

## Scope

We recognise our duties to protect Special Category Personal Data as defined in Article 9 of GDPR:

- a) Personal data revealing a person's:
- racial or ethnic origin
  - political opinions
  - religious or philosophical beliefs
  - trade union membership
- b) Processing of:
- genetic data
  - biometric data
  - health data
  - sex life data
  - sexual orientation data

In addition, we recognise the sensitivity and need to protect personal data relating to individuals' criminal convictions and offences.

All processing of personal data, including Special Category Data, is subject to our Data Protection Policy and all related procedures for data handling.

Negligent or malicious non-compliance with this policy may be dealt with through the disciplinary process.

## Related Documentation

- Information Asset Register (internal document)
- [Data Protection Policy](#)

## Before processing:

- A Data Protection Impact Assessment must be completed. This must be retained and regularly reviewed and revised as necessary for the duration of the processing
- Appropriate measures, including technical and organisational measures, must be implemented to ensure appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. These must be regularly reviewed and revised as necessary for the duration of the processing, for example by updating the Data Protection Impact Assessment, and records of those reviews must be retained
- Those who are to have access to this data must have completed appropriate data protection training before processing the data
- A clear and transparent Privacy Notice must be provided to Data Subjects which includes a clear indication of how long the Personal Data will be retained and when it is likely to be erased. The Information Rights team must be consulted in relation to the Privacy Notice
- A record in the Information Asset Register must be created and maintained which includes the following information:

- (a) the relevant condition in the Data Protection Act 2018 which is relied on
- (b) the legal basis for processing
- (c) whether the data is retained and erased in accordance with the retention periods set out in the Information Asset Register record, and if it is not, the reasons for this.

## **Processing of special category data to which this applies:**

- Any processing of criminal convictions data, and any processing of special category data which falls under Schedule 1 of the Data Protection Act 2018, section 1 and Parts 2 and 3.
- A summary of the likely purposes is provided below:
  - Where the processing is necessary for obligations or rights that we have in law in connection with employment, social security or social protection (Sch 1.1)
  - Where the processing is necessary for sing is necessary (no reasonable alternative) for a reason of substantial public interest, i.e.
    - Sch1.6 For a function conferred on the OU by law, or for the exercise of a government function
    - Sch1.8 Identifying or keeping under review equality of opportunity or treatment (paragraph 8)
    - Sch1.9 Promoting or maintaining diversity in the racial and ethnic origins of individuals who hold senior positions in the organisation
    - Sch1.11 For the exercise of a function protecting the public from dishonesty, malpractice, unfitness, incompetence or maladministration
    - Sch1.12 Regulatory requirements relating to unlawful acts and dishonesty, malpractice or other seriously improper conduct
    - Sch1.14 The purposes of preventing fraud and consisting of disclosures by an “anti-fraud organisation”
    - Sch1.15 A disclosure of suspicion of terrorist financing or money laundering
    - Sch1.16 Support by a not-for-profit body which provides support to individuals with a particular disability or medical condition
    - Sch1.17 The provision of confidential counselling, advice or support or of another similar service provided confidentially
    - Sch1.18 The safeguarding of children and of individuals at risk
    - Sch1.19 Safeguarding of economic well-being of certain individuals
    - Sch1.20 Insurance purposes
    - Sch1.22 The political activities of a political party
    - Sch1.23 Elected representatives responding to requests
    - Sch1.24 Disclosure to elected representatives working on behalf of a data subject at their request
    - Sch1.27 and 28 Anti-doping and Standards of behaviour in sport
    - Sch1.29 to 37 All processing of personal data relating to criminal convictions and offences

All references relate to the Data Protection Act 2018 Schedule 1

See the Information Asset Register for specific information about the special category data processed.

# Compliance with the Principles

Below is a summary of our procedures for special category data compliance with the principles under Article 5 of GDPR.

Data Protection Principle	Procedures for securing compliance	Relevant documents
<i>a) processed fairly, lawfully and transparently</i>	<p>All use of Special Category Data will be</p> <ul style="list-style-type: none"> <li>subject to clear justification under Article 6 and 9 of GDPR</li> <li>described clearly and precisely in privacy notices available to data subjects</li> </ul>	<p>Data Protection Policy</p> <p>Information Asset Register</p>
<i>b) collected for specific purposes and not used for incompatible purposes</i>	<ul style="list-style-type: none"> <li>Staff will be trained to ensure that they do not use personal data for purposes other than those authorised by the organisation.</li> <li>Business procedures will document how personal data will be used for specific processes</li> <li>Data Protection Impact Assessments document any additional measures to ensure data is not used for incompatible purposes</li> </ul>	<p>Data Protection Policy</p> <p>Staff Training materials</p> <p>Information Asset Register</p> <p>Data Protection Impact Assessments</p>
<i>c) adequate, relevant and limited to what is necessary</i>	<ul style="list-style-type: none"> <li>Data Protection Impact Assessments ensure only data relevant to the business requirement is captured, held and made available.</li> <li>Staff will be trained to record only the minimal necessary personal data for business needs.</li> </ul>	<p>Data Protection Impact Assessments</p> <p>Staff Training Materials</p> <p>Individual business procedures/training materials</p>
<i>d) accurate and, where necessary, kept up to date</i>	<ul style="list-style-type: none"> <li>Data subjects can update certain data themselves</li> <li>The relevant teams check the accuracy of data with data subjects regularly.</li> </ul>	<p>Individual business procedures</p>
<i>e) retained no longer than necessary</i>	<ul style="list-style-type: none"> <li>Heads of Unit (Information Asset Owners) have the responsibility for ensuring the appropriate retention periods are applied to personal data</li> <li>Where systems do not have the functionality to automate disposal, staff have a scheduled task to manually delete time-expired data.</li> <li>Retention periods are noted in the Information Asset register</li> </ul>	<p>Data Protection Policy</p> <p>Records Retention Schedule</p> <p>Information Asset Register</p>
<i>f) kept securely</i>	<ul style="list-style-type: none"> <li>All use of personal data is subject to our Information Security Policy and related controls.</li> <li>Staff are trained to be particularly aware of the additional risks to Special Category Data</li> <li>Relevant teams have appropriate data-handling processes and guidance.</li> </ul>	<p>Information Security Policy</p> <p>Staff Training Materials</p> <p>Individual business procedures/training materials</p>