**Data Protection Impact Assessment Policy**

1. **Introduction**
   1. The UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA) require the University as a data controller to consider and apply appropriate measures designed to implement their key principles effectively. Necessary safeguards must be incorporated into all activities involving the processing of personal data in order to ensure that the rights and freedoms of individuals are protected.
   2. A key element of the UK GDPR’s focus on accountability is the requirement to undertake a Data Protection Impact Assessment (DPIA) where any processing of personal data is “likely to result in a high risk” to the rights and freedoms of individuals. A Data Protection Impact Assessment (DPIA) is a tool that enables the University to identify and minimise the data protection and privacy risks of processing (using personal data). At the same time, a DPIA should ensure compliance with data protection law and other legal and regulatory requirements (for example, the Equality Act 2010).
   3. DPIAs are a legal requirement under Data Protection law for any processing that is likely to be high risk. Failure to carry out a DPIA when required, carrying out a DPIA in an incorrect way, or failing to consult the ICO where required, can result in a fine in the region of £10 million pounds or, in the case of an undertaking, up to 2% of the total annual turnover of the preceding financial year whichever is higher.
2. **Scope of this Policy**
   1. This Policy is to be used in all cases where new processing of personal data is planned. This could include a new administrative system, novel uses of data (particularly where this could not reasonably be expected by data subjects), a new external supplier (or new processing for an existing supplier), or application or portal used by participants or attendees at an event. This guidance is also to be used where there is a contract renewal where the University are using an existing supplier.
   2. This policy applies to all staff at the University. This includes temporary, casual or agency staff and contractors, consultants and suppliers working for, or on behalf of, the University.
3. **Roles and responsibilities**
   1. All members of staff involved in the development of projects, initiatives, studies, processes and systems (collectively referred to in this Policy as Initiatives) are responsible for ensuring that they are aware of this Policy and understand the circumstances in which a DPIA should be undertaken.
   2. The University Secretary’s Office is responsible for overseeing and reviewing the implementation of this Policy and must be consulted in relation to any DPIAs undertaken in accordance with its requirements.
   3. In practice, it is the responsibility of the staff member or team (i.e. the project manager, system owner, principal investigator etc.) leading an Initiative to undertake the screening questions and produce the first draft of a DPIA if necessary. This can then be further worked up in collaboration with the Head of Data Protection and Legal Services, who is the Data Protection Officer, and other relevant stakeholders.
   4. Draft DPIAs should be sent to the Data Protection team at: [dataprotection@sheffield.ac.uk](mailto:dataprotection@sheffield.ac.uk).
4. **Identifying the need for a DPIA**
   1. A DPIA must be undertaken before the processing of any personal data which is “likely to result in a high risk to the rights and freedoms” of individuals. As such, it is necessary to identify whether there are any factors that warrant the need for a DPIA to be undertaken.
   2. In the case of any Initiatives involving the processing of personal data that were commenced before 25th May 2018 (when the UK GDPR came into force) and which are ongoing, such Initiatives should be reviewed and the need to undertake a DPIA considered.
   3. Where any new Initiative will involve the processing of personal data, the DPIA Screening Questionnaire should be completed. It is expected that the questionnaire will be completed by those leading the development of the Initiative.
   4. Before completing the questionnaire, it is important to:
      1. identify the key stakeholders in the Initiative so that they can provide their input into the questionnaire; and
      2. have a clear understanding of the scope and objectives of the Initiative so that the questionnaire can be completed as fully and accurately as possible.
   5. Where the outcome of the questionnaire suggests that the processing is unlikely to result in a high risk to individuals, there may be circumstances where it is advisable to undertake a DPIA anyway due to:
      1. the nature, scope, context and purposes of processing personal data;
      2. the groups of individuals affected by the processing (e.g. children or vulnerable adults);
      3. the level of investment in the Initiative in terms of time, financial and other resources; or
      4. the visibility of the Initiative internally and externally.
   6. Where it has been concluded that a DPIA is unnecessary and will not be undertaken, the reasons for this should be clearly documented. The Screening Questionnaire should be sent to the Data Protection Officer in addition to being retained. This will evidence the decision made. It may need to be revisited and reviewed at a later date. The Data Protection team will maintain a register of completed DPIAs.
5. **Undertaking a DPIA**
   1. Having concluded that a DPIA is necessary or desirable for a particular Initiative, the DPIA Template should be completed. The DPIA Template explains the objectives and requirements of each section. Where any section is not completed because it is not applicable or not considered necessary, this should be explained.
   2. Part of the DPIA may involve consultation with relevant internal and external stakeholders. In the case of consultation with third party data processors, the contract with such third parties should include an obligation on them to provide assistance with undertaking DPIAs. However, this may have cost implications which should be considered and discussed with the third parties beforehand. In the case of consultation with professional advisers and other experts, the scope and cost of their involvement will need to be considered and approved by the University’s Data Protection Officer.
   3. Data protection law requires the University to have a lawful basis for processing personal data. Staff must select the appropriate lawful basis from the list of Article 6 UK GDPR lawful bases below. If the initiative will involve processing special category personal data, there must be a lawful basis under Article 6 UK GDPR and a lawful basis under Article 9 UK GDPR. Staff must select the appropriate lawful bases from the list of Article 6 UK GDPR and Article 9 UK GDPR lawful bases below. Staff may seek guidance from the Data Protection team when selecting the appropriate lawful basis.
   4. Where the DPIA identifies Legitimate Interests as a lawful basis, Appendix 1 of the DPIA Template should be completed and approval granted from the Data Protection Officer.
6. **Consultation with the ICO**
   1. Where the outcome of a DPIA is that the processing of personal data in the context of an Initiative would result in a high risk and it is not possible to take any measures to eliminate or mitigate that risk, the UK GDPR requires that the processing cannot commence before the Information Commissioner’s Office (ICO) has been consulted.
   2. The ICO should not be consulted without the approval of the University’s Data Protection Officer, who will initiate contact with the ICO. Consultation with the ICO should only be necessary in very exceptional instances as it is expected that the University will be able to apply measures to appropriately mitigate or eliminate risk on most occasions.
7. **Review of DPIAs**
   1. A DPIA should be undertaken at the earliest opportunity in the development of an Initiative and re-assessed prior to commencement of the relevant processing activities to identify whether any changes to the Initiative impact upon the outcomes of the DPIA and whether the controls and measures identified in the DPIA have been integrated into the Initiative.
   2. Once the processing of personal data has commenced in respect of an Initiative, the DPIA should be reviewed regularly having regard to the nature and risks associated with the processing, and taking into account any changes to the processing activities or scope of the Initiative. A review should be undertaken at least annually by the staff member or team leading or owning the Initiative.
8. **Disclosure and publication of DPIAs**
   1. There is no legal requirement to proactively disclose or publish a DPIA, although it could be subject to a request made under the Freedom of Information Act 2000 and so may need to be released, subject to any exemptions contained in the legislation. However, it may be necessary to disclose a DPIA to another institution to provide assurance that due and proper consideration has been given to the data protection implications of an Initiative.
   2. A decision may also be taken to publish a DPIA in order to further build trust and confidence in the processing of personal data in relation to an Initiative and to demonstrate accountability and transparency. However, such a decision may only be taken in consultation with the University’s Data Protection Officer, and any DPIA that is being published should be redacted to remove any confidential or commercially sensitive information.
9. **Policy review**
   1. This Policy will be reviewed as required and at least every two years by the University Secretary and the Head of Data Protection and Legal Services.