Data Protection Impact Assessment (DPIA)

BEDS SU

If you are beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process, The following form should be completed to assess the potential impact on our current data protection procedures and the right of individuals.

Completed by__________________ Department_______________Date____________

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of data processing it involves. Summarise why you identified the need for 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 another way of describing data flows. 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)?

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

Step 5: Identify and assess risks

Describe the 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	Minima, 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 or accepted	Low, medium or 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*
DP Champion advice provided:		*DP Champion should advise on compliance, step 6 measures and whether processing can proceed*
Summary of DPO advice (if any):		
Review Date:		