**PRIVACY IMPACT ASSESSMENT – guidance notes**

The aim of a Privacy Impact Assessment (PIA) is to help an organisation identify the privacy risk (the risk of harm through use or misuse of personal information) of new projects, proposals or policies and to help ensure that any potential problems are addressed at an early stage. The format of the PIA is intended to allow the process to be integrated with the University’s existing project management procedures.

PIAs benefit both the individual whose information is being used by the University and the University. Individuals can be assured that the University has followed best practice and can more easily understand how and why their information is being used; benefits to the University include increased trust with its ‘customers’, better policies and systems and a reduced likelihood of the University failing to comply with its legal obligations under the Data Protection Act 1998 (DPA) and (from May 2018) the General Data Protection Regulation (GDPR) and related legislation.

**What Is Personal DAta?**

Personal data is any information which relates to a living person who can be identified either from that information itself or from using that information in connection with other information held by the University. This can include information such as descriptions of a person, details of their employment or studies or records of their opinions.

Sensitive personal data is information which contains details on an individual’s racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life, or commission of or proceedings for any offence committed or alleged to have been committed by the individual. Special care and secure safeguards need to be put in place if sensitive personal data is to be collected or used.

**WHEN SHOULD A PIA BE USED?**

Before embarking on any new project, proposal or policy, consideration should be given as to whether a PIA is required.

The following are examples of projects that might require a PIA, although the list is not exhaustive and each project should be considered individually to determine whether a PIA is required:

* A new IT system for storing and accessing personal data.
* Permitting a third party contractor access to University IT systems (e.g. for software maintenance, etc)
* A data sharing initiative where two or more organisations seek to pool, link or transfer sets of data.
* A proposal to identify people in a particular group/demographic and initiate a course of action.
* Using existing data for a new and unexpected or more intrusive purpose.
* A new surveillance system or the application of new technology to an existing system.
* A new database which consolidates information held by separate parts of an institution.
* A new policy or strategy which will impact on privacy through the collection or use of information, or through surveillance or other monitoring.
* Purchase of new software where the provider may have access to personal data (e.g. through maintenance or storage arrangements).

**Part 1 – Screening Questions**

This section asks you some basic questions to decide whether you need to answer part 2 of the PIA. If your answer to any of the questions in part 1 is ‘yes’ or ‘maybe’ then please complete Part 2 Steps 1-3 of this form and return it to the University Archivist and Records Manager (UARM), who will complete Steps 4 and 5 in consultation with you and return it. This will usually take 2-3 weeks unless the PIA is marked as urgent.

**Part 2**

**Step 1 – Outline the project**

The purpose of this section is to clarify what the aim of your project is, what data you need to collect and why. You need to make sure that you answer these questions fully so that you are confirming all the information that you will need to use/collect and why this is relevant to your project.

**Step 2 – Describe the Information processes**

The purpose of this section is to look at what you will be doing with the data and to ensure that you are collecting the data in an appropriate way and storing and disposing of the data in a timely manner.

**Collection**

In this section you need to cover where the data comes from. For example: is it already held by the University, are we collecting it by questionnaires, online, or through other research or will we be receiving data from a third party?

You also need to think how the individual will be made aware of the use of their data. Will you be asking the individual’s permission to use the data; or does the University need to update its privacy notices (which explain how personal data is used by the University); or will a third party be responsible for this? If you do not think we need to inform the individual of the University’s intended use of their data or gain their consent, explain why.

**Storage**

Under the DPA we must ensure that data is kept securely, particularly if it is sensitive (such as school or medical records) or can easily be used to identify people. It is important that you think about how the information will be stored (electronically or otherwise) and the potential risks of unauthorised access.

**Destruction**

You can only keep the data for as long as is reasonably necessary to fulfil the purpose. Please detail in this section when you will have finished utilising the information and when the data should be destroyed. For more information on the University’s standard procedures which may be applicable, see the University’s [Records Retention and Disposal Schedule](file:///R%3A/Records-Management/Policy/Retention-Schedule.doc).

**Ongoing monitoring**

Ensuring the reasonable collection, use, storage and destruction of data is an ongoing obligation. You must ensure that before you begin the project you have thought about how you are going to continue to monitor the use, storage and retention of data. You should look to put in place a strategy to identify privacy risks and ensure they are dealt with effectively.

For example: ensuring that databases are password protected and regularly changing the passwords or removing users who are no longer authorised to access the data.

**Consultation**

In this section you should think about who you need to consult with about the proposed project and detail how you intend to carry out that consultation. You should think about who the key stakeholders are both within and outside the University and whether there are any other third parties whose views should be taken into consideration on this project. You need to list here who you will be consulting and how you plan to do this.

Examples of people/departments/organisations you may need to consider include CLS, Procurement, Marketing, the Legal Office, the Student Union, external funders, partnership organisations, etc.

You should also confirm when you intend to consult them, whether this will be before or after you start collecting, transferring or using data.

**Step 3 – Identify the privacy and related risks**

Having outlined what you intend to do, this step allows you to perform a critical analysis on the key risks and weaknesses in your project. Types of risks you may want to consider include:

**Risks to individuals:**

* Inadequate security controls increase the likelihood of information being shared inappropriately
* Has the context in which information is used changed over time, so that it is being used for a different purpose without the individual’s knowledge?
* Could the method of collecting information be seen as intrusive?
* Could information be collected and linked with other data which means that the data is not being used anonymously
* Is the information being collected and stored unnecessarily or is not properly managed so that duplicate records are created

**Risks to the University:**

* Non-compliance with the DPA and other legislation can lead to sanctions, fines and reputational damage
* Problems only identified after project launch can result in more expensive fixes
* Information which is collected and stored unnecessarily or is not properly managed so that duplicate records are created are less useful and can lead to increased time spent on administration
* Data losses which damage individuals could lead to claims for compensation
* Public distrust about how information is used can lead to damage to the University’s reputation

**Compliance risks:**

* Non-compliance with the DPA and other legislation, including human rights legislation

**Step 4 – Identify the Privacy solutions**

Once you have identified the key risks in your project, you should identify what level of risk is posed, what steps could be taken to minimise the risk and what effect that is likely to have. The risks should be categorised as follows:

**Eliminate** – the risk can be totally eliminated by the proposed actions

**Reduce** – the risk will be significantly reduced by the proposed action

**Accept** – the risk cannot be reduced or removed but will be acceptable to the University.

The main question to answer in carrying out this task is whether the final impact on individuals after implementing each solution is a justified, compliant and proportionate response to the aims of the project?

There are many different steps that the University could consider taking to reduce a privacy risk. Some examples are set out below:

* 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 by updating the University’s record retention schedule
* Implementing appropriate IT security measures
* Developing ways to safely anonymise the information where 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
* Ensuring that the University’s Privacy Notices (where the University informs individuals about how their information is used) are up to date
* Select contractors who will provide a greater degree of security and ensuring that agreements are in place which include data protection obligations
* Producing data sharing agreements which make it clear what information will be shared with a third party, how and for what purpose

In the evaluation column you should confirm that the solution is a justified, compliant and proportionate response and the reason(s) why. This is particularly important when a risk cannot be eliminated, as you will need to outline why you consider that it is justified for the University to continue the project despite the risk.

Once you have completed step 4, you should send the form to the UARM who will review the risks and set out what action should be taken in relation to the risks.

**What the UNIVERSITY ARCHIVIST AND RECORDS MANAGER will do**

**Step 5 – Sign off and Record Result**

This section is to summarise and record the actions that the UARM will request be taken to make the data as secure as possible. This section will include a record of the key action points and will be signed off by the senior member of staff responsible for the project, once these are agreed.

The UARM may also include the key dates for reviewing the outcomes and ensure that it is clear who is responsible for the ongoing monitoring and implementation of data protection solutions.

**Who can sign off?**

The UARM will review the risks and set out what action should be taken in relation to the risks. She will also set timescales for implementing these action points, if appropriate and set review dates to review the impact on privacy. It is the responsibility of the senior member of staff responsible for the project/system/proposal/policy to sign off the UARM’s recommended solutions.

It will usually take approximately 2-3 weeks for the PIA to be returned to you, however if you require an urgent response please clearly mark your form accordingly and the UARM will do her best to review it sooner.

**Publication**

A copy of the PIA (redacted as appropriate depending on the sensitivity of the information contained in it) will be retained by the UARM and monitored by the Information Governance Group.

**contact details**

The University Archivist and Records Manager is Amy-Jo Cameron-Williams. Enquiries regarding completion of a PIA should be sent to a.cameron-williams@hud.ac.uk.

If the University Archivist and Records Manager is out of the office and the enquiry is urgent, please redirect your enquiry to Rebecca McCall, Data Protection Officer and University Solicitor, data.protection@hud.ac.uk.