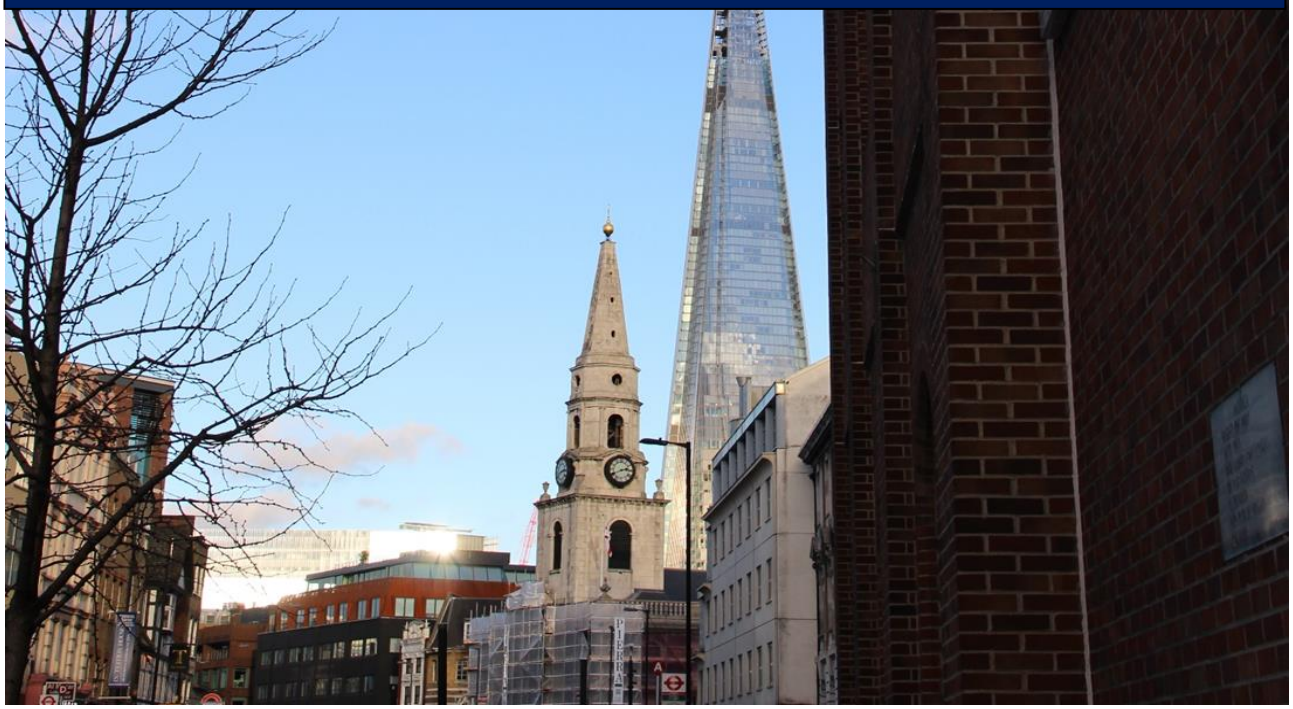
Data Protection Impact Assessment Policy



Core Documentation Cover Page					
Data Protection Impact Assessment Policy					
Version number	**Dates produced and approved (include committee)**	**Reason for production/ revision**	**Author**	**Location(s)**	**Proposed next review date and approval required**
V1.0	Aug 2018 SMT	To reflect updated guidance published by the Information Commissioner's Office	Data Protection & Freedom of Information Officer	All master versions will be held in: J:\0 Quality Team - Core Documentation Website	Aug 2020 Or in line with legislative changes

Equality Impact	
Positive equality impact (i.e. the policy/procedure/guideline significantly reduces inequalities)	
Neutral equality impact (i.e. no significant effect)	X
Negative equality impact (i.e. increasing inequalities)	

If you have any feedback or suggestions for enhancing this policy, please email your comments to: quality@uco.ac.uk

Data Protection Impact Assessment (DPIA) Policy

CONTENTS

Data Protection Impact Assessment Policy & Guidance

1. Introduction

This policy and guidance document ensures that a Data Protection Impact Assessment (DPIA) is undertaken routinely as part of the development of any new projects or reviews of current projects to consider any impacts on individuals' privacy appropriately and consistently from the outset and assures a 'privacy by design' approach to projects.

This policy and guidance document aligns with guidance published by the Information Commissioner's Office.

2. Data Protection Impact Assessments (DPIAs)

A DPIA is a process that systematically and comprehensively analyses the processing of data and helps to identify and minimise data protection risks.

DPIAs consider not only compliance risks but broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus of a DPIA is on the potential for harm - to individuals or to society at large, whether it is physical, material or non-material.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. A DPIA does not have to eradicate the risks altogether, but should help to minimise risks and assess whether or not remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping to demonstrate accountability and building trust and engagement with individuals whose data is being processed.

A DPIA may cover a single processing operation or a group of similar processing operations.

A DPIA is a project development requirement and serves the purpose of influencing project plans to mitigate privacy risks.

A DPIA is not a one-off exercise and but an ongoing process which should be reviewed regularly.

3. When to Conduct a DPIA

Under the General Data Protection Regulation (GDPR) it is mandatory to conduct a DPIA before carrying out types of processing likely to result in high risk to individuals' interests. In particular if the project plans to:

a) Use systematic and extensive profiling with significant effects;

b) Process special category or criminal offence data on a large scale; or

c) Systematically monitor publicly accessible places on a large scale

The ICO also requires organisations to conduct a DPIA if the project plans to:

d) Use new technologies;

e) Use profiling or special category data to decide on access to services;

f) Profile individuals on a large scale;

g) Process biometric data;

h) Process genetic data;

i) Match data or combine datasets from different sources;

j) Collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');

k) Track individuals' location or behaviour;

l) Profile children or target marketing or online services at them; or

m) Process data that might endanger the individual's physical health or safety in the event of a security breach.

In cases where it is not clear whether a DPIA is required, it is recommended that a DPIA is carried out nonetheless as a DPIA is a useful tool to help controllers comply with data protection law and demonstrates good practice.

A DPIA should be undertaken when it can have an effective impact on a project. Preferably this would be at an early stage in a project to ensure that potential problems are identified early and can be built into the project's development plan. This approach will also be time and cost efficient.

4. PRIVACY RISKS

A privacy risk is the risk of harm to an individual arising through an intrusion into privacy where "privacy" in this context relates to an individual's right of being let alone in the following respects:

a) Physical Privacy whereby an individual is able to maintain their own physical space or solitude and where intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.

b) Informational Privacy whereby an individual is able to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others and where intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information, collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages.

Normally most DPIAs will be related to Informational Privacy where risks may arise due to personal information being:

- Inaccurate, insufficient or out of date.
- Excessive or irrelevant.
- Kept for too long.
- Disclosed to those who the person it is about does not want to have it.
- Used in ways that are unacceptable to or unexpected by the person it is about.
- Not kept securely.

For the purposes of a DPIA, Privacy Risks are categorised into three groups as shown in Table 1. These lists include examples and are not exhaustive.

Risks to individuals can be categorised in different ways and it is important that all types of risk are considered – these range from risks to physical safety of individuals, material impacts (such as financial loss) or moral (for example, distress caused).

TABLE 1: DPIA PRIVACY RISK CATEGORIES & POSSIBLE RISKS

Category	Possible Risks
1. Risks to Individuals	Inadequate disclosure controls increase the likelihood of information being shared inappropriately. The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge. New surveillance methods may be an unjustified intrusion on their privacy. Measures taken against individuals as a result of collecting information about them might be seen as intrusive. The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect. Identifiers might be collected and linked which prevent people from using a service anonymously. Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information. Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk. If a retention period is not established information might be used for longer than necessary. If released could cause harm and distress to data subjects.
2. Corporate Risks	Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage. Problems which are only identified after the project has launched are more likely to require expensive fixes. The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business. Public distrust about how information is used can damage an organisation's reputation and lead to loss of business. Data losses which damage individuals could lead to claims for compensation.
3. Compliance Risks	Non-compliance with the Data Protection Act (DPA). Non-compliance with the General Data Protection Regulations (GDPR). Non-compliance with the Privacy and Electronic Communications Regulations (PECR).

	Non-compliance with sector specific legislation or standards. Non-compliance with human rights legislation.

5. The DPIA process

The DPIA process consists of the stages described in Figure 1.

Figure 1: The stages of a DPIA

The advice of the Data Protection & Freedom of Information Officer must be sought when you conduct a DPIA and individuals and stakeholder should be consulted throughout the DPIA process.

The DPIA should follow the stages described above and the DPIA template provided in Appendix 1 should be used to record the progress and outcomes of each stage in order to ensure that the process is consistent for all projects, that all privacy risks are carefully considered and that those affected by the project are provided with the opportunity to give their feedback.

A DPIA does not need to be started and finished before a project can progress further. The DPIA should run alongside the project development process so that what begins as a more informal early consideration of privacy issues can be developed into part of the DPIA.

6. Conducting Effective DPIAs

An effective DPIA requires a good understanding of the relationship between an individual and the organisation within the context of the project being developed including the consideration of:

- Reasonable expectations of how the activity of individuals will be monitored.
- Reasonable expectations of the level of interaction between an individual and an organisation.
- The level of understanding of how and why particular decisions are made about people

This means seeing the project from the perspective of those whose privacy may be at risk to enable the project to be designed to minimise privacy risks and around their legal rights and expectations.

Relevant legislation will also therefore need to be considered to ensure that the DPIA is effective, including:

- The Data Protection Act 2018 (DPA)
- The General Data Protection Regulation (GDPR)
- The Human Rights Act (HRA)

7. Responsibilities for Conducting a DPIAs

The UCO's Data Protection & Freedom of Information Officer (DPFIO) is responsible for conducting DPIAs in liaison with staff leading or responsible for the project.

The DPFIO should also be consulted if a new project is being considered or developed to advise on whether a DPIA is needed.

8. Reducing Privacy Risks

There are many different steps which can be taken to reduce a privacy risk. Some of the more likely measures include:

- Deciding not to collect or store particular types of information.
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

9. CONSULTING THE ICO

If the DPIA identifies a high risk and measures cannot be put in place to reduce that risk the ICO must be consulted before the processing of that data can begin.

If a DPIA needs to be consulted on by the ICO, the DPFIO shall act as the contact point between the UCO and the ICO.

The UCO shall act on the ICO's advice.

10. MONITORING THE DPIA

DPIAs shall be kept under review and revisited when necessary, for example if the type of data being processed changes or the purpose for the data processing changes.

DPIAs shall be reviewed at least annually to ensure that any privacy impact risks are revisited and amended where necessary.

It shall be the responsibility of the project manager / head of department in liaison with the DPFIO to undertake the review of the DPIA, the outcome of which shall be considered by the Information Security & Governance Committee and noted by the Senior Management Team.

APPENDIX A: DPIA TEMPLATE

This template should be used to record each DPIA process and outcome. It follows the process set out in the Information Commissioner's Office DPIA guidance, and should be read alongside that guidance[1] and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Step 1: Identify the need for a DPIA

Explain broadly what the 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 (please refer to Do I Need to Conduct a DPIA?)

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?
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?
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)?

[1] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

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?

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?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? 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?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	**Minimal, significant or severe**	**Low, medium or high**

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	**Name/date**	**Notes**
Measures approved by:		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
DPFIO advice provided:		DPFIO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPFIO advice:		
DPFIO advice accepted or overruled by:		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 DPFIO should also review ongoing compliance with the DPIA.