DATA PROTECTION IMPACT ASSESSMENT FORM

Project Title:	
Brief Description of the project:	

Name of Responsible Person	**Position:**

Department:

Timing of the project: (start/end dates/duration etc.)

Date form completed:

PART 1

Screening Questions

	Yes	No
Will the project involve the collection of new information about individuals?		
Will the project compel individuals to provide information about themselves?		
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		
Are you using the information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example the use of biometrics or facial recognition		
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		
Is the information about individuals a kind particularly likely to raise privacy concerns or expectations including special categories of data? For example, health records, criminal records or other information that people would consider to be particularly private?		
Will the project require you to contact individuals in a way which they may find intrusive?		
Will the project introduce new facilities that might be used by individuals in the institution to gather, process, analyse or share personal information in ways that would previously have required specialist support?		
Will the project involve the processing of personal data by third parties (third parties could include cloud based services)?		
Will the project expose personal data to elevated levels of security risks?		
Are stakeholders likely to have privacy concerns about the project?		

If the answer to any of the questions above is "Yes", Part 2 should be completed. Otherwise, just complete part one and submit a copy to the Data Protection Officer.

PART 2

1) **Project Details**
   Explain what the project aims to achieve, what the benefits will be to the University, to individuals and to other parties. You may find it helpful to link to other relevant documents relating to the project, for example, a project proposal.

2) **Details of Personal Data**
   Please indicate what personal data will be collected/stored/processed.

   Administration Data
   Name ☐
   Date of Birth/Age ☐
   Gender ☐
   Contact Details ☐
   Unique identifier e.g. student number ☐
   Other data (please specify):

   Special Categories of Data
   Racial or ethnic origin ☐
   Political opinion ☐
   Religious or philosophical beliefs ☐
   Trade Union Membership ☐
   Physical or mental health condition ☐
   Sexual life and sexual orientation ☐
   Genetic Data ☐
   Biometric Data used to identify an individual ☐

   Other sensitive information
   Financial information/bank account details ☐
   Criminal convictions and offences ☐
   Other (please specify):

Under article 6 of the GDPR one of the following conditions needs to apply before the processing is lawful. Please indicate which position applies:

- The individual who the personal data is about has given/will give unambiguous consent to the processing ☐
- The processing is necessary for the performance of a contract with the individual ☐
- The processing is necessary for a legal obligation
- The processing is necessary for the vital interest of someone (i.e. a life or death situation) ☐
- The processing is carried out by a public body in the public interest ☐
- The processing is in the legitimate interests of the University or another party and does not prejudice the rights and freedoms of the individual (please provide further details): ☐

If special categories of data are being processed different conditions for processing apply. Please speak to the Data Protection Officer for further information.

---

3) Describe the information flows
The collection, use and deletion of personal data should be described here and it may also be helpful to refer to a flow diagram or other way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

---

4) Consultation requirements
Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

---

5) Identification of privacy and related risks
Identify the key privacy steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

Privacy Issue	Risk to Individuals	Compliance Risk	Associated organisation/corporate risk

6) Identification of privacy solutions
Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing systems)

Risk	Solution	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?

7) Sign off and record the outcomes

Risk	Approved Solution	Approved By

8) Integrate the outcomes back into the project plan
Who is responsible for integrating the outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Action to be taken	Date of completion of action	Responsibility for action

Please submit a copy of the completed form to the Data Protection Officer.

Date last revised: 13/04/2018

Notes on completing the form

1) Project details

Identify why the project is being planned, what the project is intending to achieve and why it is necessary. As well as providing a clear case for the project as a whole, it should highlight those features that may have the potential to impact on privacy. If other organisations are involved in the processing please say who they are and what their involvement is.

2) Details of personal data

Provide details of the personal data involved, including whether it includes special categories of personal data or other sensitive data. Also provide details of the justification for processing the personal data.

3) Describing the information flows

Describe the information flows of the project, how information is collected, stored, used and deleted. How will data be checked for accuracy and kept up to date. Explain what information is used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information. If the project involves new links with personal data held in other systems please explain. What security measures will be in place? Will any information be sent off site or transferred outside of the EEA? How will individuals be told about the use of their personal data?

Have similar projects been carried out before, either by the University of other organisations?

4) Consultation requirements

Consultation allows people to highlight privacy risks based on their own area of interest or expertise. It also provides an opportunity for them to suggest measures to reduce the risks. Relevant internal stakeholders should be consulted whilst ensuring their attention is focused on privacy issues. In some cases external consultation may be appropriate. Consultation should be timely, clear, proportionate, reach representative individuals, ask objective questions and seek feedback.

5) Identification of privacy and related risks

Examples of risks include inaccurate, insufficient or out of date information; excessive or irrelevant data; information kept for too long; disclosing the information to someone who should not see it; using information in a way that is unacceptable or unexpected to the person it is about; and information not kept securely. These could cause upset or unnecessary intrusion on privacy. Risks can include risks to physical safety, financial loss or distress caused. Sharing or merging datasets allows the collection of much wider information than an individual might expect.

Some risks will be to the organisation – for example damage to reputation, or the financial costs or a data breach.

Legal compliance risks include the EU General Data Protection Regulations (GDPR), Privacy and Electronic Communications Regulations 2003 (PECR), and the Human Rights Act 1998 (see table below for more details)

6) Identification of privacy solutions

Explain how you could address each risk. Some might be eliminated altogether. Other risks might be reduced. In some cases the chances of risks being realised are small or the impact will be minimal and it may be appropriate to recognise and accept the risks. In these cases the risks should be recorded along with the reasons for accepting the risks.

Evaluate the likely costs and benefits of each approach. Think about the available resources, and the need to deliver a project which is still effective. Consider whether the impact on privacy is proportionate to the aims of the project by balancing the project's outcomes with the impact on individuals. Examples of steps that could be taken to reduce privacy risks include:

⬜ Not collecting or storing some information
⬜ Devising retention periods and planning secure destruction of information
⬜ Using appropriate technology
⬜ Anonymising information when possible
⬜ Producing guidance on the use of the system
⬜ Allowing user access to information so they can correct and access their own data
⬜ Having the necessary agreements in place when data processors are used.
⬜ Having data sharing agreements making it clear what information will be shared and who it will be shared with

For more information about building privacy into a project during the design stages please see the separate guidance on 'Data Protection by Design and by Default'

7) Sign off and record of outcomes

Make sure that the privacy risks have been signed-off at an appropriate level. This can be done as part of the wider project approval.