|  |  |
| --- | --- |
| A picture containing text  Description automatically generated | **POLICY DOCUMENT – OUR PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA AND CRIMINAL OFFENCE DATA** |

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

This document applies in addition to the Cardiff University’s general [data protection notices](Our%20data%20protection%20policy%20-%20Public%20information%20-%20Cardiff%20University), which set out our legal bases and purposes for processing personal data. This Appropriate Policy Document will provide further information on the conditions for processing SC and CO data under Schedule 1 of the DPA 2018. The applicable conditions relied upon the University are as follows:

**Article 9 conditions for processing special category data**

1. Employment, social security and social protection **UK GDPR Article 9(b) and DPA 2018 Schedule 1 para 1**
2. Reasons of substantial public interest **UK GDPR Article 9(g)**

**DPA 2018 Schedule 1 conditions**

1. Statutory etc. and government purposes **DPA 2018 Schedule 18 para 6**
2. Equality of opportunity or treatment **DPA 2018 Schedule 18 para 8**
3. Racial and ethnic diversity at senior levels of organisations **DPA 2018 Schedule 18 para 9**
4. Preventing or detecting unlawful acts **DPA 2018 Schedule 18 para 10**
5. Protecting the public against dishonesty **DPA 2018 Schedule 18 para 11**
6. Regulatory requirements **DPA 2018 Schedule 18 para 12**
7. Support for individuals with a particular disability or medical condition **DPA 2018 Schedule 18 para 16**
8. Counselling **DPA 2018 Schedule 18 para 17**
9. Safeguarding of children and or individuals at risk **DPA 2018 Schedule 18 para 18**
10. Safeguarding of economic well-being of certain individuals **DPA 2018 Schedule 18 para 19**

**Our purpose for processing Special Category Data**

* Equality monitoring (2, 4, 5)
* Student/staff/WP support and wellbeing (1, 2, 6, 9, 10, 11, 12)
* Strike action (1)
* Reasonable adjustments (1, 2, 4, 9)
* Close Personal Relationships (1, 2, 4, 6, 7, 8, 11)
* Occupational Health (1)
* External returns (e.g. HEIW, HESA) (2, 3)
* Health data (e.g. sickness records) (1)
* Complaints/Disciplinary/Grievance (1, 2, 4, 6, 7)

**Our purpose for processing Criminal Offence Data**

* Application – HR/Admissions/Residences (1, 2, 6, 7, 11)
* Employment (1, 2, 6, 7, 11)
  + DBS checks
  + Disciplinary/Grievance
* Current student (2, 6, 7, 11)
  + DBS checks – courses/placements/WP/Research
  + Risk assessment
  + Fulfilling obligations under Prevent
* Day Care Centre (1, 2, 6, 7, 11)

**How we comply with Data Protection Principles**

Cardiff University has a [Data Protection Policy](https://www.cardiff.ac.uk/public-information/policies-and-procedures/data-protection/research-participants-data-protection-notice) which requires all staff to adhere to the requirements of data protection legislation and in particular the data protection principles. Our website also sets out how data subjects can assert their [individual rights](https://www.cardiff.ac.uk/public-information/policies-and-procedures/data-protection/your-data-protection-rights), including the right to rectification. We are committed to processing personal information lawfully, fairly and transparently and maintain a record of processing activities. Our data protection notices and this document set out the purposes for which we collect personal, SC and CO data. The [Records Management Policy](https://www.cardiff.ac.uk/public-information/policies-and-procedures/record-management-policy-and-retention-schedules) and supporting retention schedules, set out our retention periods to ensure that we retain data for no longer than is necessary. We provide tools to assist with managing risks around compliance security and undertake a Data Protection Impact Assessment and Information Security Risk Assessment where appropriate.

The university has an [Information Security Framework](https://www.cardiff.ac.uk/public-information/policies-and-procedures/information-security), of which the Data Protection Policy and Records Management Policy form part, which also includes our Information Security Policy and sets out the requirements for handling university data (including personal, SC and CO data. These requirements cover the university’s security measures which may be put in place to protect the information, such as system security specifications, contractual arrangements with processors, encryption of devices, multi-factor authentication. The framework also contains the Information Security Incident Management Policy and supporting procedure which covers how we address any potential or actual information security incidents or personal data breaches in proportion to the sensitivity of the data.

The Information Security Framework is regularly reviewed to ensure it remains fit for purpose to ensure compliance with data protection, information security and other regulatory requirements. Individual responsibilities under the framework, is communicated in a number of ways, to all staff upon induction and addressed in annual mandatory Information Security training module and delivered in non-mandatory and other bespoke training sessions.