Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) should be completed at the outset of any project, or change to an existing system or process, that involves or may involve the collection or handling of personal information that is considered high risk. It identifies risks to individuals' privacy rights and/or corporate risks (such as failure to comply with relevant data protection legislation), and where relevant identifies measures required to mitigate those risks. UUSU takes the safeguarding of personal data very seriously and therefore employs a DPIA in these instances. To decide whether it will be necessary to conduct a DPIA UUSU will consider the following screening questions:

- Will the project or process involve the collection of new information about individuals?
- Will the project or process compel individuals to provide information about themselves?
- Will information about individuals be disclosed to individuals or organisations who have not previously had routine access to the information?
- Are we using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project or process involve us using new technology that may be perceived as being intrusive such as the use of biometric technology?
- Will the project or process result in us making decisions or acting against individuals in ways that can have a significant impact upon them?
- Is the information about individuals of a certain kind particularly likely to raise privacy concerns or expectations e.g. health records, criminal records or any other information individuals would consider to be private?
- Will the project require us to contact individuals in ways they may find intrusive?

DPIAs are strongly recommended by the Information Commissioner's Office. From May 2018, DPIAs will be mandatory where the personal data processing is "high risk". Further guidance is also available from the Information Commissioner's Office.

Examples of where a DPIA must be considered by UUSU:

- Implementation of new systems or projects that process high volumes of personal data, such as HR and/or student records system.
- Systems or projects that process particularly sensitive personal information (e.g. concerning health).
- Third parties processing high volumes of personal data or any sensitive personal data on behalf of UUSU.
- Processing of personal data that could be considered 'profiling' of individuals (e.g. learning analytics).
- Any automated personal data processing that results in decisions being made about individuals without human input
- Processing perceived to be particularly intrusive (e.g. enhanced/increased CCTV).
- Processing personal data involving children or vulnerable adults.
- Where a contract/agreement or grant requires UUSU to conduct a Data Protection Impact Assessment.
- Any processing of biometric data, such as fingerprints or face recognition

This policy shall be reviewed by UUSU annually, or more frequently if appropriate, to reflect relevant legislative, regulatory, or organisational developments.