Appropriate Policy Document

Required by s.39, Schedule 1, Part 4 of the Data Protection Act 2018

Document Title: Appropriate Policy Document			
Version No.	2.0	Policy Owner	Legal & Governance Services
Superseded version	1.0	Author Role Title	Head of Information Governance
Approval Date	18.05.2021	Approved by	UET
Effective Date	18.05.2021	Review Date	June 2022

APPROPRIATE POLICY DOCUMENT

1. Introduction

1.1 The University processes a variety of personal data about lots of groups of individuals, including, but not limited to, prospective, current, and previous students, alumni, current, prospective and previous employees and Board members. We use this information for a variety of purposes in the proper functioning and administration of the University.

1.2 In some cases, the University is required to process special category data and data about actual or alleged criminal convictions. This type of personal data is afforded additional protection under Data Protection Legislation (the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA)) and we must only process it if certain conditions can be met. Section 39, Schedule 1 Part 4 of the DPA requires the Data Controller to have appropriate policy documentation in place to enable this processing to be carried out where certain conditions are met and this policy is designed to fulfil that requirement.

2. Scope

2.1 This Policy applies to all employees of the University including temporary, casual, contract and agency staff, as well as any contractors or service providers acting on behalf of the University who processes special category data or data about actual or alleged criminal convictions.

2.2 This policy sets out how the University will comply with the data protection principles when processing special category data and data about criminal convictions when it does so in reliance on a condition from Part 1, 2 or 3 of Schedule 1 of the DPA. It also explains our policies in relation to retaining and erasing this type of personal data. This policy should be read alongside the University's Data Protection Policy.

3. Objectives

3.1 This Policy aims to ensure that:

3.1.1 The University complies with its obligations under Data Protection Legislation when processing special category data and criminal convictions data; and

3.1.2 University staff are aware of the institution's legal obligations and how to comply with the legislation.

4. Guidance and related policies

4.1 Further guidance on the practices and procedures necessary to comply with this Policy and the University's legislative obligations is available from the Legal and Governance Services intranet pages.

4.2 Reference should also be had to the University's Data Protection Policy and Code of Practice, Information Security Policy and the Data Breach Management Policy. Copies of all related policies are available from the Information Governance unit in Legal & Governance Services (email: dpo@tees.ac.uk) and are also accessible from the Legal & Governance Services intranet available here.

5. Responsibilities

5.1 The University as Data Controller has a corporate responsibility to process Personal Data with due regard to the rights and freedoms of individuals, and to comply with the requirements of Data Protection Law. It is the role of the DPO to ensure that the University complies with Data Protection Law and this policy.

5.2 USMT members must ensure that the activities and processes within their school or departments (as applicable) are compliant with this Policy and related Data Protection Policy and Code of Practice, and that their staff have a sufficient awareness and knowledge of relevant requirements and that appropriate processes are in place to ensure compliance.

5.3 Local Information Governance Champions are assigned within each School and Department by the Dean/Director as a champion for ensuring a consistent approach to implementing this policy and to liaise as appropriate with Legal & Governance Services in ensuring and demonstrating compliance.

5.4 The University's Executive will continue to review the effectiveness of this policy to ensure it is up to date and is achieving its stated objectives.

6. Staff Responsibilities

6.1 All staff must comply with the requirements of this Policy.

6.2 Staff may only process Special Category Personal Data and Criminal Convictions Data to the extent to which they have been specifically authorised by the University, or are generally authorised as part of their role within the University.

6.3 Staff are responsible for ensuring any Special Category Data and Criminal Convictions Data processed in the course of their employment is managed

securely. Specifically, individuals are responsible for ensuring that special category data and criminal convictions data in their possession is not left unsecure, for example in meeting rooms, public spaces, open plan environments or mobile devices, without adequate protection.

7. Conditions from Schedule 1 DPA

7.1 The University processes special category data and data about criminal convictions in reliance on the following conditions from Schedule 1 DPA. These are not the only legal bases/conditions on which we process special category data or criminal convictions data but they are the only ones to which this policy applies:

7.1.1 Paragraph 1 – Employment, social security and social protection

The University processes a variety of information about prospective, current and previous employees for employment purposes, including data about health and criminal convictions and associated proceedings. It is not appropriate to obtain consent for such processing due to the nature of the employer-employee relationship and because consent cannot be freely given or withdrawn; therefore the University relies on this condition for much of this processing. Personal data processed for employment purposes is treated confidentially and maintained by HR as part of applicant and employee personal files. It is only shared within the University on a strict need-to-know basis where the law allows. Where employees are seconded under contract to another organisation, or a secondee carries out work for the University, the University and the other organisation may share personal data in reliance on this condition, as set out in the applicable contract. Any information about criminal convictions obtained as part of a Disclosure and Barring Service (DBS) check is stored and retained in line with DBS requirements.

7.1.2 Paragraph 6 – Statutory etc. and government purposes

The University is legally required to provide some special category data about staff and students to external organisations for statutory returns and reporting, such as the data we provide to the Higher Education Statistics Agency (HESA). Only the minimum amount of data necessary to fulfil this requirement is provided and all data is shared securely.

We also rely on this condition to process data about students' criminal convictions. This applies if a student is offered a place on a course which can result in employment in a regulated profession and the course involves an integral work placement which could not be undertaken if the student has a criminal conviction. We must process this data to ensure we do not admit a student onto a course which they cannot possibly complete. Any information about criminal

convictions obtained as part of a Disclosure and Barring Service (DBS) check is stored and retained in line with DBS requirements.

7.1.3 **Paragraph 8 – Equality of opportunity or treatment**

The University recognises the importance of equality of opportunity or treatment and monitors and reviews the existence or absence of this across all areas so that equality can be promoted and/or maintained. Any processing of the specified categories of personal data used for these purposes is carried out confidentially and securely. When it is collected as part of an application form, the data is stored separately from the rest of the application data.

7.1.4 **Paragraph 10 – Preventing or detecting unlawful acts**

We rely on this condition to process data about applicants' and students' criminal convictions, in certain circumstances, to enable us to manage any potential risks to the University community. Any information about criminal convictions obtained as part of a Disclosure and Barring Service (DBS) check is stored and retained in line with DBS requirements. We may also rely on this condition to process information about employees' criminal convictions, if appropriate.

We also rely on this condition to disclose certain items of personal data to the police, DWP, or other similar bodies for the prevention and detection of unlawful acts. Any personal data disclosed under these circumstances is shared securely and only the minimum amount of information necessary is shared in any case.

The University has a duty to prevent individuals from being drawn into terrorism (known as the Prevent duty). Where we process special category data such as personal data about religious beliefs or political opinions, or data about criminal convictions, for the purposes of fulfilling our Prevent duty, we may rely on this condition where it is not appropriate to obtain an individual's consent. This may be the case where we are carrying out initial investigations into concerns that one or more individuals are being drawn into terrorism, or making initial reports or requests for advice to the police or the Office for Students Prevent Lead. Any personal data processed for these purposes is processed sensitively and confidentially on a strict need-to-know basis, in line with Teesside and national Prevent procedures and guidance.

7.1.5 **Paragraph 11 – Protecting the public against dishonesty etc.**

The University runs many courses which lead to entry into a regulated profession or occupation. We may disclose special category data or data about criminal convictions to those who regulate such professions so that those regulators can exercise their

functions appropriately by ensuring practitioners are fit and proper. There is a substantial public interest in enabling regulators to ensure that only those who are fit to practise a particular profession or occupation are able to do so.

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

Where it is not appropriate to rely on consent, the University relies on this condition when it processes special category data and criminal convictions data about its Board Members/Governing Body Members (as well as some employees) to ensure they are fit and proper persons to fulfil the role. To enable us to register as a higher education provider with the Office for Students, we must be able to demonstrate that the University has appropriate management arrangements in place which do not present a risk to students or to public funds.

7.1.7 **Paragraph 17 – Counselling etc.**

The University provides staff and student counselling services and a number of other student wellbeing services delivered by Student Services. The majority of special category data or data about criminal convictions is processed with the explicit consent of the individual using one of the counselling services; however if a circumstance arose which required us to process personal data without consent in order to provide confidential counselling, advice or support e.g. from Student Services, and such processing was in the substantial public interest, we would do so in reliance on this condition. All information held in counselling records is treated confidentially and stored securely and all counsellors comply with professional guidelines.

7.1.8 **Paragraph 18 – Safeguarding of children and of individuals at risk**

The University admits students who are under 18, as well as those over 18, to our courses and to our accommodation. We rely on this condition to process data about applicants' and students' criminal convictions, in certain circumstances, to enable us to identify and manage any potential risks to the University community. Any information about criminal convictions obtained as part of a Disclosure and Barring Service (DBS) check is stored and retained in line with DBS requirements. We may also rely on this condition to process information about employees' criminal convictions, if appropriate.

We also rely on this condition to process special category data for the purposes of safeguarding children who are under 18, or individuals who are over 18 and at risk, where there is a substantial

public interest and we are unable to obtain consent for the processing. This condition is most likely to be relied upon where we act in students' best interests to provide support via our Student Services teams.

8. Data protection principles

8.1 When processing personal data, anyone to whom this policy applies will comply with the six data protection principles set out in Article 5 of the GDPR. These are expressly referred to in the University's Data Protection Policy.

8.2 These are principles of good practice and compliance is a requirement of the data protection legislation, enforced by the Information Commissioner. The principles are summarised below, along with an explanation of how the University will comply with them whenever we process special category data or data about criminal convictions in reliance on a condition from Part 1, 2 or 3 of Schedule 1 DPA, as set out in this policy:

8.2.1 Processed lawfully, fairly and in a transparent manner

(a) The data protection legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and in a transparent manner and without adversely affecting the rights of the data subject. In every case, the data subject will be told who the controller is, the purposes for which the data are to be processed and the identities of any other parties to whom the data may be disclosed or transferred, among other things. This information will be provided to the data subject in a privacy notice at the time the data is collected, unless an exemption from the right to be informed applies in a particular case.

(b) Teesside will process personal data lawfully by ensuring there is a legal basis for all the processing we undertake. This may include ensuring the processing is necessary for the performance of a contract, obtaining the data subject's consent to the processing or ensuring the processing is necessary for the legitimate interests of Teesside or the party to whom the data is disclosed. When special category data or data about criminal convictions is being processed, we will ensure that an additional legal basis applies.

(c) Advice from the Data Protection Officer DPO@teesside.ac.uk will be sought before processing special category data or data about criminal convictions.

8.2.2 Processed for limited purposes

(a) In every case set out in Section D, personal data will only be processed for the specific purposes notified to the data subject via the privacy notice when the data was first collected or for any other purposes specifically permitted under the data protection legislation. Personal data will not be further processed in a manner which is incompatible with these purposes. This means that personal data will not be collected for one purpose and then used for an entirely different, unrelated purpose. If it becomes necessary to change the purpose for which the data is processed, the data subject will be informed of the new purpose before any processing occurs. It may be the case that we cannot use the personal data for another purpose unless the data subject consents.

8.2.3 Adequate, relevant and not excessive (data minimisation)

(a) Personal data held about data subjects will be sufficient for the purposes for which it is held. Information which is not needed or is not relevant for a purpose will not be collected or otherwise processed. The minimum amount of personal data needed to properly achieve the purpose in question will be identified and collected; additional, excessive personal data will not be held.

8.2.4 Accurate and up-to-date

(a) Personal data will be accurate and, where necessary, kept up-to-date. Information which is incorrect or misleading is not accurate; steps will be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards.

(b) Personal information identified as being factually inaccurate will be amended or erased; however it may not be appropriate to delete this information altogether if historic decisions have been based on it. In these cases, the information will be rectified for future use with an explanatory note placed on file as required to explain the situation. Where a data subject disagrees with a professional opinion about him or herself which does not – by definition – constitute verifiable fact, the data subject's difference of opinion will be noted on the file in the relevant places.

8.2.5 Not kept for longer than is necessary (storage limitation)

(a) Personal data will not be kept longer than is necessary for the purposes for which is it being processed. This means that data will be securely destroyed or erased from our systems when it is no longer required i.e. there is no legal

requirement to retain it and there is no business or operational need for the information, taking account of the purposes for which it was originally requested.

(b) Criminal Convictions data which is collected for the purposes of determining whether or not a student may study at the University will be retained only for a reasonable period to be able to evidence the University's decision or, if an applicant is successful, it will be retained for the duration of their studies. Thereafter it will be deleted and no record will be retained.

8.2.6 Secure (integrity and confidentiality)

(a) We will ensure that appropriate technical and organisational measures are taken to protect against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data (see section F of Teesside's Data Protection Policy for further information).

8.2.7 Retention and erasure of personal data

(a) Personal information will be managed in line with the University's Document Classification and Retention Schedule, which provide guidance on how long certain types of information should be retained and when and how they should be destroyed. Staff will consult the Information Governance pages of the Teesside University intranet for the current guidance.

(b) Any information which forms part of a student record will usually be retained for six years following graduation.

(c) Any information which forms part of an employee record will usually be retained for six years after the termination of employment. Some information will be retained for longer, for example pension records.

(d) Any information about criminal convictions of staff or students which has been obtained as part of a DBS check will be retained in line with current DBS requirements and any information obtained for the purposes of a Criminal Convictions Panel, will be held in accordance with the Criminal Convictions Policy.

9. Breach of the policy

Failure to follow this Policy and the Data Protection Code of Practice may result in disciplinary action.