**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 – Subject Access Requests (SARs)**

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

**1 Scope**

* 1. Under data protection law individuals have the right, in certain circumstances, to access the personal data which the University processes about them by making a Subject Access Request (SAR).

1.2 This SOP provides a framework which must be followed when the University receives a SAR. It specifically applies to requests by Data Subject for personal data as opposed to general information about the University or its business. It does not apply to Freedom of Information or Environmental Information requests.

1.3 IF YOU ARE NOT SURE WHICH PROCEDURE APPLIES TO A REQUEST FOR INFORMATION, PLEASE CONTACT THE INFORMATION GOVERNANCE TEAM FOR ASSISTANCE by emailing dataprotection@dundee.ac.uk.

**2 Does the SAR have to be in writing?**

2.1 Ideally SARs should be made in writing and sent to dataprotection@dundee.ac.uk.

2.2 SARs do not have to be in writing, however, receiving them in that format allows for a quicker and more effective response from the University.

2.3 If you receive a SAR in a different format please consult with Information Governance.

**3 How can the University be sure the SAR is from a genuine individual?**

### Confirming identity when SARs are from the Data Subject

3.1 Before responding to a SAR we must make sure that there is enough information to be sure of the individual’s identity. If more information is needed to confirm this, we must let the individual know as soon as possible.

3.2 It is important that, when requesting additional information to confirm identity, any request is proportionate and necessary.

### What about SARs made on behalf of others?

3.3 Data subjects can make a SAR via a third party. Often this will be a solicitor acting on behalf of their client, but it could be that an individual feels comfortable allowing someone else to act for them. If the request comes from any third party, we should ensure that third party has the authority to make the request on behalf of the Data Subject who is the subject of the SAR.

### How should identity be confirmed?

3.4 If the SAR has come from the Data Subject, we should write to them and ask for a copy of their driving license or passport. Template letter 1 in Annex D should be used.

**4 How long does the University have to respond to a SAR?**

### Does the University have all of the information needed to respond?

4.1 If the University has all of the information needed to properly respond to SAR, a response must be sent without undue delay and, in any event, within one calendar month of receipt of the SAR.

4.2 The time limit starts from the day the SAR is received whether it is a working day or not.

### Can the time limit be extended?

4.3 The time limit can be extended by a further two months in certain circumstances. These include where the SAR is complex, additional information is needed or there are a number of requests from the same individual.

### When does the time limit start if extra information has had to be obtained to confirm someone’s identity?

4.4 The period for responding to the request begins when you receive the additional information.

### How is a calendar month calculated?

4.5 A calendar month starts on the day the University received the SAR, even if that day is a weekend or a public holiday. It ends on the corresponding calendar date of the next month.

Example:

SAR is received on 3 September, therefore, the time limit starts on 3 September. This means the University has until 3 October to comply with the SAR.

4.6 If the corresponding calendar date does not exist because the following month has fewer days, it is the last day of the month that is used as the deadline.

Example:

SAR is received on 31 March, therefore, the time limit starts on 31 March. As there is no equivalent date in April, the University has until 30 April to comply with the SAR. However, if 30 April falls on a weekend, or is a public holiday, the calendar month ends the next working day.

4.7 If the corresponding calendar day falls on a public holiday then the University would have until the next working day to respond.

Example:

SAR is received on 25 November, therefore, the time limit starts on 25 November. The corresponding calendar date is 25 December, but 25 and 26 December are bank holidays, therefore the University has until the next working day, 27 December, to comply with the SAR.

**5 Can the University charge a fee for processing a SAR?**

5.1 In most cases the University cannot charge a fee and personal data should be provided for free.

5.2 In certain circumstances, for example if the SAR is manifestly unfounded or excessive, we may charge a reasonable fee.

**6 What should a member of staff do if they receive a SAR?**

### Forward the SAR to Information Governance

6.1 If you receive a SAR you should bring it to the attention of Information Governance without delay. The preferred way to do that is to email details of the request and any relevant information you have to dataprotection@dundee.ac.uk.

6.2 Information Governance should acknowledge receipt of your e-mail so that you know that the SAR has been received. If you do not receive an acknowledgement within 48 hours you should contact Kate McBay, Senior Information Governance Officer, to check that the SAR was received by email to - KMcbay001@dundee.ac.uk.

**7. What will Information Governance do when they receive the SAR?**

### Identify who has made the SAR

7.1 If there are doubts about the identity of the individual making the SAR, or if the request is made by a third party, more information should be requested, as per section 3.3 above.

7.2 When requesting more information, Template 1 in section 10 should be used.

### Record receipt of the SAR

7.3 On the day that the SAR is received, a written record should be made of the following:

* who has made the SAR
* date and time of the SAR
* information requested.

7.4 Information Governance should acknowledge receipt of your e-mail so that you know that the SAR has been recorded. If you do not receive an acknowledgement within 48 hours you should contact Information Governance.

### Acknowledge receipt of the SAR

7.5 Information Governance shall acknowledge receipt of the SAR to the requestor within 3 days of receipt. Template 1 in Annex D should be used.

### Manifestly unfounded or exaggerated

7.6 If a SAR is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature, the University can:

* refuse the request
* request a reasonable fee to deal with the request.

7.7 Information Governance shall assess the SAR and decided whether or not it is manifestly unfounded or excessive and decide what should happen with the request.

### Exemptions

7.8 Certain exemptions apply to SARs. A list of these can be found at Annex C. These include:

* personal data being subject to professional privilege
* personal data processed for scientific or historical research purposes.

7.9 Information Governance shall decide whether an exemption applies to a SAR and record that decision. If an exemption does apply then the SAR should be refused.

### Search for and collate the personal data if SAR accepted

7.10 Once it is decided that a SAR shall be accepted, Information Governance should arrange for a search of all places where the relevant personal data may be held. This may include, but is not limited to:

* databases
* systems
* applications
* manual files
* notes
* papers
* emails
* shared ‘S’ drives
* personal ‘H’ drives
* Internal computer hard drives
* External computer hard drives
* USB sticks

7.11 Where the University processes a large quantity of information about a Data Subject, it is reasonable to ask them to specify the information that the SAR relates to.

### Third parties

7.12 If there are any third parties who hold personal data on the University’s behalf, Information Governance should contact them and seek their assistance with the SAR.

### Screen information

7.13 Once all relevant personal data has been obtained, Information Governance should check that it actually relates to the Data Subject concerned and not someone else with the same name.

7.14 Only information about the Data Subject who the SAR relates to should be disclosed. If another Data Subject’s personal data is also included then their personal data should be redacted prior to responding to the SAR.

### Responding to the SAR

7.15 The last thing for Information Governance to do is to respond to the SAR.

7.16 Annex B sets out in detail the information that should be included in a SAR response. Template 2 in Annex D should be used.

**8 What can the Data Subject do if they are not happy with the University’s response to the SAR?**

### Complain to the University

8.1 If the Data Subject is not satisfied with the University’s response to a SAR then they may complain to the University. If you receive a complaint relating to a SAR you should send it to Information Governance in the first instance using the e-mail address dataprotection@dundee.ac.uk.

### Complain to the ICO

8.2 If, even after the University has responded to their complaint about the SAR, the Data Subject remains dissatisfied, they may submit a claim to the Information Commissioner’s Officer (ICO).

**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 |
| **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**

**How to respond to SAR if accepted**

1. We must confirm to the Data Subject whether or not we are processing their personal data.

2. If personal data of the Data Subject is being processed, the University must provide the Data Subject with the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other electronic means:

* the purposes of the processing
* the categories of personal data concerned (for example, contact details, exam results, bank account details)
* the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients overseas (for example, US-based service providers);
* where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
* the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data or to object to such processing
* the right to lodge a complaint with the Information Commissioner’s Office (“ICO”) (and include the ICO contact details)
* where the personal data are not collected from the Data Subject, any available information as to their source
* the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject; and
* where personal data are transferred outside the EU, details of the appropriate safeguards to protect the personal data.

3. We shall also provide the Data Subject with a copy of the personal data processed by us in electronic form (unless the Data Subject has specifically requested not to be provided with the copy in electronic form) within one month of receipt of the request.

4. Before providing the personal data to the Data Subject making the SAR, we shall review the personal data requested to see if they contain the personal data of other Data Subject s. If they do, we may redact the personal data of those other Data Subjects prior to providing the Data Subject with their personal data, unless those other Data Subjects have consented to the disclosure of their personal data.

Please see Template letter 2 for our template response.

**Annex C**

**Exemptions**

**The following examples apply to SARs:**

|  |  |
| --- | --- |
| **Purpose of processing** | **Exemptions** |
| **Crime and taxation: general** | Exemption for the purposes of the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of tax or duty. |
| **Crime and taxation: risk assessment system**  | Exemption for personal data which consists of a classification applied to a Data Subject as part of a risk assessment system operated by government, local authority or another authority administering housing benefit for crime and taxation purposes. |
| **Immigration** | Exemption for the purposes of the maintenance of effective immigration control, or the investigation or detection of activities that would undermine the maintenance of effective immigration control. |
| **Required to be disclosed by law or in connection with legal proceedings** | Exemption if:• we are obliged by law to make personal data available to the public; • disclosure is required by law or court/tribunal order; or• disclosure is necessary for the purposes of actual or prospective legal proceedings, or obtaining of legal advice |
| **Functions designed to protect the public etc** | Exemption for the purpose of certain bodies or persons discharging functions, including:• to protect the public in relation to financial loss, harm by persons authorised to carry on any profession or other activity,• to protect charities and community interest companies and their property from mishandling,• to protect the health and safety of persons at work or other persons in connection with the action of persons at work,• to protect the public for maladministration and failures by a public body and to regulate anti-competitive behaviour. |
| **Protection of the rights of others** | Exemption if a disclosure of information would involve disclosing information relating to another individual identifiable from the information. |
| **Legal professional privilege** | Exemption for information subject to legal professional privilege or confidentiality of communications. |
| **Self-incrimination** | Exemption from certain GDPR provisions where compliance would reveal evidence of the commission of an offence and would expose that person to proceedings for that offence. |
| **Management forecasts** | Exemption for the purposes of management forecasting or management planning in relation to a business or other activity to the extent that the application of those provisions would be likely to prejudice the conduct of the business or activity concerned. |
| **Negotiations**  | Exemption where personal data consists of records of the our intentions in relation to any negotiations with the Data Subject to the extent that the application of those provisions would be likely to prejudice the negotiations.  |
| **Confidential references** | Exemption if the personal data consists of a confidential reference for purposes including the education, training or employment of the Data Subject. This exemption also applies to the appointment of the Data Subject to any office, including that of a volunteer, or the provision of any service by the Data Subject. |
| **Exam scripts and exam marks** | Exemption when personal data is recorded by a candidate during an exam. |
| **Research and statistics** | Exemption if personal data is processed for scientific or historical research purposes, or for statistical purposes. |
| **Archiving in the public interest** | Exemption if personal data is processed for archiving purposes in the public interest. |
| **Serious harm from health data disclosure** | Exemption when the serious harm test is met or where a controller who is not a health professional obtains an opinion from someone who appears to be an appropriate health professional. |
| **Journalistic, academic, artistic and literary purposes** | Exemption if the personal data is being processed for the special purposes with a view to publication by a person of journalistic, academic, artistic and literary material in the public interest. |

**Annex D**

**Templates**

**Template 1 – SAR Acknowledgement**

[On headed notepaper]

[ADDRESSEE]

[ADDRESS LINE 1]

[ADDRESS LINE 2]

[POSTCODE]

[*DATE*]

Dear [*NAME OF INDIVIDUAL*],

**Acknowledgment of your Data Subject request**

I write to acknowledge receipt of your request for [*INSERT DETAILS OF REQUEST*].

Your request was received on [*DATE*]. Unless there are grounds for extending the deadline to reply, which we consider below, we expect to be able to respond to you by [*DATE*].

In order to proceed we need confirmation of your identity. I would therefore be grateful if you could provide a copy of your driving licence or passport to [*INSERT*] at [*ADDRESS*].

[We require further information to be able to investigate your request. [*DETAILS OF THE INFORMATION REQUIRED*]].

Once we have received your confirmation of identity [and we have considered the additional information requested] we will be able to consider your request.

Taking into account the complexity and number of the requests you have made, we may need to extend the period for responding. We will advise you if this is the case. In addition, if any of your requests are unfounded or excessive, we may either charge a reasonable fee to take account of the administrative costs of taking the action you have requested or refuse to act on your request. We will advise you if this is the case

We look forward to hearing from you.

Yours sincerely,

**Template 2 – Response to a SAR**

[On headed notepaper]

[ADDRESSEE]

[ADDRESS LINE 1]

[ADDRESS LINE 2]

[POSTCODE]

[*DATE*]

Dear [*NAME OF INDIVIDUAL*],

**Response to your data subject access request dated [DATE OF REQUEST]**

We write further to your subject access request [and our acknowledgment letter of [DATE]].

Enclosed with this letter are copies of personal data relating to you.

[Further to your request to us dated [DATE], we can provide the following details which may enable you to determine whether you wish to make a subject access request relating to a particular matter. [We confirm that the following individuals were involved in the [recruitment exercise OR redundancy exercise] you asked about: [NAMES].]

[Some personal data has been omitted for the following reasons:

* [It is subject to legal privilege.]
* [It consists of a confidential reference given by us for employment purposes.]
* [It consists of records of intentions in relation to negotiations between us and you, disclosure of which we consider would be likely to prejudice those negotiations.]
* [It consists of health records and we consider that disclosure would be likely to cause serious harm to another person.]
* [OTHER]]

**Your rights in connection with personal data**

You may be interested to know of certain rights that you have in connection with your personal data. In particular, you have the right to correct the personal data that we hold about you or restrict the processing of your personal data under certain circumstances. You may also, under certain circumstances, have the right to object to the processing or to request erasure of your personal data.

You also have the right to make a complaint to the data protection supervisory authority in the UK, the Information Commissioner. For further information, see the Information Commissioner's Office website at <https://ico.org.uk/concerns/>. Alternatively, you may seek judicial remedy.

We can confirm the following in respect of the data existing on the date your request was made:

1. **THE PURPOSES FOR WHICH THE PERSONAL DATA IS PROCESSED**

 [LIST OF PURPOSES]

1. **THE CATEGORIES OF PERSONAL DATA CONCERNED**

[LIST OF CATEGORIES OF PERSONAL DATA]

1. **THE RECIPIENTS OR CATEGORIES OF RECIPIENTS TO WHOM THE PERSONAL DATA HAS OR MAY HAVE BEEN DISCLOSED**

[LIST OF RECIPIENTS (BY NAME OR GENERIC CLASS) TO WHOM DATA DISCLOSED]

[LIST OF RECIPIENTS IN COUNTRIES OUTSIDE THE EEA OR INTERNATIONAL ORGANISATIONS]

1. **SAFEGUARDS IN PLACE IN RELATION TO PERSONAL DATA TRANSFERRED TO THIRD COUNTRIES OR TO AN INTERNATIONAL ORGANISATION**

[STATE WHETHER THERE IS AN ADEQUACY DECISION FROM THE EU COMMISSION IN RESPECT OF THIRD COUNTRY OR INTERNATIONAL ORGANISATION]

[LIST OF SAFEGUARDS IF NO ADEQUACY DECISION]

1. **THE PERIOD FOR WHICH PERSONAL DATA WILL BE STORED OR CRITERIA USED TO DETERMINE THAT PERIOD**

[LIST OF CATEGORIES OF DATA AND PERIOD STORED OR CRITERIA USED TO DETERMINE THAT PERIOD]

1. **ANY INFORMATION AVAILABLE TO [EMPLOYER] ON THE SOURCE OF THE DATA**

[IDENTIFY SOURCES OF DATA HELD]

[Some names and identifying particulars have been deleted to protect the identity of third parties.]

1. **THE EXISTENCE OF ANY AUTOMATED DECISION-MAKING**

[IDENTIFY ANY AUTOMATED DECISION-MAKING, INCLUDING PROFILING, AND ANY MEANINGFUL INFORMATION ABOUT THE LOGIC INVOLVED, ANY SIGNIFICANCE OR ENVISAGED CONSEQUENCES]

We have done our best to respond to your request and hope that you have found our approach helpful. You will see that when providing copies of personal data, we have sometimes gone beyond what is required in that not all of the information provided, strictly speaking, constitutes personal data relating to you. Please do not hesitate to contact us if you have any questions about the contents of this letter.

Yours sincerely,