**Data Protection Standard Operating Procedure**

The Data Protection Standard Operating Procedures (SOPs) are practical guides on what the University must to do in order to comply with Data Protection Laws. Details of who is responsible for this SOP and the definitions used in it are set out in Annex A.

**Data sharing**

**THE UNIVERSITY IS COMMITTED TO “PRIVACY BY DESIGN” AND “PRIVACY BY DEFAULT” OBLIGATIONS. IF YOU ARE CONSIDERING PROCESSING PERSONAL DATA ON BEHALF OF THE UNIVERSITY YOU MUST FOLLOW THIS PROCEDURE AND DEMONSTRATE THAT YOU HAVE DONE SO.**

1. **Scope**
	1. This SOP provides a 3 STAGE Frameworkwhich **must** be followed before providing, sharing or receiving personal data and entering into data protection agreements with third parties.
	2. A quick start guide which summarises the practical steps can be found here.
	3. If you have any queries in connection with this SOP or the University’s standard data protection agreement templates, please contact Information Governance for assistance by emailing dataprotection@dundee.ac.uk.

**STAGE 1 – ASSESSMENT STAGE**

1. **Initial Data Risk Assessment**
	1. **Every time** the University is considering sharing personal data with, or receiving personal data from, another party, an Initial Data Risk Assessment (IDRA) **must** be undertaken.
	2. If the outcome of the IDRA indicates that a full Data Protection Impact Assessment (DPIA) should be carried out (e.g. because data sharing/processing is likely to result in a high risk to individuals), then a DPIA must be completed.
2. **Data Protection Impact Assessment**
	1. You must complete a DPIA if any of the responses to the screening questions in the IDRA are ‘Yes’.
	2. The DPIA helps to identify and address risks at an early stage by analysing how the proposed uses of personal information and technology will work in practice. Unwanted risks are mitigated through action plans.
	3. All information required from you is set out within the DPIA available here. **You must complete the form.** If you require any assistance, please refer to Information Governance. See 4.1.

**STAGE 2 - DOCUMENTATION STAGE**

1. **Contract (AKA Data Sharing Agreements)**
	1. The University will not allow for the sharing and/or receiving of personal data if that is likely to result in a high risk to individuals and where the risk cannot be appropriately managed and mitigated.
	2. The control that the University exercises in this regard is through the use of contracts to document the rights and responsibilities and safeguards when sharing and receiving personal data.
	3. The IDRA or DPIA should identify the need for a contract and the relevant type applicable.
	4. The University has its own data protection agreement templates. It is essential to select the correct template which accurately describes what the parties are doing and their roles under Data Protection Laws. To help you select the correct template, please see guidance at Annex B.
	5. The University’s preferred position is to use our own templates rather than agreements or terms provided by the other party; however, this may not always be possible or acceptable to the other party. If using a University template, you should complete the Processing Details at the start of the template as much as you can. Once the Processing Details are completed you should then send the agreement to Information Governance (dataprotection@dundee.ac.uk) for review as part of the documentation required under section 6.
	6. If it is agreed that the other party’s data protection agreement or terms are used, then you should complete the sections relevant to the University as much as you can and send a copy to Information Governance (dataprotection@dundee.ac.uk) as part of the documentation required under section 6
	7. Sometimes data protection terms are not included in a separate agreement specifically for covering the sharing of data but are included in a clause or schedule/annex in another contract the University is going to enter into with the other party. If that is the case, you should send that agreement to Information Governance in order that they can review the data protection section of the contract.
	8. If you are using one of the University’s template agreements, please ensure that you have it reviewed by Information Governance before you send it to the other party for their comments/approval.
	9. IF YOU ARE NOT SURE WHAT TEMPLATE TO USE PLEASE ASK INFORMATION GOVERNANCE FOR GUIDANCE.
	10. IN **ALL** INSTANCES, PERSONAL DATA SHARED WITH ANY THIRD PARTIES REQUIRES A CONTRACT.
2. **Privacy Notice**
	1. Depending on the outcome of your IDRA and/or DPIA a new privacy notice may be required. All privacy notices of the University are contained here. If you consider that there already is an existing relevant privacy notice in place which covers your intended activity, please forward a copy to the Information Governance team for review and amendment where necessary to cover the personal data being processed.
	2. If your data sharing is not covered by an existing privacy notice please complete the template privacy notice and then send it to the Information Governance for review.

**STAGE 3 – REVIEW AND FEEDBACK**

1. **Information Governance**
	1. The Information Governance team is headed by the University’s Data Protection Officer (DPO) who is responsible for the compliance management and risk oversight by the University in respect of Data Protection Laws and reporting to the ICO.
	2. You must send all completed IDRAs, DPIAs, Contracts and privacy notices to Information Governance.
	3. You should send the above documentation to Information Governance at least 30 days before you need to be able to share, supply or receive personal data.
	4. If there is a difference of opinion between you and Information Governance in respect of compliance with this SOP, the DPO will decide whose decision shall be final.
	5. All decisions of the DPO shall be kept on file by the Information Governance team.
2. **Information Governance review process**

7.1 Information Governance help complete relevant documents.

7.2 Information Governance will review the documents (mentioned in 6.2 above) that you send to them and help you to complete them, if required.

* 1. Information Governance will assess any changes to the University’s standard templates or any agreements/terms proposed by the other party.
	2. Information Governance will support you to have any agreements relating to data protection negotiated and agreed with the other party or parties.
	3. Information Governance will not review any of the documents if you have not supplied an IDRA as it is important that they have sufficient background information before spending time looking at a DPIA and/or legal agreement.

### Identify Serious Issues

* 1. Information Governance will consider the documents (mentioned in section 6.2 above) to identify if the proposed arrangements include any Serious Issues. To help with this assessment, Information Governance will refer to the Information Governance Legal Risk Management Protocol Statement for Data Sharing Agreements.
	2. Information Governance may request further information from you and/or consult others (such as IT) to help with its assessment.
	3. If Information Governance identify a Serious Issue they must consult Legal for advice.
	4. If **at any time** there are changes to the proposed arrangement, for example to the agreement/terms (e.g. proposed by the other party), Information Governance should be made aware of these, and it will consider whether the changes give rise to any Serious Issues.

Confirm whether an agreement/term may be signed

* 1. When Information Governance are satisfied that all the relevant documents have been agreed and/or completed and that any identified Serious Issues have been mitigated, they will confirm by email that the agreement/terms may be signed under the University’s Schedule of Delegation. Once signed by each party, the proposed provision, sharing and/or receipt of personal data may start. A copy of the fully signed agreement should be sent to Information Governance for logging and retention.

1. **Ongoing contract management and changes**
	1. Information Governance will maintain a register of data protection agreements entered into by the University. It will make a note of the date on which the relevant agreement is due to expire, and you will need to manage issues in connection with the end of the agreement.
	2. You are responsible for managing the relationship with the other party including taking any appropriate and/or required actions in connection with the agreement.
	3. If you become aware of a data breach in connection with the agreement, you should follow the University’s SOP – Data Breaches.
	4. If you become aware of any other breach (either by the University or the other party) of the agreement or Data Protection Laws (which is not a personal data breach), you should immediately contact the DPO.
	5. If, after the agreement has been signed, there are any proposed changes to the arrangement or the agreement relating to data provision, sharing and/or receipt, the process set out in this SOP must be followed in full in connection with such changes. You must have prior written permission from Information Governance for changes to be made and/or for any agreement to be amended.

**Annex A**

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Meaning**  |
| **Data Protection Laws** | means any law, statute, subordinate legislation regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body which relates to the protection of individuals with regard to the processing of personal data, electronic communications and privacy to which a party is subject including the Data Protection Act 2018 and any statutory modification or re-enactment thereof and the UK GDPR |
| **DPIA** | Data Protection Impact Assessment |
| **DPO** | Data Protection Officer |
| **IDRA** | Initial Data Risk Assessment |
| **Information Governance** | The University’s Information Governance team |
| **ICO** | Information Commissioner |
| **personal data** | Any information relating to an identified or identifiable Data Subject. |
| **Serious Issue** | means red or amber issues set out in the Information Governance Legal Risk Management Protocol Statement for Data Sharing Agreements |
| **SOP** | Standard Operating Procedure |

**Who is responsible for the Data Protection SOPs?**

### Data Protection Officer (DPO)

The DPO is responsible for implementing and overseeing the University’s compliance with the Standard Operating Procedures (SOPs).

The DPO shall provide such guidance, resources and training in Data Protection as required in order for University staff to have a reasonable level of awareness in respect of Data Protection Laws and regulation as they apply to their role. The SOPs form part of this.

### General need for compliance

All University staff are responsible for complying with the SOPs and ensuring that any matters relating to data protection are actioned appropriately and in a timely manner. Staff are also expected to attend any training relating to data protection as required.

If a member of University staff is found to have willfully or negligently breached this procedure, they may be subject to the University’s disciplinary procedures.

**Who is the University’s DPO?**

The University’s DPO is Dr Richard Parsons. Contact details are set out below:

|  |  |
| --- | --- |
| Email | dataprotection@dundee.ac.uk  |
| Telephone | x84441 |

**General duties of the DPO**

In terms of Article 39 of the UK GDPR, the DPO shall have at least the following tasks:

* to inform and advise the University and its employees about our obligations to comply with the UK GDPR and other data protection laws;
* to monitor compliance with the UK GDPR and other data protection laws, and with our data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
* to advise on, and to monitor, [data protection impact assessments](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/);
* to cooperate with the ICO; and
* to be the first point of contact for the ICO and for individuals whose data is processed (employees, students etc).

**ANNEX B**

**Selecting the right University agreement template**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  **University = controller**  **Party 2 = processor** **ONLY UOD GIVING DATA** The University decides on data. Party 2 has very restricted rights on data use. e.g. is not permitted to use the data for its own purposes; |  | **University = controller**  **Party 2 = controller** **ONLY UOD GIVING DATA** Party 2 can decide the purposes for which it uses the personal data provided by the University. |  | **University = controller**  **Party 2 = controller****UOD AND PARTY 2 EACH GIVING AND TAKING DATA** Each party decides the purposes for which it shares/uses the personal data. |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| **UOD TEMPLATE A**  |  | **UOD TEMPLATE B**  |  | **UOD TEMPLATE C**  |