APPROPRIATE POLICY DOCUMENT

1. INTRODUCTION

As part of its daily operations Keele University needs to collect and process personal data about its current, prospective and former staff and students, research participants and other individuals with whom it deals, in order to carry out its responsibilities and fulfil its functions as a Higher Education provider.

It is sometimes necessary to process special category personal data and data regarding actual or alleged criminal convictions, which are types of data that must only be processed if certain conditions are met, as set out within the UK General Data Protection Regulation (**GDPR**) and the Data Protection Act 2018 (**DPA**). In specific instances Part 4 of Schedule 1 of the DPA requires an 'appropriate policy document' to also be in place to enable processing of these types of data.

1.1 Purpose

This Policy sets out how the University will comply with data protection principles where it processes special category personal data and criminal conviction data in reliance upon a condition from Parts 1, 2 or 3 of Schedule 1 of the DPA.

1.2 Scope

This Policy applies to special category personal data and data regarding actual or alleged criminal convictions processed by the University, held in any system, in digital or physical format and stored in any location either on or off campus. It applies to all individuals accessing University information in conducting work for the University ('**staff**'), including but not limited to: fixed-term, contract and variable hours employees; students employed by the University; partner organisations' employees; consultants; volunteers; representatives and agents.

2. POLICY

2.1 Processing requiring an 'Appropriate Policy Document'

The University processes special category personal data and data about criminal convictions in reliance on the conditions detailed below, as set out in Schedule 1 of the DPA.

Part 1 of Schedule 1
Paragraph 1 – Employment, social security and social protection

Paragraph 2 – Health and social care purposes

Paragraph 3 – Public Health

Paragraph 4 – Research

Part 2 of Schedule 1
Paragraph 6 – Statutory and government purposes

Paragraph 8 – Equality of opportunity or treatment

Paragraph 9 – Racial and ethnic diversity at senior levels

Paragraph 10 – Preventing or detecting unlawful acts

Paragraph 11 – Protecting the public against dishonesty etc.

Paragraph 12 – Regulatory requirements relating to unlawful acts and dishonesty etc.

Paragraph 13 – Journalism etc

Paragraph 14 – Preventing fraud

Paragraph 15 – Suspicion of terrorist financing or money laundering

Paragraph 17 – Counselling etc.

Paragraph 18 - Safeguarding of children and of individuals at risk

Paragraph 19 – Safeguarding of economic wellbeing of certain individuals

Paragraph 21 – Occupational pensions

Paragraph 24 – Disclosure to elected representatives

Part 3 of Schedule 1
Paragraph 33 – Legal claims

2.2. Compliance with the data protection principles

When processing special category personal data and criminal conviction data in reliance upon a condition within Parts 1, 2 or 3 of Schedule 1 of the DPA, the University will comply with the data protection principles in Article 5 of the GDPR, as follows:

a) Processing is lawful, fair and transparent
The appropriate lawful basis for processing is stated in the University's Privacy Notices outlining the processing, unless a valid exemption from the right to be informed is applicable.

b) Processing is for specified purposes; no further processing that is incompatible with those specified purposes
Personal data will only be processed for the specific purposes notified to the data subject via a Privacy notice or for any other purposes permitted under data protection legislation. Personal data will not be collected for one purpose and then used for a separate, unrelated purpose. Should it become necessary to change the purpose for which the data is processed, data subjects will be informed of the new purpose before any processing occurs.

c) Processing is adequate, relevant and limited to what is necessary for the purpose
Only the minimum personal data needed to fulfil the specified purpose will be collected, information which is not needed or is not relevant to the purpose will not be collected or otherwise processed.

d) Personal data is accurate and kept up to date

Where the University has been notified that information is incorrect, steps will be taken to correct it. Accuracy of personal data will be checked at the point of collection and reviewed at necessary intervals.

e) Personal data is kept no longer than necessary
Personal data will be managed in line with the University's Records Management Policy and Records Retention Schedule, which detail how long certain types of information should be retained and when and how it should be securely destroyed. Retention periods are based on both legal and operational requirements. Any information about criminal convictions of staff or students which has been obtained as part of a DBS check will be retained in accordance with DBS standards.

f) Processing is carried out securely to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage
Personal data is stored securely using appropriate technological controls with access restricted both internally and externally on a need-to-know basis. The University will ensure that appropriate technical and organisational measures are taken to protect against unlawful or unauthorised processing of personal data and against its accidental loss, destruction or damage.

3. ROLES AND RESPONSIBILITIES

Adherence to the processing of special category personal data detailed within this Appropriate Policy Document is the responsibility of all University staff handling such personal data. Compliance with this policy will be monitored via internal data protection audits carried out by the University's Data Protection Officer.

All staff and those with approved access to University information and systems must complete annual mandatory Information Security Training. Any suspected or actual misuse, unauthorised disclosure of, or access to, personal data must be immediately reported to the University's Joint Information Governance team via the data breach notification form on the Service Desk or to DPO@keele.ac.uk

Any queries regarding this Policy, or concerns that data protection principles have not been followed, should be raised with the Data Protection Officer via DPO@keele.ac.uk

4. RELATED POLICIES AND PROCEDURES

- Data Protection Policy
- Information Governance Framework
- Records Retention Schedule
- Records Management Policy
- Data Classification and Handling Policy

5. REVIEW, APPROVAL & PUBLICATION

5.1 Review This Policy will be reviewed and agreed by the University Executive Committee before final approval.

5.2 Final Approval This Policy will require final approval from Council.

5.3 **Publication** This Policy will be published on the website within the Policy Zone and retained for the duration of the University's processing activities of the data and for a minimum of 6 months thereafter. The University's Information Governance web pages will maintain prominent links to this Policy as appropriate on both external and internal facing pages.

6. DOCUMENT CONTROL INFORMATION

Document Name	Appropriate Policy Document
Owner	Director of Legal, Governance & Compliance
Version Number	1.1
Equality Analysis Form Submission Date	Not applicable
Approval Date	16/9/2021
Approved By	Council
Date of Commencement	16/9/2021
Date of Last Review	n/a
Date for Next Review	16/9/2024
Related University Policy Documents	See section 5
Administrative update	10/03/2022; Head of Legal, Governance & Compliance updated to Director of Legal, Governance & Compliance
For Office Use – Keywords for search function	