University of York

Special Categories of Personal Data and Criminal Offence Data Policy

We process special category data and criminal offence data for the purposes laid out in our Charter and Statutes. At all times, we process both categories of data in accordance with the requirements of Articles 9 and 10 of the UK General Data Protection Regulation ('GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Special category data

Special category data is defined at Article 9 of the UK GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

Criminal offence data

Article 10 of the UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11 (2) of the DPA 2018 specifically confirms that this includes data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

This policy document

Some of the DPA 2018 Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 of the UK GDPR and policies regarding the retention and erasure of such personal data.

This document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

In addition, it provides some further information about our processing of special category and criminal offence data where a policy document is not a specific requirement. The information supplements our existing privacy notices.

Description of data processed

We process special category data of our employees to fulfil our obligations as an employer. This includes information about health and wellbeing, ethnicity and membership of any trade union. Further information can be found in this policy document and our staff privacy notice.

We process special category data of our students to fulfil our obligations as an education provider. This includes information about health and wellbeing, ethnicity and race. Further information can be found in this policy document and our applicant and student privacy notice.

We process special category data of research participants in line with Article 89 (1) of the UK GDPR. Further information can be found in this policy document and in our bespoke privacy notices issued as part of individual research projects.

We process special category data of other customers and stakeholders e.g., attendees at open days, graduation ceremonies and public lecturers. Further information can be found in our bespoke privacy notices issued by the department/service hosting the event or managing the interaction.

We also maintain a record of our processing activities in accordance with Article 30 of the UK GDPR.

Conditions for processing special category data and criminal offence data

We process special category data under the following UK GDPR Articles:

i. Article 9 (2) (a) - explicit consent

Where we seek consent, we ensure it is unambiguous, obtained for one or more specified purposes, given by an affirmative action and recorded as the condition for processing.

Examples of processing where we rely on consent include the collection of student and staff dietary requirements for purposes of events management and the collection of health information to allow us to put in place appropriate reasonable adjustments.

ii. Article 9 (2) (b) - where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the University or the data subject in connection with employment, social security or social protection.

We are subject to various laws relating to employment and social protection e.g., laws relating to health and safety, equality and diversity, right to work, maternity pay, paternity leave and sick pay. We process special category data to comply with these legal requirements.

Examples of processing include maintaining records of statutory sick pay, deducting trade union subscriptions from payroll and managing the health, safety and welfare of our employees.

iii. Article 9 (2) (c) – where processing is necessary to protect the vital interests of the data subject or of another natural person.

Where an individual is physically or legally incapable of giving consent, we may process their data in a life and death situation.

An example would be using health information about a student or staff member in a medical emergency.

iv. Article 9 (2) (f) - where processing is necessary for the establishment, exercise or defence of legal claims.

We process special category data, where necessary, for actual or prospective court proceedings, when obtaining legal advice or establishing, exercising or defending legal rights in any other way.

Examples would include processing as part of an employment tribunal or other litigation.

v. Article 9 (2) (g) - reasons of substantial public interest

We process special category data, where necessary, for reasons outlined in paragraphs 6 to 28 of Schedule 1 of the DPA 2018.

Examples include processing data for purposes of preventing fraud (e.g., plagiarism), protecting the public against dishonesty (e.g., through the operation of a fitness to practice procedure for regulated professions such as medicine and nursing), for reasons of monitoring racial and ethnic diversity at senior levels, in delivery of our Counselling Service and to support individuals with particular disabilities or medical conditions.

vi. Article 9 (2) (h) Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

We process special category data, where necessary, for purposes of assessing the working capacity of employees and for putting in place appropriate reasonable adjustments.

An example would be processing undertaken by our Occupational Health Adviser.

vii. Article 9 (2) (i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices

We process special category data, where necessary, for reasons of public interest in the area of public health.

For example, we process health data for reasons of running a Covid 19 testing programme and for reporting results to relevant public health contact tracing authorities.

viii. Article 9 (2) (j) Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89 (1)

We collect, preserve and make available archives to support and expand our cultural endeavour and to contribute to human understanding. In addition, we undertake historical and scientific research using special category data in line with our Charter which states, 'we advance learning and knowledge by teaching and research'. Research involving human participants is only undertaken where ethical approval has been obtained, where there is a clear public interest and where appropriate safeguards to protect data have been put in place.

We process criminal offence data under Article 10 of the UK GDPR.

For example, we process criminal offence data to perform pre-employment checks. We also perform checks on applicants applying to study on regulated programmes (e.g., medicine, nursing and teaching) at point of application and for non-regulated programmes at point of firm acceptance. Criminal conviction data is also used in research projects where ethical approval has been obtained, where there is a clear public interest and where appropriate safeguards to protect data have been put in place.

Processing which requires an Appropriate Policy Document

Almost all of the substantial public interest conditions (see Article 9 (2) (g) above) in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD (see Schedule 1 paragraphs 1 and 5 of the DPA 2018).

This section of the policy is the APD for the University. It demonstrates that the processing of special category and criminal offence data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. In particular, it outlines our retention policies with respect to this data.

Schedule 1 conditions for processing

Special category data

We process special category data for the following purposes in Part 1 of Schedule 1:

- Paragraph 1 - employment, social security and social protection.

We process special category data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:

- Paragraph 8 - Equality of opportunity or treatment;
- Paragraph 9 - Racial and ethnic diversity at senior levels of organisations;
- Paragraph 10 - Preventing or detecting unlawful acts;
- Paragraph 11 - Protecting the public against dishonesty;
- Paragraph 12 - Regulatory requirements relating to unlawful acts and dishonesty;
- Paragraph 17 - Counselling;
- Paragraph 18 - Safeguarding of children and of individuals at risk.

Criminal offence data

We process criminal offence data for the following purposes in parts 1 and 2 of Schedule 1:

- Paragraph 1 – employment, social security and social protection;
- Paragraph 10 - Preventing or detecting unlawful acts;
- Paragraph 18 - Safeguarding of children and of individuals at risk;
- Paragraph 30 - protecting individual's vital interests;
- Paragraph 33 - legal claims.

Procedures for ensuring compliance with the principles.

Accountability principle

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a Data Protection Officer who reports directly to our highest management level.
- Taking a 'data protection by design and default' approach to our activities.
- Maintaining documentation of our processing activities.
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.
- Implementing appropriate security measures in relation to the personal data we process.
- Carrying out data protection impact assessments for our high-risk processing.

We regularly review our accountability measures and update or amend them when required.

Procedures for ensuring compliance with the principles

The University processes special category data and criminal offence data in accordance with the data protection principles.

Principle (a): lawfulness, fairness and transparency

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our published privacy notices. We are open and honest with data subjects and do not deceive or mislead individuals about how we use their data.

Principle (b): purpose limitation

We process special category data and criminal offence data for the purposes outlined in this policy document and in our privacy notices. We do not re-use special category or criminal offence data for secondary purposes that are incompatible with the purposes for which the data was originally obtained.

Principle (c): data minimisation

We collect the minimum amount of data necessary for the intended purpose and periodically review our data to determine whether it can be pseudonymised, de-personalised, fully anonymised or deleted, in part or in full.

Principle (d): accuracy

Where we become aware that personal data is inaccurate or out of date, we take reasonable steps, where appropriate, to ensure that data is erased or rectified without delay. If we decide not to erase or rectify data, we document our decision and justification under UK GDPR.

Principle (e): storage limitation

We retain personal data for no longer than is necessary. Retention timeframes are based on legal requirements and/or business needs. For further information see our Information and Records Management Policy and retention schedules.

Principle (f): integrity and confidentiality (security)

We have implemented appropriate technical and organisational measures to protect special category data and criminal offence data. Access to information is restricted on a need-to-know basis and our data security and data handling arrangements are regularly reviewed to ensure their continued suitability. For further information see our information policies and associated IT security guidance.

APD review and retention

This policy will be updated as necessary and reviewed at least annually.

A copy of this policy and all subsequent revisions will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

Date of next review: April 2022