**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.

**Requests for personal data from external agencies**

**IT IS A CRIMINAL OFFENCE TO ALTER OR DELETE PERSONAL DATA TO PREVENT DISCLOSURE ONCE IT HAS BEEN REQUESTED.**

**1 Scope**

1.1 Data Protection Laws permits the disclosure of personal data to external agencies without the consent of the Data Subject where certain circumstances apply.

1.2 This SOP details the process to be followed by the University where an external agency requests personal data from the University pertaining to its students, staff, or other stakeholders. It does not apply to SARs for personal data made by Data Subjects.

**2 Who makes decisions about sharing personal data?**

2.1 The University’s DPO will make any decisions about what personal data the University can share with external agencies except in the following circumstances:

* the request is urgent and there is no time to consult with the DPO at the time
* the University is closed and the DPO is unavailable.

**3 Does the request have to be in writing?**

### Requests from Police Scotland

3.1 Any request for information from Police Scotland must be in writing and will normally be made using a standard Police form. If the Police have not provided a form they should be asked to complete one before sharing any information with them. Details of what information the form should contain are at Annex B.

### Other agencies

3.2 A request must be in writing and include the following information:

* details of the external agency submitting the request
* the authority for the claim in reference to any applicable Acts, Regulations, or other frameworks, including any lawful basis for accessing/processing the data requested
* the relevant case number or file reference (where applicable)
* an explanation of the purposes of the claim on the information.

### Exceptions

3.3 Exceptions to the above may apply when a request for information is urgent – see section 4.5 below.

**4 What should you do if you receive an urgent request for personal data?**

### What is an urgent request?

4.1 Urgent requests for personal data include those where a delay in responding to a request may result in:

* the requestor failing to prevent or detect crime
* the requestor failing to apprehend or prosecute an offender
* an immediate threat to a Data Subject’s life or safety.

4.2 Examples of urgent requests are:

* the emergency services require personal data about an individual in order to treat them in the event of an accident or to protect them from harm from themselves or others
* the Police have requested to view CCTV footage or obtain personal data as part of a current incident in which a crime may have been committed.

4.3 If you decide that the request is urgent, and it is appropriate for the personal data requested to be shared immediately, then you should do the following:

* confirm the identity of the person making the request
* share the information
* make a written record of the request and the data you have shared
* send the record to the DPO without delay - dataprotection@dundee.ac.uk

4.4 If the request relates to viewing CCTV, you should contact Campus Security by calling 4141 from a campus phone or 01382 384141.

### Who should you contact for assistance in case of an emergency?

4.5 If the request is an urgent one you should contact the DPO immediately by calling 01382 384082 . If the DPO is not available then you should contact Campus Security by calling 4141 from a campus phone or 01382 384141.

**5 What should I do if the request is not urgent?**

5.1 You should refer the request on to the DPO as soon as possible using the e-mail address dataprotection@dundee.ac.uk. If the DPO is unavailable due to the University being closed, you should refer the request to Campus Security.

**6 How should the DPO or Campus Security deal with a request?**

### Confirm identity

6.1 The identity of the person making the request should be confirmed. This may be done by calling the agency on a general telephone number and confirming the contact details, role and status of the requestor.

###  Review information provided

6.2 A review of the authority for the claim on the personal data should be carried out with reference to any Acts, Regulations or mandates cited by the agency. If the request for personal data is complex or unclear, advice should be sought from Legal.

6.3 Any supporting information provided by the agency should also be reviewed. In addition, a check should be made to ensure that all applicable aspects of the claim, such as reference numbers and an explanation of the purpose of the request, have been provided.

### Decide whether or not to disclose the personal data

6.4 The options are:

* disclose the personal data requested in full
* disclose only part of that data redacting/withholding any other personal data or unrelated data.
* refuse the request.

6.5 Where disclosure of some or all of the data is considered appropriate, a decision shall be made as to how the data will be shared securely. This may include:

* agreeing methodologies for the secure transfer of the data to be disclosed between the University and the agency claiming the information
* agreeing the scope of any disclosure of data, the limitation of the purposes for which the data may be used by the agency, its retention and disposal.

6.6 Where disclosure by the University is not considered appropriate, the agency should be provided with written confirmation that the personal data shall not be disclosed.

6.7 Examples of circumstances which may lead to the University considering disclosure to be inappropriate include:

* where there is doubt as to the identity or authority of the person making the request
* where it is unclear why the information cannot be obtained directly from the individual.

In circumstances such as the above, it may be useful to discuss the request with the agency to establish whether any additional information could be provided that would address the reason for not disclosing the data. If any additional information is provided then it should be reviewed and decided upon.

### Make a full and accurate record

6.8 Full and accurate records of the above process should be made and retained. These should include:

* details of the request made and the requesting agency
* the process carried out to confirm the identity of the requestor
* the reasoning for the decision to disclose or not to disclose the personal data, including any relevant Act, Regulations or mandates; and
* where personal data is disclosed, details of the personal data disclosed and the method of disclosure.

6.9 If the data was disclosed by Campus Security, the above information must be sent to the DPO and/or Information Governance without delay using the e-mail address dataprotection@dundee.ac.uk.

**Annex A**

Definitions

|  |  |
| --- | --- |
| **Definition** | **Meaning**  |
| **Data Subject** | Anyone who can be identified, directly or indirectly, by reference to an identifier such as a name, email address or student identification number. |
| **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 |
| **DPO** | Data Protection Officer |
| **external agency** | Includes, but is not limited to, the Police, Local Government, Electoral Registration Officers, Health and Social Care Agencies. |
| **ICO** | Information Commissioner |
| **personal data** | Any information relating to an identified or identifiable Data Subject. |
| **SOP** | Standard Operating Procedures  |
| **SAR** | Subject Access Request |

**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 Richard Parsons. His contact details are set out below:

|  |  |
| --- | --- |
| Email | dataprotection@dundee.ac.uk  |
| Telephone | 01382 384082 |

**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**

# Police requests for personal data

### What can we release to the Police?

The Data Protection Act 2018 allows for the University to share personal data with Police Scotland for the following purposes:

* the prevention or detection of crime
* the apprehension or prosecution of an offender
* the assessment or collection of any tax or duty or of any imposition of a similar nature.

Unless a Court order is made, the University will only consider releasing information where:

* denying the information request would impede the Police’s ability to undertake a lawful duty, connected with the prevention or detection of crime or for taxation
* the Police could not obtain the information requested from a source other than the University
* release of the information would not conflict with other legal obligations which the University is required to comply with.

### What information should a Police request comprise of?

A written request will usually be on a Police standard form. In any event, any request for personal data must be made in writing and include:

* a summary of the reason as to why the information is required and is not otherwise obtainable
* details identifying the individual(s) about whom personal data is being sought
* the precise information required about the individual(s)
* the name, rank and number of both a requesting and authorising Police Officers
* the signatures of both the requesting and authorising Police Officers

### What rank should an authorising officer be?

The authorising Police Officer must be a senior rank to the requesting Officer and of a rank no lower than an Inspector. If the Police cannot provide sufficient details as to why they seek the information without prejudicing an investigation, the request must be authorised by an Officer of the rank of Superintendent or above.