

**Policy document – our processing of special categories and criminal offence data**

**Purpose of this policy document**

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document to be in place when processing special category and criminal offence data under certain specified conditions as per DPA 2018, Schedule 1, Paragraphs 1(b) and 5.

This document explains how we process special category data and how we comply with these conditions alongside the requirements of the General Data Protection Regulation (GDPR) Principles (GDPR Article 5).

**Special category data**

Special category data is defined at Article 9 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
* Data concerning a natural person’s sex life or sexual orientation.

**Criminal conviction data**

Article 10 GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, Part 2, Chapter 2, Paragraph 11(2) of the DPA 2018 specifically confirms that this includes personal 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’.

**Conditions for processing special category and criminal offence data**

We process special category and criminal offence data under the following GDPR Articles:

Article 9(2)(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

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 ICO or the data subject in connection with employment, social security or social protection.

Examples of our processing include staff sickness absences and political activity declarations.

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

Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

The lawful basis under which DWFRS collects special category or criminal offence data varies depending on the purpose for processing. The Information Asset Register provides a detailed breakdown (including Article 6 and Article 9 of the GDPR).

**Substantial public interest**

Part 1, Chapter 2, Paragraph 10(3) of the DPA 2018 sets out that in order for processing of special categories of personal data and criminal offence data to be necessary for reasons of substantial public interest under Article 9(2)(g) of the UK GDPR, that processing must meet one of the conditions set out in Schedule 1, Part 2.

DWFRS processes special category and criminal offence data in the performance of its statutory and corporate functions when the following conditions set out in the following paragraphs of Schedule 1, Part 2 of the DPA 2018 are met:

* paragraph 6 (Statutory etc and government purposes)
* paragraph 8 (Equality of opportunity or treatment)
* paragraph 10 (Preventing or detecting unlawful acts)
* paragraph 18 (Safeguarding of children and of individuals at risk)

These conditions apply to DWFRS’s statutory and corporate functions. All processing is for the first listed purpose and might also be for others, depending on the context.

**Employment, social security and social protection law**

Part 2, Chapter 2, Paragraph 10(2) of the DPA 2018 sets out that in order for processing of special categories of personal data to be necessary for the purposes of carrying out the obligations and exercising specific rights of DWFRS or of the data subject in the field of employment, social security and social protection law under Article 9(2)(b) of the UK GDPR, that processing must meet one of the conditions set out in Schedule 1, Part 1 of the DPA 2018.

DWFRS processes special category data for HR purposes when the condition set out in Schedule 1, Part, 1, Paragraph 1 of the DPA 2018 is met.

**Procedures for ensuring compliance with the data protection principles**

**Accountability principle**

We have appointed a Data Protection Officer who reports to the Senior Information Risk Owner and is responsible for monitoring compliance with data protection legislation.

Information Asset Owners (IAOs), at Head of Department or Area Manager level, have risk ownership and accountability of the special category data that is processed within their department.

We carry out Information Governance impact assessments prior to undertaking any new, or changes to, processing of special category data.

**Lawfulness, fairness and transparency**

To ensure our processing is lawful, fair and transparent, we:

* Maintain a Record of Processing Activity via our Information Asset Register.
* Ensure that an appropriate lawful basis is applied is applied under Articles 6 and 9 conditions under Schedule 1 of the DPA18 for all processing of special category data.
* Publish and regularly review privacy notices for each of our core service delivery functions and provide an internal privacy notice for all employee related data.

**Purpose limitation**

To comply with this principle, we have:

* clear terms and conditions and appropriate agreements in place when working with third parties to set out the required processing purposes.
* procedures in place to determine incompatible processing.

**Data minimisation**

To ensure we process the minimum amount of special category data, we:

* Have an information screening process in place as part of a wider Information Governance Impact Assessment, to ensure that information value is understood and monitored.
* Challenge the necessity for special category data processing where business need is unjustified.

**Data accuracy**

To comply with the data accuracy principle, we:

* Take reasonable steps to ensure that data is rectified or erased when notified that is inaccurate.
* Document any decision taken not to correct data where rights to rectification do not apply.

**Storage limitation**

To ensure that we do not keep data longer than required, we:

* Document retention schedules for each special category processing purpose within our Information Asset Register and regularly review these.
* Obtain annual assurance from our Information Asset Owners that retention schedules are being managed and applied.

**Integrity and confidentiality**

To comply with this principle, we:

* Have in place a suite of acceptable use and information security procedures
* Undertake technical security assessments (as part of a wider information governance impact assessment) for new or changes to systems and software
* Have data processor agreements in place with third parties to ensure that they adhere to our expectations for securely managing our information
* Ensure all our staff undertake regular data protection and information security training.