrived etc.) will be held on the Microsoft mail servers and the recipients’ mail servers. See also the assessment for RISK 003.  Communication using Skype for Business is all encrypted using SSL/TLS, and if the communication is between two internal users, it does not leave the home network (although initial call set-up is performed via the Office 365 servers). Even for external communication, the metadata captured would reveal only that a connection took place, and very little about the nature of the communication. | None | The risk is reduced to a level where it is accepted. | CIO and DPO |
| RISK 015 - Data may be accidentally disclosed, lost or corrupted | Microsoft have implemented a multi layered approach to security complying with ISO 27001. Their compliance with this standard is independently audited at least annually. The results of these audits are available to customers, see RISK 005. The likelihood of unauthorised access to Office 365 content by virtue of a compromise of Microsoft’s security is very small compared with the likelihood of unauthorised access by virtue of a compromise at the client end.  The data held in Office 365 is replicated across two datacentres in seismically and politically stable locations. Data is replicated across redundant servers in each datacentre, and backed up regularly. More information about service continuity is available at <https://products.office.com/en-us/business/office-365-trust-center-welcome> . A discrete, immutable backup regime would provide additional protection against corruption caused by virus, user edits or ransomware. | Regularly review whether a discrete, immutable backup regime is required. | The risk is reduced to a level where it is less than is currently accepted. | CIO and DPO |
| RISK 016 - Search facilities may be inadequate to fulfil Subject Access and/or FoI Requests | Search facilities to allow Data Protection subject access requests are available in Office 365. Information in Skype for Business instant messages are sent to the participants’ mailboxes, so would be discovered in the Office 365 search.  As with the current email system, the search facility does not extend to ‘archived’ data held in PST files on users’ computers, but these can be imported to Office 365. | Encourage the import of existing PST files to Office 365. | The risk is reduced to or below the levels currently accepted. | CIO and DPO |
| RISK 017 - Presence information gathered by Office 365 may be used for unauthorised purposes | Office 365 does not keep historical data on users’ presence – only their current status. There is therefore no risk of Office 365 presence information being gathered, unless someone develops software to continually poll and record users’ presence status. Of course, someone intent on doing this could just as easily find other ways to harvest activity information so the move to Office 365 has no bearing on this risk. | None | The risk is eliminated. | CIO and DPO |
| RISK 018 - Documents containing personal information may be inappropriately shared outside the University accidentally | OneDrive for Business allows users to share documents outside the University. SharePoint Online provides facilities to easily publish team web sites, including documents and lists. This may be set up in a way that allows end users to control the visibility of content, documents and lists outside the University. Users should be made aware of the importance of considering data protection principles and confidentiality, and applying appropriate access controls to this type of information. Of course, the same considerations also apply to other types of web publishing, social media, cloud storage and even attachment of documents to emails.  Staff are known to be currently using DropBox and Google Drive for storage and collaboration purposes. The adoption of OneDrive for Business and SharePoint Online would allow these alternative facilities to be superseded.  Rights Management features available in Office 365 as part of Azure Information Protection[[16]](#footnote-16) allow policy based restrictions to be placed on certain categories of document. For example, users might be able to share documents categorised as highly confidential outside the University, and the recipients would be able to read them, but the recipients would not be able to forward, save or print them. This would require categories of confidentiality to be defined and applied to all documents and information in Office 365, together with protection levels for each category.  Data Loss Protection is a related technology available within Office 365 that automatically categorises information based on recognising ‘patterns’ of sensitive information such as payment card numbers, National Insurance numbers, bank account numbers and sort codes etc. | Issue reminders about security and privacy considerations when using collaboration features in Office 365.  Emphasise the risks associated with attachments, e.g. it is easy to send attachments to the wrong person.  Consider enhancing information security by introducing Rights Management and Data Loss Prevention (DLP) | The risk is reduced to the level where it is accepted. | CIO and DPO |
| RISK 019 - Personal data might be retained longer than necessary | Exchange Online and SharePoint Online provide facilities to apply document retention policies for stored information. The defaults are as follows:  • Individual mailboxes are permanently deleted 30 days after the corresponding user account is suspended; and  • Deleted’ documents remain in the ‘Recycle bin’ for 30 days and are then deleted permanently.  The mailbox recovery settings are effectively the same as used currently. Current file recovery (from the F: drive) allows files to be recovered up to 30 days after they are deleted. | None | The risk is reduced to a level where it is accepted. | CIO and DPO |
| RISK 020 – Existing policies may not be adequate | A review of existing policies should be undertaken to identify the policies that require updating, and appropriate changes incorporated to take account of the implementation of Office 365. | Review and modify existing policies. | The risk is eliminated. | CIO and DPO |
| RISK 021 – Personal Information might be inappropriately disclosed through the external directory service | Azure Active Directory can be configured by the University both in terms of the nature of information about individuals that is held, and in terms of the ability of various types of user to gain access to the information – this includes access restrictions that can be placed on users from outside the University’s domain. The personal information held in Azure is already kept at a minimum necessary for Office 365 to function, but will include such items as name, department, email address etc. The inherent security of Azure Active Directory infrastructure is the same as for Office 365, i.e. it is governed by a security management system certified to ISO 27001 etc.  The University should review what personal information is held in Azure Active Directory to ensure that it is no more than necessary and what access controls are configured to prevent unauthorised access. | Review the necessity of personal information held in and the access controls of Azure Active Directory. | The risk is reduced to a level where it is accepted. | CIO and DPO |
| RISK 022 – The introduction of new Office 365 components and integrated apps could lead to inappropriate sharing of personal data | Microsoft would generally review the security and privacy aspects of any new components and integrated apps before releasing them to the Office 365 community. However, the University should take a more proactive approach than this. The availability of new integrated apps in Office 365 to general users should be disabled, and the University should closely monitor the relevant Microsoft channels for information about the release of new components. | Disable access in Office 365 to new integrated apps for general users and closely monitor the release of new Office 365 components. | The risk is reduced to a level where it is accepted. | CIO and DPO |
| RISK 023 – The use of Microsoft Forms could lead people to supply personal information without understanding how it is processed | The University already makes widespread use of externally hosted survey software, including Bristol Online Surveys and Survey Monkey (which stores data on servers in the USA). The use of Microsoft forms would not be fundamentally different. A Fair Processing Notice on each survey should alert participants to the service being used, and where their information is being processed.  Forms (and indeed Survey Monkey) should not be used to gather sensitive personal data.  The DPO should consider reviewing policy, training, support and guidance around online surveys in the light of *GDPR.* | Issue reminders about Fair Processing Notices.  Prohibit use of Forms for gathering sensitive data.  Consider reviewing use of online surveys. | The risk is reduced to a level where it is accepted. | CIO and DPO |
| RISK 024 - Failure to meet confidentiality requirements of research grants | If mandated by the grant confidentiality requirements, those involved should arrange with IT Services to provide / use dedicated storage for the information and communication related to the work. | Issue reminders of the need to comply with contract conditions. | The risk is reduced to a level where it is accepted. | PVC Research |

Table 3 - Risks, solutions, and acceptance

# Step Six – Integrate the outcomes into the project plan

The agreed actions need to be built into the project plan. This involves identifying a date by which they will be completed, and the name of the individual responsible for their completion.

Table 4 - Action Plan, records the outcomes of Step Six. Note that those privacy risks for which no actions are required are omitted from this table.

Table 4 - Action Plan

| Risk ID and Title | Action required | Date for completion | Responsibility for Action |
| --- | --- | --- | --- |
| RISK 001 - Personal data handled outside EEA | Turn off Yammer and Sway. | May 2018 | Office 365 project team |
| Keep hosting location for Office 365 applications under review[[17]](#footnote-17). | Ongoing | IT Services - operations |
| RISK 003 - Access to Office 365 content by UK authorities  RISK 004 - Access to Office 365 content by foreign authorities | Issue a policy statement prohibiting the storage on Office 365 of particularly sensitive material. | September 2018 | Governance office |
| Consider implementing a hybrid Exchange solution allowing the on-site storage of some mailboxes, or a ‘bring your own key’ approach. | January 2018 | Office 365 project team |
| Continue to provide onsite data storage facilities. | Ongoing | IT Services - operations |
| RISK 005 - Unauthorised access to Office 365 content by third parties | Periodically review the independent audit of Microsoft data centre security. | Ongoing | DPO and CIO |
| RISK 008 – ‘Internal’ communication content may be intercepted by UK authorities in transit  RISK 009 – ‘Internal’ communication content may be intercepted by foreign authorities in transit  RISK 010 – ‘Internal’ communication content may be intercepted by third parties in transit | Enforce the use of strong encryption between email clients and the Office 365 mail service. | July 2017 | IT Services - Infrastructure |
| RISK 015 - Data may be accidentally disclosed, lost or corrupted | Regularly review whether a discrete, immutable backup regime is required. | Ongoing | CIO and IT Services |
| RISK 016 - Search facilities may be inadequate to fulfil Subject Access Requests | Encourage the import of existing PST files to Office 365. | September 2018 | IT Services – customer services |
| RISK 018 - Documents containing personal information may be inappropriately shared outside the University accidentally | Issue reminders about security and privacy considerations when using collaboration features in Office 365. Emphasise the risks associated with attachments, e.g. it is easy to send attachments to the wrong person. | September 2018 | IT Services – customer services |
| Consider enhancing information security by introducing Rights Management and Data Loss Prevention (DLP) | February 2018 | CIO, DPO and Governance Office |
| RISK 020 – Existing policies may not be adequate | Review and modify existing policies. | July 2017 | Governance office, DPO and Office 365 project team |
| RISK 021 – Personal Information might be inappropriately disclosed through the external directory service | Review the necessity of personal information held in and the access controls of Azure Active Directory. | July 2017 | IT Services - infrastructure |
| RISK 022 – The introduction of new Office 365 components and integrated apps could lead to the inappropriate sharing of personal data | Disable access in Office 365 to new integrated apps for general users, and closely monitor the release of new Office 365 components. | July 2018 | Office 365 project team |
| RISK 023 – The use of Microsoft Forms could lead people to supply personal information without understanding how it is processed | Issue reminders about Fair Processing Notices for all surveys. | July 2017 | DPO |
| Prohibit use of Forms for surveys gathering sensitive personal data. | July 2017 | Governance office |
| Consider reviewing policy, training, support and guidance on the use of online surveys in the light of *GDPR.* | November 2017 | DPO, PVC Research and Governance office |
| RISK 024 - Failure to meet confidentiality requirements of research grants | Issue reminders of the need to comply with contract conditions. | July 2017 | PVC Research and Finance Director |
| Consultation process | Publish PIA as part of the project communications, and link to it from the Service Catalogue. Bring the results of the Office 365 Privacy Impact Assessment to the attention of all the project consultative groups. | June 2017 | Office 365 project manager |

Table 4 - Action Plan

# Consultation

The conduct of this Privacy Impact Assessment has involved the following consultation:

Individual discussions with:

* Data Protection Officer;
* Registrar and Secretary;
* Chair of the Research Ethics committee;
* Legal advisor (information and compliance);
* PVC Research;
* Finance Director;
* HR Director;
* CIO; and
* Chief Information Security Officer.

Group discussions with:

* Office 365 project team;
* IT Strategy Committee;
* IT Committee of the Faculty of Science and Technology;
* IT Infrastructure team;
* Faculty registrars group;
* Executive group of the Students Union; and
* Staff consultative group.

Copies of the outcome of the PIA will go to:

* All the individuals and groups who participated in the assessment;
* The Office 365 project website; and
* The Data Protection Officer’s PIA website.

# Annexe – Further information on Office 365 components

This PIA is not able to go into depth about all the features and capabilities of Office 365 and the applications available.

The following table gives URLs for more information on each of the Office 365 components available in the Education plan at the time of writing.

|  |  |
| --- | --- |
| Element | More Information |
| Office 365 | <https://products.office.com/en-gb/academic/compare-office-365-education-plans> |
| Exchange Online | <https://products.office.com/en-gb/exchange/exchange-online> |
| SharePoint Online | <https://products.office.com/en-us/sharepoint/sharepoint-online-collaboration-software> |
| OneDrive for Business | <https://products.office.com/en-gb/onedrive-for-business/online-cloud-storage> |
| Online Office Applications | <https://products.office.com/en-gb/office-online/documents-spreadsheets-presentations-office-online> and  <https://products.office.com/en-gb/business/office-365-mobile-apps-for-business> |
| Skype for Business | <https://products.office.com/en-gb/business/office-365-video-conferencing> |
| Video | <https://products.office.com/en-gb/business/explore-office-365-video> |
| Yammer | <https://products.office.com/en-gb/yammer/yammer-overview> |
| Sway | <https://sway.com> |
| Delve | <https://products.office.com/en-gb/business/explore-office-delve> |
| Flow | <https://flow.microsoft.com> |
| Forms | <https://forms.office.com/> |
| Planner | <https://products.office.com/en-gb/business/office-365-planner> |
| Project | <https://products.office.com/en-gb/project/project-online-premium> |
| PowerApps | <https://powerapps.microsoft.com> |
| Dynamics 365 | <https://www.microsoft.com/en-us/dynamics365> |

# Acknowledgements

**Lead author**

Jerry Niman, Jerry Niman IT Services

Anna Mathews, UCISA Head of Policy and Projects was the project manager for this publication. We are grateful to the following people for their helpful comments in the preparation of this document:

Victoria Cetinkaya, Senior Policy Officer (Public Services), Information Commissioner’s Office

Stuart Aston, National Security Officer, Microsoft UK

# Copyright, disclaimer and availability

**Copyright**

This publication is licensed under the Creative Commons Attribution-NonCommercial 4.0 International licence. Subject to the source being appropriately acknowledged and the licence terms preserved, it may be copied in whole or in part

and incorporated into another document or shared as part of information given, except for use for commercial gain.

The publication also contains resources from institutions; where this material is copied or otherwise reused, both UCISA and the institution concerned should be acknowledged.

**Disclaimer**

The information contained herein is believed to be correct at the time of issue, but no liability can be accepted for any inaccuracies. The reader is reminded that changes may have taken place since issue, particularly in rapidly changing areas, such as internet addressing, and consequently URLs and email addresses should be used with caution. UCISA cannot accept any responsibility for any loss or damage resulting from the use of the material contained herein.

**Availability**

The UCISA Privacy Impact Assessment Toolkit and the UCISA Privacy Impact Assessment – Worked example for Office 365 is freely available to download for non-commercial use from [www.ucisa.ac.uk](http://www.ucisa.ac.uk)

1. [www.ucisa.ac.uk/PIAToolkit](http://www.ucisa.ac.uk/PIAToolkit) [↑](#footnote-ref-1)
2. [www.ucisa.ac.uk/PIAToolkit](http://www.ucisa.ac.uk/PIAToolkit) [↑](#footnote-ref-2)
3. <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf> [↑](#footnote-ref-3)
4. For simplicity, from now on “students” will be taken to mean undergraduate and taught Master’s students [↑](#footnote-ref-4)
5. For simplicity, from now on “staff” will be taken to include research Master’s and postgraduate students [↑](#footnote-ref-5)
6. Except for Yammer, Forms and Sway data, which are hosted on servers in US datacentres [↑](#footnote-ref-6)
7. Information Security Management [↑](#footnote-ref-7)
8. Protection of personally identifiable information (PII) in public clouds [↑](#footnote-ref-8)
9. <https://www.privacyshield.gov/welcome> [↑](#footnote-ref-9)
10. <http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment> [↑](#footnote-ref-10)
11. See datacentre map at <http://o365datacentermap.azurewebsites.net/> [↑](#footnote-ref-11)
12. See <https://www.microsoft.com/about/csr/transparencyhub/lerr/> [↑](#footnote-ref-12)
13. Microsoft has a strong interest in safeguarding the privacy of its clients’ data and has demonstrated a willingness to fight warrants it considers to be unjustified. In July 2016, Microsoft successfully challenged a warrant for customer emails stored in their Irish datacentre, setting an important precedent. See <https://digitalconstitution.com/> [↑](#footnote-ref-13)
14. See <https://docs.microsoft.com/en-us/information-protection/plan-design/plan-implement-tenant-key> [↑](#footnote-ref-14)
15. See <https://servicetrust.microsoft.com/Documents/ComplianceReports> under the ISO reports tab. [↑](#footnote-ref-15)
16. See <https://www.microsoft.com/en-gb/cloud-platform/azure-information-protection-features> [↑](#footnote-ref-16)
17. See datacentre map at <http://o365datacentermap.azurewebsites.net/> [↑](#footnote-ref-17)