APPROPRIATE POLICY DOCUMENT - SPECIAL CATEGORY & CRIMINAL OFFENCE DATA V1.0

26/03/2020

Elaine Grant, Data Protection Officer

Version control and history

Title	Description	Author	Approval
Special Category Data – Policy Document v1.0	First standalone version of policy	Elaine Grant	Information Strategy

			Committee 26/03/2020

Contents

1. Introduction

1.1 The University processes special category data, as defined in Article 9 of the General Data Protection Regulation (GDPR). We also process some criminal offence data, as defined in Article 10 of the General Data Protection Regulation (GDPR) and section 11(2) of the Data Protection Act 2018 (DPA 2018). This data must be processed in accordance with the requirements of the GDPR and, where applicable, Schedule 1 of the Data Protection Act 2018 (DPA 2018).

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

1.3 The information in this policy supplements the University's Data Protection Policy and also our privacy notices.

2. Purpose

2.1 This document explains our processing in relation to special category and criminal offence data and satisfies the requirement to have an APD in place, as set out in Schedule 1, Part 4 of the DPA 2018.

3. Scope and status

3.1 This policy applies to all processing of special category or criminal offence data, undertaken by or on behalf of the University, which is based on a condition in Schedule 1 of the DPA which requires an APD.

3.2 Special category data is defined at Article 9 of the 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.

3.3 'Criminal conviction data' covers processing in relation to criminal convictions and offences or related security measures. It also includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing.

4. Conditions for processing

4.1 We process special categories of personal data as set out in our privacy notices.

5. Compliance with the principles

5.1 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 has a direct reporting line to the University Secretary and Compliance Officer;
- 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; and
- carrying out data protection impact assessments for our high risk processing and where otherwise deemed helpful.

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

5.2 Principle (a): lawfulness, fairness and transparency

We have put in place appropriate measures to ensure we meet this principle. These include:

- ensuring that we always meet relevant lawful basis/bases for processing, including at least one of the conditions in Schedule 1, where required;
- providing clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notices; and
- setting out our main processing activities in our privacy notices;

5.3 Principle (b): purpose limitation

Our purposes for processing are set out in our privacy notices.

We will not process personal data for purposes incompatible with the original purpose it was collected for.

5.4 Principle (c): data minimisation

We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

5.5 Principle (d): accuracy

Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

5.6 Principle (e): storage limitation

All special category or criminal conviction data processed by us is retained for the periods set out in our retention schedules. Where bespoke retention schedules have been created for the University, the retention periods for this data are based on our business needs, best practice and/or legal obligations. Our retention schedules are reviewed regularly and updated when necessary.

For some records we refer to the JISC retention schedules for the HEI sector. These schedules have been developed for the sector, incorporating legal requirements and best practice.

5.7 Principle (f): integrity and confidentiality (security)

Electronic information is processed within our secure network. Hard copy information is processed in line with appropriate security procedures. Both our electronic systems and physical storage have appropriate access controls applied.

The systems we use to process personal data allow us to erase or update personal data at any point in time, where required.

6. Retention policies

Our retention policies are available via our website.

7. APD review

This policy will be reviewed in line with the review procedures for the University's Data Protection Policy. It may be revised more frequently if necessary.