

Middlesex University Appropriate Policy Document

|  |  |
| --- | --- |
| Policy owner | Legal Team |
| Author if different from above | N/A |
| Version | Version 2  |
| Last Review Date | 01/09/2022 |
| Next Review Due | March 2024, unless circumstances require an earlier review |

**Approvals**

|  |  |
| --- | --- |
| **Committee / Individual** | **Date** |
| Information Governance Group (IGG) | Approved by the Information Governance Group on 28 Nov 2022 |

Special categories of personal data and criminal convictions data Appropriate policy document

**How we protect special category and criminal convictions data**

This ‘appropriate policy document’ sets out how we will protect special categories of personal data and criminal convictions data. (See Appendix A below).

We have this document in place to explain the basis on which we process special category and criminal convictions data and to demonstrate that our processing is compliant with principles set out in data protection legislation.

1. **The special category and criminal convictions data that we process**

The special category data that we process can be found in our privacy notices.

Generally, when we are processing special category or criminal convictions data, it is on the basis that the individual has given explicit consent to the processing. This document sets out the other circumstances where we process such data and the conditions that we rely on under Schedule 1 of the Data Protection Act 2018.

Reference to **‘data’** in the remainder of the document means special category data and / or criminal convictions data.

 **Schedule 1 Part 1:** employment, social security and social protection: we process the

**data** for the purposes of performing or exercising our obligations or rights under employment law, social security law or the law relating to social protection. This includes our health and safety responsibilities as well as other employment rights and obligations.

**Schedule 1 Part 1 -** health or social care purposes: we will process the **data** for the purpose of assessing the working capacity of our employees so that we can safeguard their welfare. This means that we can provide any adjustments necessary for our staff and implement any changes advised by our occupational health provider.

**Schedule 1 Part 1 - research:** we will process the **data** for the purpose of our research, where such research is in the public interest.

**Schedule 1 Part 2 - equality of opportunity or treatment:** we will process certain categories of **data** for the purposes of monitoring, promoting and maintaining equality of opportunity and treatment of our staff and students, for example, in relation to our Equality Act duties and our work to widen participation in Higher Education. This **data** is limited to racial or ethnic origin, religious or philosophical beliefs, health and sexual orientation. Most of this **data** will be collected with the explicit consent of the individual.

**Schedule 1 Part 2 - preventing or detecting unlawful acts:** this condition applies when we process **data** about criminal convictions and offences, for example, as part of the recruitment of staff or the admissions process for applicants to certain courses, such as social work or education. We have a duty to do so to safeguard our students, staff and others and, in line with Part 3 of Schedule 1, we will only process this **data** with consent and only it if it is relevant to the role, position or course.

**Schedule 1 Part 2 - counselling:** we may need to process **data** in order to provide confidential counselling, advice or support to our staff and students. Usually, we will have consent for this purpose but that may not be possible in some instances, for example where the individual cannot give consent.

**Schedule 1 Part 2 – safeguarding of children and of individuals at risk:** we may need to process **data** in order to meet our safeguarding responsibilities, for example, to protect an individual at risk from physical, mental or emotional harm.

**Schedule 1 Part 3 – criminal convictions and offences data:** we will process such **data** with the consent of the individual or, for example, where it is necessary to protect the vital interests of a person, it is necessary for legal proceedings or advice, or it is necessary for reasons of substantial public interest (such as preventing or detecting unlawful acts or safeguarding individuals in relation to discipline proceedings).

**Schedule 1 Part 3 – legal proceedings:** we will process such **data** where it is necessary for obtaining legal advice, or in connection with legal proceedings (including prospective proceedings) or for the purpose of establishing, exercising or defending legal rights.

1. **Accountability**

The University has to be able to demonstrate that we are accountable for the personal data we process, that we are responsible for complying with our obligations under data protection legislation, and that we can demonstrate that compliance.

To demonstrate our compliance and accountability we will:

* Document our processing activities and keep these records up to date;
* Keep a record of personal data breaches;
* Have appropriate contractual arrangements in place with organisations that process personal data on our behalf;
* Complete a Data Protection Impact Assessment for any high-risk personal data processing; and
* Implement processes to make sure that personal data is only collected, used or handled in a way that is compliant with data protection legislation.
1. **Procedures for ensuring compliance with the principles**

When processing data, we meet the requirements of the data protection principles, as set out in data protection legislation:

**Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.**

To stay compliant with this principle we will:

* Make sure that we only process personal data lawfully and where we have identified a clear lawful basis to do so;
* Process personal data fairly and make sure that data subjects are not misled about the purposes of any of our processing;
* Provide data subjects with full privacy information so that we are transparent in how and why we process personal data.

**Principle 2 - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.**

To stay compliant with this principle we will:

* Only collect personal data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in a privacy notice;
* Not use personal data for purposes that are incompatible with the original purpose.

**Principle 3 - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.**

To stay compliant with this principle we will:

* Ensure that we do not collect **data** that we do not need and will only collect the minimum personal data that is necessary for the purpose for which it is collected.
* We will ensure that the **data** we do collect is adequate for our purpose and relevant.

**Principle 4 - Personal data shall be accurate and, where necessary, kept up to date.**

To stay compliant with this principle we will:

* Make sure that the personal data we hold is accurate;
* Ensure there are processes for us or individuals to correct and keep data up to date where necessary.

**Principle 5 - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.**

To stay compliant with this principle we will:

* Only keep personal data in identifiable form as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so.

**Principle 6 - Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against personal data breaches.**

To stay compliant with this principle we will:

* Make sure that there are appropriate organisational and technical measures in place to protect personal data.
1. **Retention and erasure of personal data**

As part of our ongoing compliance obligations we will make sure that data is only retained for as long as is necessary and we will publish information about the retention periods for different categories of data. Data subjects have access to information about how their data will be handled and how long it will be retained.

Where we no longer require special category or criminal convictions data for the purpose for which it was collected, we will delete it, put it beyond use or make it permanently anonymous.

1. **Further information**

If you require further information or have a question about our handling of special category or criminal convictions data, you can contact the University’s Data Protection Officer.

**Appendix A** **- Special Category and Criminal Offence Data**

Special categories of personal data and criminal convictions data Appropriate policy document

 **What are the ‘special categories of personal data’?**

While all types of personal data require secure and proper handling, data protection legislation specifies some types of personal data which are likely to be more sensitive and which require a greater level of security and governance. These are called ‘special categories of personal data’.

We process these categories of personal data for a limited range of purposes and only where necessary. These types of data are listed below:

* personal data revealing **racial or ethnic origin;**
* personal data revealing **political opinions;**
* personal data revealing **religious or philosophical beliefs;**
* personal data revealing **trade union membership;**
* **genetic data;**
* **biometric data** (where used for identification purposes);
* data concerning **health;**
* data concerning a person’s **sex life;** and
* data concerning a person’s **sexual orientation.**

 **What is ‘criminal conviction data’?**

We also process some criminal offence data (although we only do this for limited purposes). This type of data includes information about criminal allegations, convictions, and proceedings. It also includes information linked to security measures and restrictions, such as bail conditions, cautions, and restraining orders, and less obvious types of information, such as personal data relating to witnesses, victims of crime, and the absence of any criminal record or convictions, and details of allegations (proven and unproven). It may also include information about civil measures which may lead to a criminal conviction if not adhered to.

**How do we process these types of data and remain compliant with legislation?**

Due to the sensitive and impactful nature of these categories of data, we need to have additional security measures in place to keep it safe. We take steps to stop this data being lost, stolen or disclosed inappropriately, and we make sure that the correct controls are in place before we start to process the data. For example, we may consider completing a Data Protection Impact Assessment, or we may use differing handling methods as appropriate. Other measures include breach management, contract reviews, up to date record keeping and reviews of data protection legislation in advance of new processing.

In addition to these measures we must also identified a specific reason for processing each of these types of data, when we process them. We must also meet the conditions set out in legislation to ensure our processing is lawful.

The conditions that we, as a Data Controller, need to meet are detailed in the UK General Data Protection Regulation (‘UK GDPR') and the Data Protection Act 2018. In the UK GDPR there are ten conditions for processing special categories of personal data in Article 9, and in the Data Protection Act 2018 they can be found detailed in Schedule 1, where you can also find details of the conditions for processing criminal conviction data.

Not all of the conditions for processing which are listed out in the legislation apply to us, so we do not use all of them. Those that we commonly use are listed below:

* The lawful basis that we often rely on to process such data is **consent.** Put simply, consent means **“any freely given, specific, informed and unambiguous indication”** of an individual’s wishes / agreement to the processing of their personal data;
* We also process special categories of data for **employment, social security and social protection purposes;**
* For **health or social care purposes;**
* To ensure **equality of opportunity or treatment;**
* For the **prevention or detection of unlawful acts;**
* So that we can **protect the public against dishonesty;**
* So that facilitate the provision of **counselling** and other support;
* So that we can manage **legal claims** and proceedings.