

Data Protection Impact Assessment (DPIA)

Project name:

Teaching Support – Recruitment and Timesheet Submission Enhancements
Part 2

Date DPIA started:

Stage 1 - preparation for screening

1.1 Project outline – what and why

Note: Explain the scope of the project to ensure you know its aims and its potential impact, explain what the project consists of and why it is undertaken. Map the data flows – where do you obtain the data, how are they processed, where are they stored.

The systems developed for Teaching Support Recruitment and Financial processes have been running throughout 2017/18. This project is to pick up on the few things that were never completed in time for the original project. Also it is to address some changes and feature enhancements that have become apparent from running the system over the past year. A second aspect of the project is to re-implement and enhance the current course proposal form done with a CGI and paper submission so it is entirely done through a Webmark form.

1.2 List of stakeholders

Note: This should cover all individuals involved in the project and those that may be affected by it – internal stakeholders and data subjects. At this stage you want to have as broad a list of groups as possible - this can be edited down at a later stage for more focused consultation.

Internal stakeholders:

Alexander Welsh (Informatics Teaching Organisation - Administrative)

Vicky MacTaggart (Informatics Teaching Organisation - Administrative)

Graham Dutton (Informatics Computing – Lead Developer)

Tim Colles (Informatics Computing – Co-Developer and Project Manager)

Martin Wright (Informatics Director of Professional Services – Project Approval Role)

Neil Heatley (Informatics Director of Teaching – Project Approval Role)

Data subjects affected by the project:

Students applying for and recruited onto teaching support posts. Academic teaching staff bidding for posts. Academic staff making course proposals.

1.3 External context

Note: This involves conducting a search for prior projects of a similar nature, from both inside and outside the organisation. This may reveal design features that have been created by other project teams in order to address much the same categories of problem confronted by your project. Note any lessons that can be learned.

We are not aware of any system within the University. We did not conduct a search for a system outside of the University but the high level of local system integration required and the fact that this project is simply refining and building on top of existing local technology means introducing a new external system would be prohibitively expensive.

Stage 1 completed by:

Tim Colles

Date:

Stage 2 - Compliance with privacy laws

Note: Data Protection legislation is relevant to any DPIA, and a DP compliance check should always be carried out. The Data Protection Officer will be able to advise you on the relevance of other privacy laws.

2.1 General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA)

Note: The template you have to fill in for the data protection compliance check can be found in Appendix A of this document. Your local Data Protection Champion and the Data Protection Officer will be able to assist with the completion.

A Data Protection compliance check has been carried out as part of this DPIA, the details of which are in appendix A. From this we have concluded:

The legal basis for processing is that it is necessary for public tasks as this covers all data processing to perform tasks that are required to provide an education. The data is used by administrative staff in Informatics Student Services (covering taught and research students). Selected subsets of the data are made available to academic teaching staff and some categories of other staff (such as computing support) that need access to it under the same legal basis.

2.2 Human Rights Act (HRA) (Article 8)

Note: In most cases HRA considerations will be covered by the other work on this DPIA, including the DP compliance check. If that is the case, you can simply record here that there are no special considerations that are not covered by other aspects of the DPIA. If there are any outstanding issues, describe them here.

Not Applicable

2.3 Privacy and Electronic Communications Regulations 2003 (amended 2011) (PECRs)

If the project involves electronic marketing messages (by phone, fax, email or text), cookies, or providing electronic communication services to the public, you also need to make sure you comply with the PECRs.

The following guidance will help:

[Information Commissioner's Office PECR guidance.](#)

[University marketing and data protection guidance](#)

[University cookies guidance *EASE restricted*](#)

Describe any issues here, or confirm if not applicable.

Not Applicable

2.4 Common Law duty of confidence

Not Applicable

2.5 Others

Not Applicable

Stage 2 completed by:

Tim Colles

Date:

Stage 3 - Screening

Note: The information you have gathered in Stage 1 should assist you in addressing the screening questions.

3.1 Technology

3.1.1 Will there be new or additional information technologies that have substantial potential for privacy intrusion?

Yes:

No:

3.2 Data collection

3.2.1 Will the project involve the collection of new information about individuals?

Yes:

No:

3.2.2 Will the project compel individuals to provide information about themselves in the course of the project?

Yes:

No:

3.3 Identification methods

3.3.1 Will there be new or substantially changed identity authentication requirements that may be intrusive or onerous?

Yes:

No:

3.4 Involvement of multiple organisations

3.4.1 Will the initiative involve multiple organisations that will have access to the personal data?

Yes:

No:

3.5 Changes to the way data is handled – considering the actual processing

3.5.1 Will there be new or significant changes to the handling of special categories of personal data or data that would be considered sensitive by the data subjects? Examples are data about racial and ethnic origin, political opinions, health, sexual life, offences and court proceedings, finances and information that could enable identity theft.

Yes:

No:

3.5.2 Will the personal details about each individual in an existing database be processed in a new and different way?

Yes:

No:

3.5.3 If yes to the above, will this involve a large number of individuals?

Yes:

No:

3.5.4 Will there be new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?

Yes:

No:

3.6 Changes to data handling procedures – considering policy documents and standards

3.6.1 Will there be new or changed data collection policies or practices that may be intrusive?

Yes:

No:

3.6.2 Will there be changes to data quality assurance or processes and standards that may be unclear or unsatisfactory?

Yes:

No:

3.6.3 Will there be new or changed data security arrangements that may be unclear or unsatisfactory?

Yes:

No:

3.6.4 Will there be new or changed data security access or disclosure arrangements which may be unclear or permissive?

Yes:

No:

3.6.5 Will there be new or changed data retention arrangements that may be unclear or extensive?

Yes:

No:

3.6.6 Will there be changes to the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?

Yes:

No:

3.7 Decision on how to proceed

Note: From the work you have done above, you should now be in a position to determine whether you need to do a DPIA, or whether a privacy law compliance check is sufficient. Record your conclusion below:

No DPIA is necessary as this project is only enhancing existing processes, including migrating to already existing technology – no changes to technology or collected data are being made.

Stage 3 completed by:

Tim Colles

Date:

--

Stage 4 - Internal stakeholder consultation

Note: Consult all internal stakeholders identified under 1.2 to conduct a preliminary identification of risks.

4.1 Risk analysis

The table below lists the key privacy risks that have been identified by the internal stakeholders.

Note: You do not need to do a detailed assessment of the risks at this at this stage. It is, however, important to be reasonably clear about what the main risks are.

	Description of risk	Preliminary assessment of exposure Low/Medium/High
Risk 1	Click here to enter text.	L <input type="checkbox"/> M <input type="checkbox"/> H <input type="checkbox"/>
Risk 2	Click here to enter text.	L <input type="checkbox"/> M <input type="checkbox"/> H <input type="checkbox"/>
Risk 3	Click here to enter text.	L <input type="checkbox"/> M <input type="checkbox"/> H <input type="checkbox"/>
Risk 4	Click here to enter text.	L <input type="checkbox"/> M <input type="checkbox"/> H <input type="checkbox"/>
Risk 5	Click here to enter text.	L <input type="checkbox"/> M <input type="checkbox"/> H <input type="checkbox"/>
Risk 6	Click here to enter text.	L <input type="checkbox"/> M <input type="checkbox"/> H <input type="checkbox"/>
Risk 7	Click here to enter text.	L <input type="checkbox"/> M <input type="checkbox"/> H <input type="checkbox"/>

Risk 8	Click here to enter text.	L <input type="checkbox"/> M <input type="checkbox"/> H <input type="checkbox"/>
---------------	---------------------------	--

Note: From the risks identified by the internal stakeholders you should now be in a position to assess whether an external stakeholder consultation is appropriate. If there are only few low to medium risks, you might wish to continue straight to **Stage 6**.

Is an external stakeholder consultation needed? Note any rationale behind the decision.

Click here to enter text.

Stage 5 - External stakeholder consultation

Note: For Large DPIAs, where there has been extensive consultation, you may wish to produce a separate consultation report, which should then feed into the analysis. **Always** complete Stage 5 to ensure compliance with the Data Protection Act and other privacy laws.

5.1 External consultation

Note: Decide what type of external consultation will be most appropriate and will give you the best and most complete results – focus groups, mail shots, ...

5.2 External stakeholders

Stakeholder name	The privacy issues they raised
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.

Stage 6 - Risk analysis

Note: You should carry out the risk analysis using exactly the same methodology as you do for other project risks. The table in Appendix B is provided as a guide only and should be adapted to conform to your project risk register. some useful pointers on the types of solutions to privacy risks that can be explored (see section 7).

The
Guide to
DPIAs
provides

The table in Appendix B shows the key risks that have been identified, and the options for avoiding or mitigating those risks.

Stage 7 - Approval

7.1 Recommendation

Note: Drawing on your analysis of the privacy risks and other project risks, explain which option presents the best way forward. If significant risk remains, you should explain what the problem is and why the stakeholder consultation failed to resolve this. Your recommendation may then be that the project needs to be re-thought.

[Click here to enter text.](#)

7.2 Approval

Note: For large projects, this stage should align with the Full Business Case and approval should be given by the relevant budget holder. All you need to record below is who has approved the recommendation at 7.1 and the terms of that approval.

[Click here to enter text.](#)

Stages 4-7 completed by:

[Click here to enter text.](#)

Date:

Stage 8 - Readiness for service

Note: Explain below what checks were carried out before the service went live to ensure that the privacy solutions approved as part of this DPIA are working, and that the system or process is still legally compliant, as well as whether updates were required to any relevant privacy notices:

Click here to enter text.

Stage 8 completed by:

Click here to enter text.

Date:

Stage 9 - Review

Note: Indicate below how and when the post-implementation review will be carried out:

Click here to enter text.

Stage 9 completed by:

Click here to enter text.

Date:

About this guidance

Version control	Author/editor	Date	Edits made
7	Data Protection Officer	December 2018	Changed references in 1.2 to 'data subjects' instead of 'external'

			stakeholders', for clarity
6	Assistant Data Protection Officer	October 2018	Stage 8 edited to include requirement to update privacy notices
5	Claire Friend	May 2018	Review section, renamed from Review or Audit
4	Claire Friend	March 2018	DPO edits made.
3	Claire Friend	15/03/2018	Document edited to conform to accessibility guidelines. Also edited numbering to make it run concurrently.
2	Provided by Data Protection Officer, minor edits by DICM	8 March 2018	Links added in, and PECR section amended

If you require the guidance in an alternative format, please contact Records Management:

recordsmanagement@ed.ac.uk or 0131 651 4099

Appendix A

Data protection compliance check

Note: completion of this template requires knowledge of data protection legislation. Assistance can be obtained from your local Data Protection Champion and the Data Protection Officer.

Where you have already provided the information at Stage 1 of the main DPIA Template, simply cross-refer to the relevant answer.

	Question	Answer
1.	What type of personal data is going to be processed?	Click here to enter text.
2.	Which of the legal bases in Article 6 (1) will provide a legitimate basis for the processing? Consult the guidance Guidance –determine the legal basis for processing personal data	Click here to enter text.
3.	<p>If special categories of personal data are going to be processed, which of the legal bases in Article 9 (in addition to the Article 6(1) legal bases) will provide a legitimate basis for that processing? Consult the document Guidance – determine the legal basis for processing special categories of personal data</p> <p>Note – special categories of personal data are personal data consisting of information as to (a) the racial or ethnic origin of the data subject, (b) political opinions, (c) religious beliefs, (d) Trade Union membership, (e)</p>	Click here to enter text.

	physical or mental health, (f) sexual life, (g) genetic data and (h) biometric information.	
4.	<p>Are there any special considerations relating to Article 8 of the Human Rights Act that will not be covered by the DPIA?</p> <p>Note – This Article provides that everyone has the right to respect for his private and family life, his home and correspondence. It is subject to qualifications relating to national security, crime etc.</p>	Click here to enter text.
5.	Will any of the personal data be processed under a duty of confidentiality? If yes, how is that confidentiality being maintained?	Click here to enter text.
6.	How are individuals being made aware of how their personal data will be used?	Click here to enter text.
7.	Does the project involve the use of existing personal data for new purposes?	Click here to enter text.
8.	What procedures will be in place for checking that the data collection procedures are adequate, relevant and not excessive in relation to the purpose for which the data will be	Click here to enter text.

	processed?	
9.	How will the personal data be checked for accuracy?	Click here to enter text.
10.	Has the personal data been evaluated to determine whether its processing could cause damage or distress to data subjects?	Click here to enter text.
11.	Will there be set retention periods in place in relation to the storage of the personal data?	Click here to enter text.
12.	What technical and organisational security measures will be in place to prevent any unauthorised or unlawful processing of the personal data?	Click here to enter text.
13.	Will you be transferring personal data to a country outside of the European Economic Area? If so where, and what arrangements will be in place to ensure that there are adequate safeguards over the data?	Click here to enter text.

Risk register for privacy impact assessment

Risk description	Inherent Privacy Risk			*Options for avoiding or mitigating this risk	Risk Owner	Residual Privacy Risk		
	Impact	Likelihood	Exposure			Impact	Likelihood	Exposure

* For each privacy risk, there could be a number of options for avoiding or mitigating that risk. You should list all the options then consider the residual risk for each one.