Data Protection Impact Assessment

16747 - Office 365
Director: Miranda Cannon
Manager:

Complete the following and return to info.requests@leicester.gov.uk

These questions are intended to help you decide whether a DPIA is necessary.

Answering "yes" to both/either of the first 2 questions indicates that a DPIA will be required.

Answering "no" to these, but "yes" to any of the other questions is an indication that a DPIA would be a useful exercise.

You should seek further advice and can expand on your answers as the project develops if you need to.

You can adapt these questions to develop a screening method that fits more closely with the types of project you are likely to assess.

1) Will the project involve any high risk, special category or monitoring activities? e.g.

- Evaluation or scoring of individuals
- Automated decision making resulting in legal / significant effects
- Systematic monitoring e.g. internet tracking, CCTV cameras
- Large-scale processing (e.g. large numbers of records or data subjects, long length of retention, large geographical spread)
- Data Matching
- Vulnerable people
- Children (under 18)
- New technology
- Service can be refused / withdrawn
- Sensitive data (race/ethnicity, political opinions, religious beliefs, trade union membership, health/ mental health, criminal, biometric, genetic, sex life/sexual orientation)

Yes. Use of OneDrive in particular could include storage / sharing of sensitive data and large scale processing, plus the data of children and vulnerable people.

2) Will it have significant impact on the data subjects / service users?

Maybe – it depends on how much people adapt to the new way of working and whether or not they just restrict themselves to the basic InterFace use only initially. If users begin to operate OneDrive, risks are immediately increased.

If the answer to any of the above questions is yes-consider the following:

3) Will it involve the collection of new information about individuals?

No

4) Will the project compel individuals to provide information about themselves?

No

5) Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

No

6) 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

7) Will the project require you to contact individuals in ways that they may find intrusive?

No

Data Protection Impact Assessment

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
The Office365 implementation project is IT led with a brief to deliver a new Microsoft SharePoint based InterFace intranet site, a performance analytics and reporting platform, and an Office365 platform with associated applications by the end of 2018. These include: SharePoint Intranet: • An upgrade to our InterFace intranet site using a modern intranet platform • Includes a "yellow pages" directory, SharePoint document libraries, personal configuration and powerful search functionality Microsoft Teams Collaboration Platform: • Enables divisional and project teams to collaborate using a shared environment that includes Facebook-like conversations together with team shared storage and document sharing functionality Office365 Applications: • Online versions of MS Office applications including a personal OneDrive cloud file storage space that supports flexible and mobile working and potentially provides the capability to share documents and files with partner organisations • Includes a video streaming application with YouTube-like functionality initially being used for O365 training videos but capable of providing corporate video sharing channels User Access to InterFace and Office365 solutions can be extended with the aim to improve flexible working. This includes: From the Office: • Staff will be able to directly access the SharePoint Intranet and office365 solutions without logging in with a separate username and password • They will be able to use desktop and online versions of Office365 applications Using mobile or home based LCC devices: • Staff with Windows 10 LCC laptops or home workers with LCC networked devices will also be able to directly access InterFace and Office365 applications without a separate login Using Internet connected personal computers, tablets or smartphones: • Staff who have been assigned a security token will be able to access online Office365 applications from the office.com web portal • Staff will be able to login using the LCC email address and network password. They will be prompted to provide a security code as an additional proof of identity

- SharePoint, Teams, Planner, OneDrive, Stream and OneNote applications are available for download to mobile devices from the relevant App Stores. These will be automatically deployed to authorised LCC mobile devices and will be available on personal devices following the implementation of the BYOD security solution and policy. .
- Staff may also download the Office365 desktop applications on up to 4 home devices but usage will be secured with their work email address and password

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

There will be data sharing but we are advising that data should only be shared with authorized users. Information Services are providing the tools but we are not in control of what data is shared or where it comes from. The platform will be available to all LCC staff members with network AD accounts.

The biggest impact will be with Teams and OneDrive as we see these as being the tools that will change the way in which we work. The point of these systems is to improve document sharing, collaborative editing, document management, and administrative efficiency.

Communications, HR and Digital Transformation are creating a network of 'super users' that will help staff to understand these tools better.

We have amended our Acceptable Use Policies to incorporate these new solutions and it is attached for reference

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
Information Services haven't set retention dates on the information that is being stored on SharePoint/OneDrive or Teams. This will be down to the users to manage themselves. What we have done is applied a 14 day expiry to sharing documents regardless of whether they are shared internally or externally. If Confidential and Sensitive information is stored in OneDrive and Teams, it must only be accessed by authorised users and must not be shared with external users and organisations using the functionality of OneDrive and Teams, unless a Data Protection Impact Assessment (DPIA) has been completed in respect of the proposed activity. This affects the entire organisation throughout the city.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
We are providing a tool to enable the users to store and access information. Storing data is a BAU process, and these businesses could use this data to provide a service to service users. The system will be available to all areas of the council including Social Care but the Acceptable Use Policy makes it clear that they should not be using this for confidential or sensitive information. This technology is hosted by Microsoft and is continually being developed. It is widely adopted by all sectors of business. Microsoft have taken steps to ensure the platform is GDPR compliant. UK certification details are published on the Microsoft compliance site https://www.microsoft.com/en-us/TrustCenter/Compliance/UK-G-Cloud

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
Through Office365, LCC staff will be able to more easily share documents, collaboratively edit documents, and create document libraries. A consistent platform for storing council information.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
Information Services will be referring all staff to the Office365 Help page available on the new InterFace where they can access a variety of training materials including narrated walkthroughs. The Acceptable Use Policy specifically written for the Office365 applications will also be available here. We have consulted with Information Governance about our GDPR responsibilities and Digital Transformation/Human Resources about user adoption.

Step 4: Assess lawful basis

Describe the lawful basis for processing the data: Which of the Article 6 and Article 9 conditions apply? Please say which are valid and what legislation allows you to operate in your service area.

GDPR Article 6 (for non-sensitive data)

1. Consent
2. Contract
3. Legal Obligation (law says we must)
4. Vital Interests (life or death situation)
5. Public Task / Official Authority (law says we can)
6. Legitimate Interests

GDPR Article 9 (for sensitive data - race/ethnicity, political opinions, religious beliefs, trade union membership, health/ mental health, criminal, biometric, genetic, sex life/sexual orientation)

1. Explicit Consent
2. Employment, social security or social protection law
3. Vital interest of data subject or another
4. Made public by data subject
5. Legal claims
6. Substantial public interest
7. Medicine, health or social care
8. Public health
9. Research and statistics
10. Safeguarding

In respect of personal and special category data, there is also justification for processing of personal data under Article 6 & 9 under various statutory obligations including (but not limited to):

- Local Government Act 2000
- The Care Act 2014
- Housing Act 2004 and related legislation
- The Localism Act 2011
- The Equality Act 2010

DPA 2018 Schedule Conditions met:

Schedule 1, Part 1, 1-Employment, social security and social protection

Schedule 1, Part 2, 2-Health or social care purposes

Schedule 1, Part 2, 6-Statutory etc. and government purposes

Schedule 1, Part 2, 11-Protecting the Public against dishonesty

Schedule 1, Part 2, 16-Support for individuals with a particular disability or medical condition

Schedule 1, Part 2, 18 & 19-Safeguarding of children and individuals at risk/their economic wellbeing.

Schedule 3, Part 2, 2- Health Data

Schedule 3, Part 3, 7-Social Work Data

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Microsoft agreement is that all data is within the EU.

The alternative methods are basically what we have now. Users would continue to use network shared drives and Outlook for email communication.

We are stating that this platform is not used for sharing confidential or sensitive information unless a DPIA has been completed and authorised which will determine if there is a need to give individuals information about their data on a case by case basis.

We will prevent function creep by centrally controlling the configuration.

10

Step 5: Identify and assess risks

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Fair, lawful and transparent			
No legal basis.	Legal basis identified- each individual team will need to identify theirs.	Reduced	Yes
Not necessary or proportionate.	Considerations met- appropriate use of personal data	Reduced	Yes
Privacy Notice not given.	Privacy Notice issued to service users by services using system. If Microsoft update their ways of working, LCC's Privacy Notice may need to reflect changes so Microsoft Privacy Notice updates to be monitored.	Reduced	Yes

If consent-based processing, consent was not obtained and recorded.	Consent to be recorded by individual services as required	Reduced	Yes
Purpose			
Purpose creep: data used for something it wasn't collected for.	System administration, Staff access levels to the suitably configured, and training to be put in place, briefings in FACE produced and policy for use (AUP) adopted and promoted to users of systems.	Reduced	Yes
Unpermitted access by third party / employee.	Written contract and data processing agreement in place with supplier/provider (Microsoft)	Reduced	Yes
Theft of data.	Staff training. Disciplinary action / prosecution taken where necessary.	Reduced	Yes

Data Minimisation			
Too much data collected that's not necessary	Training provided and AUP to emphasise the importance of recording what is required; and	Reduced	Yes
	Processes to be documented by Teams that only require information appropriate to enabling the provision of service.	Reduced	Yes
Data accuracy			
Inaccurate data collected.	Provide appropriate system administration and user levels of access, plus training and standards to ensure data is correctly collected and recorded, as part of this process.	Reduced	Yes
Data corrupted or metadata altered by users.	Regular backups required via contract requirements	Reduced	Yes
Users forget they have shared files	System configured so that all documents shared internally or externally have been given a default expiry of 7 days	Reduced	Yes
	Process in place to refer users to training guides and AUP before they share information	Reduced	Yes

Files shared/deleted incorrectly	Data quality checks and audits can be undertaken via contract requirements Regular backups required via contract requirements.	Reduced Reduced	Yes Yes
Retention and disposal			
Data kept for too long.	Appropriate System administrators to have rights over deletion of records Retention periods applied as per retention and disposal in contract / Council's schedule	Reduced	Yes
No records of destruction kept.	Records can be deleted (or marked out of use) by system administrators.	Reduced	Yes
Loss of data at end of contract	Data processed by provider (Microsoft) to be returned to Council at end of contract free of charge via contract requirements.	Reduced	Yes

Security			
Access controls not in place.	Appropriate system administration/staff access levels and deletion rights to be applied	Reduced	Yes
Monitoring and audit controls not in place.	Appropriate system administration auditing to be applied	Reduced	Yes
Malware controls, patching, virus protection etc. not in place	Any updates provided by Microsoft to be quickly applied	Reduced	Yes
Authentication not strong enough.	Council Network ID required. Strong passwords forced.	Reduced	Yes
No written contract in place with data processors.	Written contract in place with Microsoft plus similar terms with subcontractors	Eliminated	Yes
No BCP, recovery plan or backups in place.	Backups and BCP in place by LCC. Regular backups by provider via contract requirements.	Eliminated	Yes
Poor physical security.	Door entry systems are in use across council buildings.	Reduced	Yes

Poor technical security	Data encrypted in transit and rest other than OneDrive sharing final resting place. Servers physically secure by provider via contract requirements.	Reduced	Yes
Staff not adequately trained. Training materials not ready for go live data	Staff training/FACE briefings to be provided and AUP for use in place.	Accepted	Yes. Training materials ready to be launched in near future. Little risk under proposed soft launch.
Data subject rights			
Data subject requests are not responded to in required timescales.	Follow the current Council corporate policy here. Information can be retrieved by appropriate system users to answer requests for information with statutory periods (20 working days)	Reduced	Yes
Complaints are not answered.	Follow Council's data protection complaints procedure.	Reduced	Yes
Data is not deleted (if applicable).	Records can be deleted (or marked out of use)	Reduced	Yes

Data is not restricted (if applicable).	Records can be restricted.	Reduced	Yes
Transfer outside EU Data transferred or stored outside EU e.g. in cloud without adequate safeguards Backups held outside EU, without adequate safeguards. Staff users send personal data insecurely outside EU due to lack of physical controls in place.	**Hosting-Preferred:** Data transferred, stored and backed up on EU servers via contract requirements. Hosted in a location/jurisdiction with appropriate Data Protection/confidentiality laws, and under a binding contractual relationship. Training / AUP in place.	Eliminated Reduced Reduced	Yes Yes Yes

Step 6: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Miranda Cannon (Director) 01.10.18	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Lynn Wyeth (DPO) 30.09.18	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: 1. System must facilitate subject rights including the deletion or restriction of data in case of a right to erasure / restriction request and search facility to be capable locate data in response to a subject access request. 2. Audit functions to be able to determine users' actions and what data they have accessed / sent. 3. Ensure appropriate policies, procedures and training issued to users in a timely manner. 4. Add the definition of confidential and sensitive to the AUP. 5. Ensure staff are aware of the AUP. 6. Processing activities conducted by teams/departments using O365 must comply with Data Protection/GDPR requirements and Council policies.		
DPO advice accepted by:	Miranda Cannon (Director) 01.10.18	If overruled, you must explain your reasons
Comments:		

Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA