



# Special Category and Criminal Offence Data Policy

## Contents

Overview and Purpose.....	2
Scope.....	3
Policy.....	3
Lawful Bases.....	3
Retention .....	4
Related Legislation, Regulations and Policies.....	5
Breach of Policy.....	6

## OVERVIEW AND PURPOSE

1. This policy is concerned with how Kingston University (the University) handles personal data that is deemed to be special category (sensitive) or related to criminal convictions and offences, as defined by the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). These classes of information pose additional potential risks to data subjects, including students and staff, and as such must be handled with particular care.
2. See below a table of definitions of special category and criminal offence data

Special category personal data	Criminal convictions and offences data
Personal data relating to: <ul style="list-style-type: none"> <li>• racial or ethnic origin</li> <li>• political opinions</li> <li>• religious or philosophical beliefs</li> <li>• trade union membership</li> <li>• genetic data and/or biometric data for the purpose of uniquely identifying a person</li> <li>• health</li> <li>• sex life or sexual orientation.</li> </ul>	Personal data relating to: <ul style="list-style-type: none"> <li>• the alleged commission of offences by the data subject</li> <li>• proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing</li> <li>• unspent convictions and risk assessments.</li> </ul>

3. The UK GDPR states that data controllers must have a legal basis for processing personal data plus an additional condition for special category or criminal offence data. The DPA 2018 provides further information on the legal bases for processing and the additional safeguards that need to be in place to protect special category or criminal offence data. This includes having an ‘appropriate policy document’ in place, which this policy constitutes. The sections below provide the information required by the appropriate policy document with regards to special category or criminal offence data.
4. Article 5 of the GDPR contains six principles relating to the processing of personal data, which require that personal data must be:
  - processed lawfully, fairly and transparently
  - collected for a specified purpose
  - limited to what is necessary in relation to the purpose for processing
  - accurate and up to date
  - retained for no longer than is necessary
  - processed in a manner that ensures appropriate security.

## Special Category and Criminal Offence Data Policy

5. In addition, organisations have an accountability requirement to demonstrate their compliance with the principles. This means keeping accurate records about the personal data that the University processes, the reasons for the processing, who it is shared with and how long it is kept.

### SCOPE

6. This policy applies to all staff, students and affiliates.
7. This policy applies to all Special Category and Criminal Offence data processed by the University.

### POLICY

#### LAWFUL BASES

8. Under Article 6 of the UK GDPR the University relies on the following legal bases for the lawful processing of special category and criminal offence data:
  - (a) consent
  - (b) contract
  - (c) legal obligation
  - (d) vital interests
  - (e) public task
  - (f) legitimate interests.
9. In addition, under Articles 9 and 10 of the UK GDPR and Schedule 1 of the DPA 2018 the University relies on the following conditions for processing special category or criminal offence data:

## Special Category and Criminal Offence Data Policy

Special category personal data	Criminal convictions and offences data
<p>Article 9:</p> <ul style="list-style-type: none"> <li>(a) Explicit consent</li> <li>(c) vital interests</li> <li>(e) made public by the data subject</li> <li>(f) legal claims</li> <li>(g) substantial public interest</li> <li>(j) archiving, research and statistics</li> </ul> <p>Schedule 1 Part 1 Employment, health and research:</p> <ul style="list-style-type: none"> <li>1. Employment, social security and social protection</li> <li>3. Public health</li> <li>4. Research etc.</li> </ul> <p>Schedule 1 Part 2 Substantial public interest:</p> <ul style="list-style-type: none"> <li>6. Statutory and government purposes</li> <li>8. Equality of opportunity or treatment</li> <li>16. Support for individuals with a particular disability or medical condition</li> <li>20. Insurance</li> </ul>	<p>Schedule 1 Part 1 Employment, health and research:</p> <ul style="list-style-type: none"> <li>1. Employment, social security and social protection</li> </ul> <p>Schedule 1 Part 2 Substantial public interest:</p> <ul style="list-style-type: none"> <li>18. Safeguarding of children and of individuals at risk</li> <li>10. Preventing or detecting unlawful acts</li> <li>11. Protecting the public against dishonesty</li> <li>20. Insurance</li> </ul> <p>Schedule 1 Part 3 Additional conditions relating to criminal convictions:</p> <ul style="list-style-type: none"> <li>29. Consent.</li> <li>30. Vital interests</li> <li>32. Personal data in the public domain</li> <li>33. Legal claims</li> </ul>

10. Staff within the University and those working in any capacity for the University who collect, store, use, transfer and delete such personal data should ensure that they comply with this and the related data protection policies as well as other relevant legislation such as the Equality Act 2010. They should also ensure that any locally held policies and procedures take account of and refer to this policy. This will include the data processing audit documents that constitute the record of processing activity.
11. It is the responsibility of University teams that process or intend to process special category or criminal offence data to ensure that both the UK GDPR legal basis and the DPA 2018 conditions for processing are recorded and kept up to date in their data processing audit documentation as a record of this processing activity. Any planned changes (including new special category or criminal offence data) to processing activity must be communicated to the University's Data Protection Officer at [dataprotection@kingston.ac.uk](mailto:dataprotection@kingston.ac.uk) so that this policy document can be amended if necessary.

### RETENTION

12. Special category or criminal offence data must only be retained for as long as the processing is necessary and during that time it must be securely held with access

## Special Category and Criminal Offence Data Policy

limited to authorised users only. In most cases the duration will be in accordance with a retention period set by regulation or law or for a specific business process. University staff must familiarise themselves with both the University's Retention Policy and Retention Schedule in the [Information regulations](#) section of the website.

13. This policy document applies and remains in place for as long as the University processes special category or criminal offence data and for a minimum period of six months after the processing ends. It will be reviewed regularly to ensure it remains up to date.
14. Staff responsible for processing such data must inform the University's Data Protection Officer at [dataprotection@kingston.ac.uk](mailto:dataprotection@kingston.ac.uk) before or as soon as possible after any changes are made, for example when:
  - a planned or amended business process will start to collect, store, use, transfer or delete special category or criminal offence data for the first time
  - an existing legal basis for the processing is altered (for example, changes to a regulation or law that affects the processing)
  - the process workflow will be altered significantly
  - there are plans to use a new supplier
  - there are plans to transfer the data overseas
  - the technology used to process the data will be changed (for example, a new software company is introduced)
  - there is a real or perceived change to the security methods protecting the processing (for example, a plan to expand access permissions)
  - special category or criminal offence data will no longer be processed.
15. The University must provide the appropriate policy document and supporting information to the Information Commissioner's Office on request. A copy of this policy will also be available online. Therefore, the ongoing accuracy of the information held in the data protection audits is important for ensuring the policy remains up to date.

## RELATED LEGISLATION, REGULATIONS AND POLICIES

16. Related legislation:
  - UK Data Protection Act 2018
  - UK General Data Protection Regulation
17. This policy should be read in conjunction with other relevant University policies and documents which can be viewed in the [Information regulations](#) section of the University website.

## BREACH OF POLICY

18. Anybody handling personal data agrees to abide by the terms of any applicable policies. Users who are found to have breached the terms of relevant policies may be subject to warnings, verbal and written. In serious cases individuals will be subject to the University's disciplinary procedures, and possible legal action.