Title:	**Ensuring Lawfulness, Fairness and Transparency when Processing Personal Data Standard Operating Procedure**		
Version:	**1.1**	**Effective Date**	**21 April 2020**
Summary:	Describes the various procedures for ensuring that personal data is handled in a lawful, fair and transparent manner under the GDPR and Data Protection Act 2018		

When using this document please ensure that the version you are using is the most up to date by checking on the University's online document system http://documents.manchester.ac.uk/list.aspx for any new versions.

1 Background and purpose

Article 5 of the European General Data Protection Regulation (GDPR) 2018 states that "Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject". The University must ensure that it treats all personal information that it processes in line with this legal expectation.

This Standard Operating Procedure (Procedure) is designed to set out the processes involved when the University processes personal data to ensure that processing is carried out in a lawful, fair and transparent manner.

Adherence to this Procedure ensures that staff adhere to established procedures when processing personal data, in order to:

- ensure that the University's processing is fair, i.e. that it is processed in such a way that the processing does not fall outside the reasonable expectations of the data subject;
- ensure that the University's processing is transparent, i.e. that sufficient information is given to each data subject when their data is collected and processed;
- ensure that the University's processing is lawful, i.e. that it meets a condition of processing as defined in Article 6 of the GDPR;
- minimise the risk of data subject complaints to the Data Protection Regulator;
- minimise the risk of the University committing a technical breach of data protection legislation, and the reputational and financial consequences thereof;
- ensure that all areas of the University are familiar with their responsibilities when processing personal data.

2 Definitions and scope

2.1 Definitions

- **Data Subject** refers to any identifiable living individual about whom the University processes personal data.
- **Data Controller** refers to the body, in this case the University, which alone or jointly with others determines the purposes and means of the processing of personal data. Most of the data which the University holds about individuals is processed on a controller- subject relationship, so subject rights apply.
- **Personal Data** means any information relating to an identified or identifiable natural person, whether held in a structured or unstructured form.

- **Special Category Data** means any personal data which refers to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and sex life or sexual orientation. It also applies to genetic data and biometric data for the purpose of identification of an individual. Personal data relating to criminal convictions and offences, allegations of criminal offences and court proceedings must also be treated as special category data for processing purposes.
- **Data Processing** means any operation performed on personal data by automated or manual means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, alignment or combination, restriction, erasure or destruction.

2.2 Scope

This Procedure applies to all processing of personal data by the University including the initial collection of such data. This could potentially involve any member of staff at the University, but will particularly impact on staff who collect personal data.

2.3 Research data

This Procedure specifically applies to personal information processed by the University for administrative purposes. Personal information processed for research processes also needs to be processed in a lawful, fair and transparent manner and the general principles are the same, but the specific procedures to ensure this will often differ from those outlined in this SOP. Research data specific guidance will be provided in a separate document.

3 Procedure and responsibilities

The Information Governance Office (IGO) is responsible for providing advice and guidance on ensuring that processing is lawful, fair and transparent. The IGO will in particular ensure that privacy notices are consistent across the institution and that local privacy notices are complete and compatible. The Head of Information Governance is ultimately accountable for the responsibilities of the IGO.

It is the responsibility of individual members of staff who process personal data to ensure that they are aware of the privacy notice under which the personal data which they are using was collected, and any wider confidentiality or legal restrictions relating to the data, and that they do not process the data in a manner which is inconsistent with these requirements.

3.1 Fair and transparent processing

Whenever the University obtains or collects personal data from an individual it must supply certain information to that individual in the form of a privacy notice. This information consists of:

- The identity of the data controller (usually the University);
- The identity of any representative of the data controller (ie any organisation which is processing data on our behalf);
- The contact details of the University's Data Protection Officer;
- The purpose(s) for which the data are intended to be processed (See the Standard Operating Procedure on Processing Purposes);
- The legal basis for the processing (ie the condition of processing outlined in 3.4 below);
- Any third parties to whom the data will be passed or disclosed;

- Any third country or international organisation to which the data will be transferred, and the legal basis for that transfer;
- An indication of the length of time for which data will be kept or the criteria by which this is decided;
- The existence of the data subjects' rights in relation to the data (see the Standard Operating Procedure on Data Subject Rights);
- The Data Subject's right to lodge a complaint with the national data protection regulator;
- The existence of any statutory or contractual requirement for the data subject to supply the data where applicable;
- The existence of automated decision making, including profiling, based on the data where applicable. If this applies please contact the Information Governance Office for further advice;
- Any other information that is necessary to enable the processing to be fair.

This information must be provided whenever new data is collected from an individual or whenever personal data already held by the University is used for a new purpose.

The privacy notice must be supplied in a form which is easily accessible to the data subject, either directly to them (preferably in writing) or through the University website.

3.2 Existing Privacy Notices

The University has created a number of privacy notices to cover its major data collections and areas of processing. These notices cover:

- DDAR Alumni
- HR – Staff
- Registered Students
- Website users
- Research participants
- Student enquirers, applicants and offer holders
- Widening participation

Any new or existing data collections which are not covered by these notices must either be added to the relevant one (please contact the Information Governance Office to arrange this) or, if they are one off collections or are unsuitable for inclusion in any of the above, a new privacy notice will need to be written. New privacy notices must include all the elements listed in 3.1 above and must be approved by the Information Governance Office before publication. A privacy notice template can be found at Appendix A of this procedure.

The information contained within a privacy notice must be concise, transparent, intelligible, and easily accessible and it must use clear and plain language.

3.3 Reviewing and updating privacy notices

All University privacy notices must be regularly reviewed, and where necessary updated. The Information Governance Office and the relevant area responsible for the processing must review central privacy notices annually. Any ad-hoc updates or additions to a centrally identified privacy notice need to be approved by the Data Protection Officer.

Local privacy notices should be reviewed by the owner of the processing activity covered by the notice . If the IGO is consulted a record will be made of the update.

3.4 Data obtained from a third party

If the University obtains personal data from a third party, rather than directly from the person(s) concerned, the University must, if practical, provide the data subjects with appropriate information as per the privacy notice list above.

There will be some circumstances where it will not be possible to contact data subjects directly, such as when to do so would constitute a disproportionate effort for the University. In these cases the Information Governance Office must be contacted for guidance.

3.5 Lawful processing

In addition to processing in a fair and transparent manner, the University must also treat data lawfully.

In practice this means that all processing of personal data undertaken by the University must meet one of a set of six conditions which are set out in Article 6 of the GDPR. The conditions are:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

In practice the University will in many cases rely on one or other of the last two of these. A large number of activities which the University carries out are either in the public interest (research, teaching etc) or are a legitimate interest of the University in the context of its status as a business (certain student administration functions, alumni relations, fund raising etc).

Most personal data about members of staff will be processed in the performance of a contract, as will some student data. Some personal data relating to staff and students may be processed under the vital interests condition or in compliance with legal obligations.

Consent may be used for the processing of some personal information, particularly in regards to marketing and automated processing of data. Consent must not be used as a condition if another condition is available as consent is easily withdrawn by the data subject. In addition, consent is not valid if there is a power imbalance between the data controller and data subject. There is an “imbalance in the relationship” between an individual member of staff or a student and the University and so it would often be hard to prove that consent has been “freely given”, thus if possible consent must not be used as a condition of processing for staff or student data.

If it is not clear which condition applies to the processing of any set of personal information held by the University, please contact the Information Governance Office for advice.

The processing of special category or criminal convictions data requires the fulfilment of a second condition from Article 9 and Schedule 1 of the Data Protection Act 2018, in addition to the Article 6 condition listed above. The processing of special category data is covered in a separate operating procedure.

3.6 Other unlawful processing

In addition to meeting one of the conditions in Article 6 of the GDPR, processing must also be carried out in accordance with other relevant UK law.

Most commonly this will apply when there are considerations of confidentiality to take into account. Information which the University receives or holds which were provided to it under an expectation of confidentiality must not generally be provided to third parties in a manner which would breach that confidentiality.

This is not an easy test to apply, and does not mean that any data can be excluded from the Act if it has "confidential" written on it. Data must be genuinely confidential, an expectation of confidentiality must have existed when it was provided to the University and its unauthorised disclosure and use must have the potential to cause damage or distress to either the data subject or another person before disclosure could be considered a breach of confidence and thus unlawful.

Information disclosed in breach of contract, copyright, the Computer Misuse Act 1990 or the Human Rights Act 1998 would be further examples of unlawful processing of personal data.

4 Monitoring compliance with the Procedure

Heads of School, Directors or equivalent are accountable for ensuring that all staff within their area act in accordance with this Procedure.

4.1 Audit

Evidence of compliance with this procedure will be audited periodically.

4.2 Reporting

The Head of Information Governance will report on this Procedure to the Information Governance Committee.

5 Review of Procedure

This Procedure will be reviewed at least every two years or when significant changes are required.

6 Contact list for queries related to this procedure

Role	Name	Telephone	Email
Head of Information Governance	Tony Brown	0161 306 2106	Tony.brown@manchester.ac.uk

Role	Name	Telephone	Email
Head of Data Protection (DPO)	Alex Daybank	0161 306 2473	Alex.daybank@manchester.ac.uk
Deputy Head of Information Governance	Barbara Frost	0161 275 2122	Barbara.frost@manchester.ac.uk

Version control

Version	Date	Reason for change
1.0	March 2019	Creation
1.1	May 2020	Added section 3.3 about reviewing and updating privacy notices

Document control box	
Procedure title:	**Ensuring Lawfulness, Fairness and Transparency when Processing Personal Data Standard Operating Procedure**
Date approved:	21 April 2020
Approver:	Information Governance Committee
Version:	1.1
Supersedes:	N/A
Previous review dates:	
Next review date:	12 March 2021
Related Statutes, Ordinances, General Regulations:	• Ordinance XIV Intellectual Property Rights (IPR), Data Protection and the Use of Information Systems • University General Regulation XV Use of Information System
Related policies:	• Information Security Policy http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6525 • Data Protection Policy http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14914
Related procedures:	• https://www.staffnet.manchester.ac.uk/igo/policy-procedures/
Related information:	
Procedure owner:	Head of Information Governance

University of Manchester: Privacy Notice – [title related to specific area of processing/data subject group]

1. Introduction

[Content – who does this apply to and what is it for]

2. What is personal data (also known as personal information)?

Personal information means any information which relates to or identifies you as an individual and includes opinions about you or information which may not explicitly identify you (e.g. where your name has been removed) but which nevertheless does identify you if it is combined with other information that is readily available. [Fixed text but can be added to]

3. How does this notice relate to other information about data protection?

[How does this link to the other notices e.g. *If individual is also a research participant or student they should be reminded about these other notices. Remove this section if it is not applicable]*

4. Who will process my personal information?

This notice explains how the University of Manchester will hold and process your personal information [add text for the specific local purpose, including any limits on access to the personal data, for example to a research group, School or role]

5. What personal information will you process?

The University needs to collect, maintain and use personal data relating to or about you. This consists of:

[Content – list all types of personal data processed e.g. names, contact details, copies of passports etc.]

6. What is the purpose of the processing under data protection law? [legal basis]

[Fixed text] We will only use your personal information when the law allows us to do so by providing us with a legal basis or valid condition. We will use your personal information in the following circumstances:

[List each Article 6 legal basis identified: consent, performance of a contract, legal compliance, vital interests, a public interest task (specify), legitimate interests]

[If you are relying on the legitimate interests of the University you should specify what these are in the case of this notice]

7. Examples of the processing to be undertaken

[Content – any further detail or clarification about how the processing will take place, why etc. Remove this section if not relevant]

8. Special Category Data

[Fixed text. Add where applicable – The University will also process some information about you that is considered more sensitive and this is referred to as 'special category' personal data in the General Data Protection Regulation and Data Protection Act 2018. When we process this type of information we are required to apply additional protections. [Special category personal data is defined as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life and sexual orientation, genetic data and biometric data which is processed to uniquely

identify a person. In the UK this also includes any personal information relating to criminal convictions. You should specify here which type/s of special category data you will be processing]

9. How will you process my Special Category personal information?

[Fixed Content to add where applicable] – We will only process special category personal information in certain situations in accordance with the law. On this occasion we are relying on

List Article 9 conditions identified: explicit consent, our obligations as an employer, your vital interests, a substantial public interest purpose (specify), occupational health, scientific or historical research or archiving in the public interest]

Other Article 9 conditions such as data which is already in the public domain or for the establishment or defence of a legal claim may be relied on by the University but will not generally be included in a privacy notice. Please contact the IGO for advice.

Where the University has a legal or statutory requirement to collect certain data you should also specify this, and provide the possible consequences of an individual not supplying the data.

10. Who will my personal information be shared with?

[Content – List other organisations and context/purpose of the sharing if this occurs; if not state that it will not be]

11. Will my data be transferred to another country?

[If data is to be transferred to another country within the EEA, including as a result of cloud storage, say so here. If the data is to be transferred outside of the EEA please consult with the IGO]

12. What are my rights in connection with my personal information?

Under certain circumstances, by law you have the right to:

12.1 Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

12.2 Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

12.3 Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing.

12.4 Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

12.5 Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

12.6 Request the transfer of your personal information to another party.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

If you would like to exercise any of these rights, you should contact the University Data Protection Officer, by email: dataprotection@manchester.ac.uk. Alternatively you can write to The Information Governance Office, University of Manchester, Christie Building, Oxford Road, Manchester M13 9PL. Further information about your rights is available from the University's data protection web pages.

13. How long is my information kept for?

[Either this text - We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for. Details about how long different types of information are retained by the University is published here

Or explain specific retention period]

14. Who can I contact if I have any queries?

[Fixed text] If you have any questions about how your personal information is used by the University as a whole, or wish to exercise any of your rights, please consult the University's data protection webpages at [insert link]. If you need further assistance, please contact the University's Data Protection Officer (dataprotection@manchester.ac.uk).

15. How do I complain?

Fixed text] if you are not happy with the way your information is being handled, or with the response received from us, you have the right to lodge a complaint with the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow, SK9 5AF (https://ico.org.uk).

16. Are changes made to this notice?

[Fixed text] We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information. [Insert date of notice]

Automated decision making- please contact the IGO if the data will be used to make automated decisions about individuals, as this will need to be included in the privacy notice.