Data Protection Impact Assessment (DPIA)

Project name:

Mock REF Reviewer System

Date DIPA started:

17/01/19

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.

Produce a system with a secure back end database where pre-determined REF panel members can be authorised to access the submitted research papers and assign a rating to them - this to be followed by a moderation process with a final rating recorded. The data on up to six research papers which each author has submitted for the REF, linked to their name, and attached a ranking (1 to 6) as well as their one hundred word summary will be extracted automatically from PURE. This system just needs to make that data locally available (read only) and provide a mechanism to assign panel members to reviewers and for panel members to record their ratings of the papers assigned to them.

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:

Jane Hillston (Head of School)

Steve Renals (Coordinator – Research Excellence Framework)

Victoria Lindstrom (Research Data Manager)

Tim Colles (Developer and Project Manager)

Data subjects affected by the project:

Academic and research staff within the School of Informatics that are submitting and/or reviewing research papers for the REF2021.

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.

The University and College stated explicitly that they would not implement a central system. The obvious external system to use for this would be PURE itself, however this does not have support enabled for the REF paper review and rating process. Any other external system (such as a general conference paper review system) would need local integration and/or modification and given we could leverage existing local technology would have been prohibitively expensive (and unnecessarily complex) by comparison.

The review function has now been switched on in PURE, meaning that it does now have support for REF paper review. However we do not want to give reviewers access to this functionality and will continue to use our locally implemented system because using PURE:

1. requires reviewers to undergo centrally arranged REF2 training

2. has associated risks of reviewer names being exposed to authors of reviewed outputs should the wrong comment functionality be used

3. requires records to be locked ("selected for review") and subsequently unlocked (set back to "proposed") should the nominator wish to apply the reviewer's feedback (e.g. on the 100 word statement), before a final estimated score is assigned to the REF2 record. Whereas with our local system, we will go through the review and potential feedback implementation before assigning final predicted scores to PURE REF2 records.

Stage 1 completed by:

Tim Colles

Date:

17/01/19

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 the University's legitimate interest in order to participate in exercises used to assess the quality of research in UK Higher Educational Institutions, including REF2021 and its successors. For the corresponding LIA please refer to the one produced by the central University REF team.

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:

17/01/19

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 many 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:

A DPIA is necessary.

Stage 3 completed by:

Tim Colles

Date:

17/01/19

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	Submitted research papers, their rankings and supporting statements become visible outside the group that should have access but not	L ■ M ☐ H ☐

	beyond members of the School. Risk to individuals.	
Risk 2	Research paper assigned reviewers/moderator, their ratings and comments become visible outside the group that should have access but not beyond members of the School. Risk to individuals.	L ■ M ☐ H ☐
Risk 3	Submitted research papers, their rankings and supporting statements become visible outside the School/University. Risk to individuals and corporate risk.	L ☐ M ■ H ☐
Risk 4	Research paper assigned reviewers/moderator, their ratings and comments become visible outside the School/University. Risk to individuals and corporate risk.	L ☐ M ■ H ☐

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.

No, minimal risk.

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. The Guide to DPIAs provides some useful pointers on the types of solutions to privacy risks that can be explored (see section 7).

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.

Proceed with implementation and deployment.

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.

Tim Colles

Stages 4-7 completed by:

Tim Colles

Date:

17/01/19

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:

The system was implemented using existing technology and configuration templates so only basic functional tests were carried out. Access control (authentication and access to parts of the system) was rigorously tested against the designed access model before and after deployment.

Stage 8 completed by:

Tim Colles

Date:

17/01/19

Stage 9 - Review

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

A review will be completed as part of the mock REF exercise in 2019.

Stage 9 completed by:

Tim Colles

Date:

17/01/19

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?	Rankings, comments, reviewers and moderators, their ratings, decisions and comments for research papers submitted for REF2021 by academic/research staff.
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	Legitimate Interest
3.	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	Not Applicable

	provide a legitimate basis for that processing? Consult the document Guidance – determine the legal basis for processing special categories of personal data 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) physical or mental health, (f) sexual life, (g) genetic data and (h) biometric information.	
4.	Are there any special considerations relating to Article 8 of the Human Rights Act that will not be covered by the DPIA? 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.	Not Applicable
5.	Will any of the personal data be processed under a duty of confidentiality? If yes, how is that confidentiality being maintained?	No
6.	How are individuals being made aware of how their personal data will	Processing is being carried out under the legitimate interest of the

	be used?	University, individuals will be aware through the University data protection policy, privacy statement and LIA for the REF2021 process.
7.	Does the project involve the use of existing personal data for new purposes?	No
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 processed?	This DPIA and a Privacy Statement will be in force. No change in data or function is expected.
9.	How will the personal data be checked for accuracy?	The accuracy of the source data from PURE is at the discretion of the individual owners and PURE system owners. The referee service users will be responsible for the accuracy of the data they enter, and ultimately the service owner (REF coordinator).
10.	Has the personal data been evaluated to determine whether its processing could cause damage or distress to data subjects?	Yes
11.	Will there be set retention periods in place in relation to the storage of the personal data?	The data will be entirely deleted within one year of the completion of the REF2021 submission.

12.	What technical and organisational security measures will be in place to prevent any unauthorised or unlawful processing of the personal data?	Using mature, secure and proven technology. Using central (School) authentication service. Using central (School) authorisation service. Using standard, secure, proven database. Minimal points of access. Minimal direct user base. Using firewall. System is actively monitored and backed up. Using system regularly patched centrally for security updates. Authentication, authorisation and functional access control implemented once in the database and used by all access points.
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?	No

Appendix B

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
Submitted research papers, their rankings and supporting statements become visible outside the group that should have access but not beyond members of the School. Risk to individuals.	**Low**	**Low**	**Low**	Adopt proven secure technology. Use official authentication mechanism. Use official authorisation control. Minimise points of access.	**School of Informatics**	**Low**	**Low**	**Low**

				Limited user base. System decommissioned after REF2021.				
Research paper assigned reviewers/moderator, their ratings and comments become visible outside the group that should have access but not beyond members of the School. Risk to individuals.	**Low**	**Low**	**Low**	Adopt proven secure technology. Use official authentication mechanism. Use official authorisation control. Minimise points of access. Limited user base.	**School of Informatics**	**Low**	**Low**	**Low**

				System decommissioned after REF2021.				
Submitted research papers, their rankings and supporting statements become visible outside the School/University. Risk to individuals and corporate risk.	**Low**	**Low**	**Medium**	Adopt proven secure technology. Use official authentication mechanism. Use official authorisation control. Minimise points of access. Limited user base. System decommissioned	**School of Informatics**	**Low**	**Low**	**Medium**

				after REF2021.				
Research paper assigned reviewers/moderator, their ratings and comments become visible outside the School/University. Risk to individuals and corporate risk.	**Low**	**Low**	**Medium**	Adopt proven secure technology. Use official authentication mechanism. Use official authorisation control. Minimise points of access. Limited user base. System decommissioned after REF2021.	**School of Informatics**	**Low**	**Low**	**Medium**

* 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.