University of Essex

University of Essex
Office 365 Privacy Impact Assessment

Step one: Identify the need for a PIA

The University of Essex currently uses Microsoft Office 365 to provide email and collaboration facilities for students.

Office 365 is a 'hosted' version of Exchange, and is provided by Microsoft to its UK Higher Education customers from its datacentres in Dublin and Amsterdam.

The Office 365 platform also offers a solid foundation for other developments including new approaches to file storage and sharing, integration with voice communication, video conferencing, instant messaging and presence management.

The University currently provides some of these facilities to staff using an on-site Exchange installation. It is considering migration this provision to Office 365, and this document assesses the impact of this proposal on the privacy of staff.

A PIA is needed because the project involves the processing of staff emails, calendar information, contact lists, tasks and notes in the Microsoft cloud. These are located within the European Economic Area (EEA), but the data may temporarily be processed outside the EEA. Microsoft has signed a 'safe harbour' agreement and has written the EU Data Protection model clauses into its agreement with the University. Furthermore, the University guidance has always been that no confidential information should be sent by electronic means unless it is encrypted. Nevertheless, the adoption by staff of Office 365 will inevitably mean that personal data may be processed by Microsoft on the University's behalf.

A 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[1].

Who is Affected?

Although this document has said that students are already using Office 365 and the University is considering the migration of Staff to Office 365, this is an oversimplification.

Current users of Office 365 include:

- Undergraduate Students;
- Taught postgraduate students;
- A small number of research postgraduate students.

The people under consideration for the migration to Office 365 include:

- Staff;
- The majority of research postgraduate students;
- Those individuals to whom the University has given an email account but who are neither students nor staff. This would include Students Union officials, Emeritus Professors etc.

This is not felt to affect the outcome of this PIA, and for brevity it will continue to refer to students and staff.

What is Affected?

The facilities included in this assessment include:

- Email (*including Calendars, Contacts, Tasks & Notes)*;
- SharePoint Online (in particular OneDrive, Team Sites, lists and workflow);

[1] http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment

- Lync online (instant messaging, persistent chat rooms, voice and video conferencing, presence management but not telephony integration);
- Yammer (organisational social networking).

The University is currently only considering the use of Office365 for email. Nevertheless, it was felt worthwhile considering the other facilities in the PIA as deploying these in future will be investigated in due course.

Step two: Describe the information flows

Email, Calendar etc

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, reply to, 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 generally within 100 days 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 they have been successfully forwarded) by the relaying mail servers between the sender and recipients. These relaying mail servers will also keep 'metadata' about the email, typically the sender, recipient(s), date & time and subject, for a period determined by local legislation and/or practice. Once delivered, the email is stored in the recipients' mailboxes until deletion.

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 this would be against University guidance. For example, external users sending confidential information by email *to* the University need not be aware of the University guidance, and may have sent confidential information unencrypted. A copy of this would remain in the recipient's mailbox until deleted. Calendar information, tasks and notes are mostly exchanged between internal University recipients, and could contain sensitive information. An exception to this would be a calendar appointment or invitation sent to a third party, and this would be handled in a very similar way to email, and has the same potential to contain sensitive information.

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

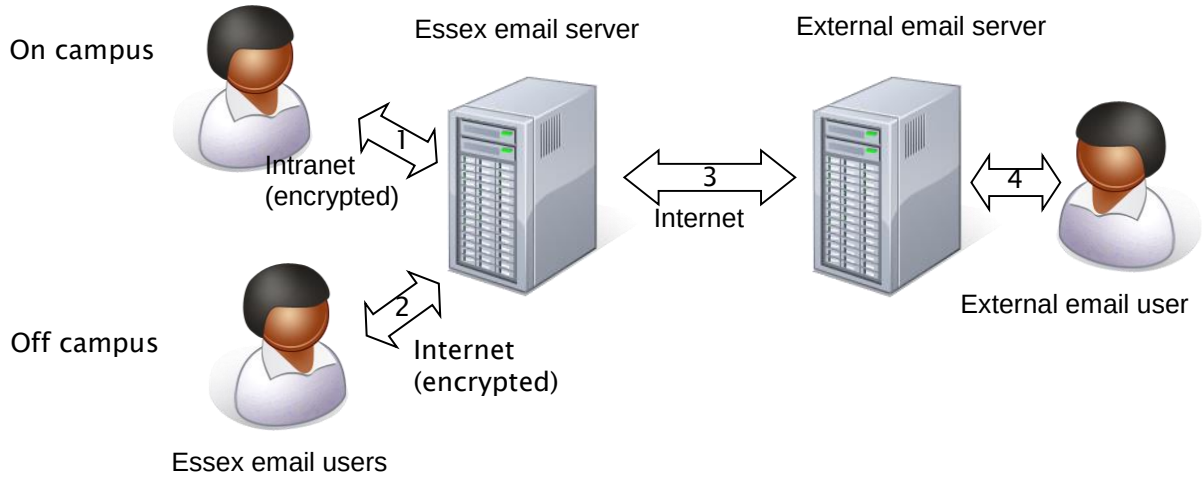

Figure 1 Current Email System

The content of emails is stored on the Essex mail server and on the correspondent's mail server.

The encrypted content of emails traverses the Essex internal network (1) from on-campus users to the mail server. If the user is off campus, it must traverse the internet, but this is in an encrypted form (2). If the correspondent is external and their mail server does not support encryption, it will traverse the internet unencrypted between the Essex mail server and the external mail server (3). How the email then traverses between the external mail server and the recipient (4) is beyond Essex'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, this is handled entirely by the Essex email service, and the data never leaves the University.

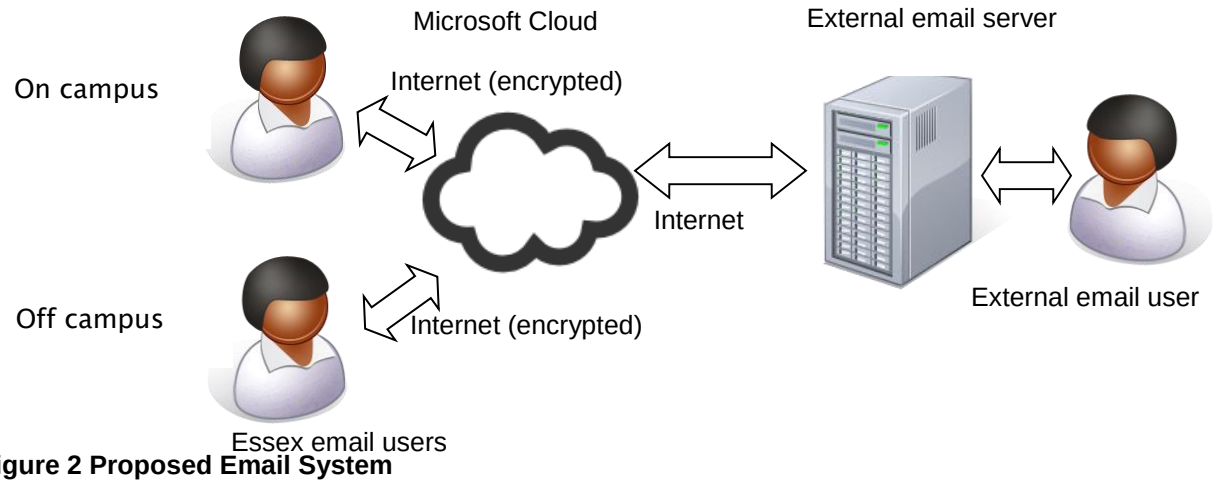

Figure 2 Proposed Email System

With the proposed email system, all email is stored on the Microsoft Cloud, and traverses the internet even if the sender and receiver are both internal, however this is in an encrypted form.

Email being sent to or received from the email servers used by external correspondents traverses the internet in exactly the same way as it currently does.

Emails that have been sent or received may also be cached on local devices (for example on a mobile device or in Outlook on a PC). Here, they are only as secure as the device itself. However, this is the same as for the current system and so does not introduce any additional risk.

SharePoint Online

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

- Individual and group document storage;
- Internal & external websites;
- Forms & workflows.

Access to the information held in SharePoint online is generally via a web browser, mobile app or other Office 365 aware application such as Office 2010 and later. In all cases, access is over the internet using 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.

Lync Online

Lync Online provides communication facilities including:

- Audio conferencing;
- Video conferencing;
- Instant messaging;
- Persistent chat;
- Presence management.

The on-site Lync product also provides telephony integration, but this is not currently available in the Lync Online offering.

All communications through Lync are encrypted in transit, and the content of persistent chat is stored in an encrypted form on the Microsoft servers. External users can be invited to take part in Lync conversations, but the communications are still encrypted.

Presence information (i.e. whether a user is busy, available, away from desk etc) is gathered by Lync from 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.

Yammer

Yammer is an enterprise social network tool, and is available free to Universities as part of the Office 365 suite. The particular communications channels it offers are very similar (from a privacy perspective) to those offered by other elements of Office 365, in particular email and persistent chat.

Significant Differences

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

- Users' mailboxes containing sent and received emails and their attachments will be stored on Microsoft's servers rather than on Essex's;
- Calendar information, contact lists, notes, tasks and any attachments will be stored on Microsoft's servers rather than on Essex'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 Essex and Microsoft's servers, although this will be encrypted;
- Cross-mailbox search facilities are those provided by Microsoft rather than those provided by the current on-site staff email system;
- SharePoint offers the potential for documents to be shared outside the University under the control of individual users;
- Lync 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;
- Yammer creates the potential for sharing documents outside of the University by connecting with external networks;
- Data retention involves Microsoft in addition to the University.

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 Essex's use of email, calendaring, SharePoint, Yammer, Lync etc.;
- Personal data contained in emails, calendar events, SharePoint documents and lists, Lync conversations and Yammer activity are being processed by a third party Data Processor[2] (Microsoft) on behalf of the Data Controller (Essex);
- Personal data contained in emails, calendar events, contact lists, tasks, notes, SharePoint documents & lists, Lync conversations and Yammer activity may be stored and processed temporarily by Microsoft in data centres outside the EEA in defined circumstances.

[2] The Data Controller is "a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed". The Data Processor is "any person (other than an employee of the data controller) who processes the data on behalf of the data controller". Further information is available at http://ico.org.uk/for_organisations/data_protection/the_guide/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data-controllers-and-data-processors-dp-guidance.pdf

Consultation requirements

The migration to Office 365 has the potential to introduce new privacy issues.

Even where the inherent and proposed controls are adequate, staff are likely to have concerns until the proposals and the security measures in place are explained.

It is therefore important that adequate communication and consultation takes place.

The following channels will be used:

- All staff communication emails;
- A web forum where questions and ideas can be shared amongst staff;
- Question & Answer sessions for staff to attend;
- Drop in sessions open to all staff who want to discuss the changes;
- A new role mailbox offering a single point of contact for anyone wanting to communicate with the project team;
- Video or screencasts to demonstrate new features and educate users ahead of any changes;
- Expansion of the ISS website to include frequently asked questions along with answers and signposting to the other channels listed above.

Steps three and four: Identify the privacy & related risks and Identify privacy solutions

Step 3 - Describe the risks to privacy in terms of the risks to individuals, the risks of non-compliance to legislation, regulations or standards and the risks to the organisation

Step 4 - Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Privacy Risk	**Risk to Individuals**	**Compliance Risks**	**Risk to University**	**Solution(s)**	**Result: Is risk eliminated, reduced or accepted?**
1 - Personal data handled outside EEA	Personal data contained in emails, calendar, contacts etc. may not be protected by data protection legislation	University might be in breach of Data Protection Act 1998 principle 8	Reputational damage, cost of defending prosecution, possible fines	Data will be handled within the EEA, other than temporarily for exceptional technical purposes. Microsoft has signed a safe harbour agreement, and has incorporated EU Data Protection Model clauses into the agreement with the University. Data access by Microsoft outside the EEA for technical purposes is subject to an audit trail and to processes for data destruction once the issue is resolved.	The data is always protected by Data Protection legislation, or equivalent commercial agreement. Risk eliminated.
2 - Unauthorised access to Office 365 content by Microsoft	Personal, sensitive or confidential information messages and documents may be disclosed inappropriately	University might be in breach of Data Protection Act 1998 principle 7	Reputational damage, cost of defending prosecution, possible fines	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 the risks 3 and 4). Data access by Microsoft is restricted to very specific circumstances and is subject to an audit trail. No advertising within Office 365 or analysis of University data for any purpose is permitted.	The risk is reduced to a level where it is accepted.

Privacy Risk	Risk to Individuals	Compliance Risks	Risk to University	Solution(s)	Result: Is risk eliminated, reduced or accepted?
3 - Access to Office 365 content by UK government / law enforcement agencies	Personal, sensitive or confidential information messages and documents may be disclosed inappropriately	University might be in breach of Data Protection Act 1998 principle 7	Reputational damage, cost of defending prosecution, possible fines	Microsoft will attempt to direct all lawful requests for data from law enforcement or national security agencies to the customer, or failing that to inform the customer that such requests have been made. They regularly publish statistics on such requests[3]. As of July 2013, Microsoft had never provided any government with customer data from any of their business customers for national security purposes. The on-site email 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.	The risk is reduced to a level where it is accepted.
4 - Access to Office 365 content by foreign government / law enforcement agencies	Personal, sensitive or confidential information messages and documents may be disclosed inappropriately	University might be in breach of Data Protection Act 1998 principle 7	Reputational damage, cost of defending prosecution, possible fines	Microsoft will attempt to direct all lawful requests for data from law enforcement agencies to the customer, or failing that to inform the customer that such requests have been made. They regularly publish statistics on such requests. As of July 2013, Microsoft had never provided any government with customer data from any of their business customers for national security purposes, although there is a theoretical possibility that under the US FISA rules they could be required to do so, without notifying the customer.	The risk is reduced to a level where it is accepted.

[3] http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/ and http://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/02/03/providing-additional-transparency-on-us-government-requests-for-customer-data.aspx

Privacy Risk	Risk to Individuals	Compliance Risks	Risk to University	Solution(s)	Result: Is risk eliminated, reduced or accepted?
5 - Unauthorised access to Office 365 content by third parties	Personal, sensitive or confidential information messages and documents may be disclosed inappropriately	University might be in breach of Data Protection Act 1998 principle 7	Reputational damage, cost of defending prosecution, possible fines	Microsoft have implemented a multi layered security approach to security complying with ISO 27001. Their compliance with this standards is independently audited at least annually. The results of these audits are available to customers on request through JANET. 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). 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 risk is reduced to a level where it is accepted.
6 - Gathering of metadata on communications by Microsoft	Microsoft may build up a detailed picture of an individual's activities and contacts	University might be in breach of Data Protection Act 1998 principle 7	Reputational damage, cost of defending prosecution, possible fines	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 the risks 3 and 4).	The risk is reduced to a level where it is accepted.

Privacy Risk	Risk to Individuals	Compliance Risks	Risk to University	Solution(s)	Result: Is risk eliminated, reduced or accepted?
7 - Gathering of metadata on communications by UK government / law enforcement agencies	UK government / law enforcement agencies may build up a detailed picture of an individual's activities and contacts	University might be in breach of Data Protection Act 1998 principle 7	Reputational damage, cost of defending prosecution, possible fines	Communications between Office 365 clients and the Office 365 server is encrypted by SSL / TLS, and by the end of the calendar year 2014, Microsoft will replace all SSL encryption by Perfect Forward Security. 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. Communication between the Office 365 server and other mail servers may or may not be encrypted – this depends on the capability of the other mail server. If the other mail server does not support encryption, the message is sent in clear and metadata can be gathered which could include any information in the mail header, sender, recipients, subject, date and so forth. This applies even if the content is encrypted using PGP or SMIME, as these do not encrypt he mail header. This is the case even when an on-site email system is used. Communication using Lync is all encrypted using SSL/TLS, and if the communication is internal, it does not leave the home network.	The risk is reduced to a level where it is accepted.
8 - Gathering of metadata on communications by foreign government / law enforcement agencies	Foreign government / law enforcement agencies may build up a detailed picture of an individual's activities and contacts	University might be in breach of Data Protection Act 1998 principle 7	Reputational damage, cost of defending prosecution, possible fines	See solution to risk 7	The risk is reduced to a level where it is accepted.
9 - Gathering of metadata on communications by third parties	Third parties may build up a detailed picture of an individual's activities and contacts	University might be in breach of Data Protection Act 1998 principle 7	Reputational damage, cost of defending prosecution, possible fines	See solution to risk 7	The risk is reduced to a level where it is accepted.

Privacy Risk	Risk to Individuals	Compliance Risks	Risk to University	Solution(s)	Result: Is risk eliminated, reduced or accepted?
10 - 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	University might be in breach of Data Protection Act 1998 principle 7	Reputational damage, cost of defending prosecution, possible fines	Microsoft have implemented a multi layered security approach to security complying with ISO 27001. Their compliance with this standards is independently audited at least annually. The results of these audits are available to customers on request through JANET. 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). The data held in Office 365 is replicated across two datacentres in seismically and politically stable locations (Dublin and Amsterdam). Data is replicated across redundant servers in each datacentre, and backed up regularly. SharePoint data is backup up every 12 hours and kept for 14 days. More information about service continuity is available at http://office.microsoft.com/en-gb/business/office-365-online-service-availability-FX104028266.aspx	The risk is reduced to a level where it is accepted.
11 - Search facilities may be inadequate to fulfil Subject Access Requests		University might be unable to fulfil requests under DPA, FoI or lawful requests from law enforcement	Reputational damage, cost of defending prosecution, possible fines, cost of implementing alternative approaches.	Search facilities to allow Data Protection subject access requests are available in Office 365 and SharePoint Online. Information in Lync IM's and persistent chats are sent to the participants' mailboxes, so would be discovered in the Office 365 search. The search facilities in Office 365 are as good as those in the current email system.	The risk is eliminated.
12 - Failure to meet confidentiality requirements of research grants			Loss of research contracts / income, reputational damage	Ensure that staff do not use Office 365 for the unencrypted storage / transmission of confidential information. If mandated by the grant conditions, provide / use dedicated storage for the information and communication related to the project.	The risk is reduced to a level where it is accepted.

Privacy Risk	Risk to Individuals	Compliance Risks	Risk to University	Solution(s)	Result: Is risk eliminated, reduced or accepted?
13 - Presence information gathered by Lync may be used for unauthorised purposes	Information on location, working patterns etc may be gathered and used inappropriately	University might be in breach of Data Protection Act 1998 principle 2	Reputational damage, cost of defending prosecution, possible fines, staff may decline to use the facility	Lync does not keep historical data on users' presence – only their current status. There is therefore no risk of Lync 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.	The risk is eliminated.
14 - Documents containing personal information may be shared outside the University accidentally	Personal, sensitive or confidential information messages and documents may be disclosed inappropriately	University might be in breach of Data Protection Act 1998 principle 7	Reputational damage, cost of defending prosecution, possible fines	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.	The risk is reduced to a level where it is accepted.
15 - Personal data might be retained longer than necessary	Personal information may be retained longer than necessary	University might be in breach of Data Protection Act 1998 principle 5	Reputational damage, cost of defending prosecution, possible fines	Office 365 and SharePoint Online provide facilities to apply document retention policies for stored information. Individual mailboxes are permanently deleted 30 days after the corresponding user account is suspended. Where information relating to an individual's role within the University is likely to be required after they leave, a separate role account will be set up and the individual granted access to it in addition to their personal account. They will be advised not to use the role account for any personal information.	The risk is reduced to a level where it is accepted.

Step five: Sign off and record the PIA outcomes & Step six: Integrate the PIA outcomes back into the project plan

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork?

Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Risk	Action(s) Required to Render Risk Acceptable	Approved by	Action to be taken	Date for completion of actions	Responsibility for action
1 - Personal data handled outside EEA	Sign up to JANET *Education Solutions Office 365 Data Processing Agreement (with EU Standard Contractual Clauses) Amendment ID CTM* to keep data within EEA.	Director of Information Systems	Sign up to JANET *Education Solutions Office 365 Data Processing Agreement (with EU Standard Contractual Clauses) Amendment ID CTM* to keep data within EEA.	Complete	n/a
2 - Unauthorised access to Office 365 content by Microsoft	No action required[4]	Director of Information Systems	n/a	n/a	n/a
3 - Access to Office 365 content by UK government / law enforcement agencies	No action required	Director of Information Systems	n/a	n/a	n/a
4 - Access to Office 365 content by foreign government / law enforcement agencies	Periodically review Microsoft statistics and JANETs advice regarding latest developments.	Director of Information Systems	Review annually (last reviewed August 2014)	n/a	n/a
5 - Unauthorised access to Office 365 content by third parties	Remind users to encrypt confidential information sent electronically to external recipients	Director of Information Systems	Periodically email all University members regarding security of confidential or sensitive data	1 Nov 2014	ISS/University Records Manager
6 - Gathering of metadata on communications by Microsoft	No action required	Director of Information Systems	n/a	n/a	n/a

[4] In this table, where the action is 'No action required', please refer to 'Steps three and four - Identify the privacy & related risks and Identify privacy solutions' (above) to see how the risk has been reduced to an acceptable level without further work being required.

Risk	Action(s) Required to Render Risk Acceptable	Approved by	Action to be taken	Date for completion of actions	Responsibility for action
7 - Gathering of metadata on communications by UK government / law enforcement agencies	No action required	Director of Information Systems	n/a	n/a	n/a
8 - Gathering of metadata on communications by foreign government / law enforcement agencies	No action required	Director of Information Systems	n/a	n/a	n/a
9 - Gathering of metadata on communications by third parties	No action required	Director of Information Systems	n/a	n/a	n/a
10 - Data may be accidentally disclosed, lost or corrupted	No action required	Director of Information Systems	n/a	n/a	n/a
11 - Search facilities may be inadequate to fulfil Subject Access Requests	No action required	Director of Information Systems	n/a	n/a	n/a
12 - Failure to meet confidentiality requirements of research grants	Ensure that University members do not use Office 365 for the unencrypted storage / transmission of confidential information. If mandated by the grant conditions, provide / use dedicated storage for the information and communication related to the project.	Director of Information Systems	Ensure that University members do not use Office 365 for the unencrypted storage / transmission of confidential information.	If mandated by specific projects	ISS and REO (see also Research data management guidance)
			If mandated by research grant conditions, provide / use dedicated storage for the information and communication related to the project.	If mandated by specific projects	Principal Investigator / ISS
13 - Presence information gathered by Lync may be used for unauthorised purposes	No action required	Director of Information Systems	n/a	n/a	n/a
14 - Documents containing personal information may be shared outside the University	University members should be made aware of the importance of considering data protection	Director of Information Systems	Periodically email all University members regarding security of confidential or sensitive data.	1 Nov 2014	ISS/University Records Manager

Risk	Action(s) Required to Render Risk Acceptable	Approved by	Action to be taken	Date for completion of actions	Responsibility for action
accidentally	principles and confidentiality, and applying appropriate access controls to this type of information		Default configuration for Office365 sharing has been made more restrictive to remove ability to share outside of the University		
15 - Personal data might be retained longer than necessary	Review business processes for decommissioning accounts when users leave. Extend use of role accounts as appropriate.	Director of Information Systems	Review business processes for decommissioning accounts when users leave. Extend use of role accounts as appropriate.	n/a	n/a

Contact point for future privacy concerns
For further information or to report a security issue contact: 365info@essex.ac.uk

Revision History

Version	Date	Comments
1	14th July 2014	First draft
2	15th July 2014	Incorporating comments on first draft. Combined table for steps three and four
3	16th July 2014	Suggested changes by RW and BG
4	28th July 2014	Risk 11 changed to No Action Required in table for steps 5 & 6. Areas where input is required from the University highlighted.
5	16 September 2014	Updated risk assessments