


TRUST POLICY FOR PROCESSING OF SPECIAL CATEGORY DATA ABOUT EMPLOYEES

Reference Number POL-XXXX	Version: 1.1	Status: Final	Author: Emily Griffiths Job Title: Information Governance/DPO	
Version / Amendment History	Version	Date	Author	Reason
	1	Jan 2023	E Griffiths	First version
	1.1	Nov 2023	E Griffiths	Amendments following consultation
Intended Recipients: All staff involved in the management and operational delivery of employee and informational services				
Training and dissemination: Will be published on the Intranet (Neti) and Internet (Koha). Staff will also be made aware through IG communications and training.				
To be read in conjunction with: Records Management Procedures and Guidelines (for all records), Information Governance Policy, Data Protection & dealing with Confidential Information Policy, Access to Personal Data Policy, Standard Operating Procedures (SOPs) for Clinical Records.				
In consultation with and Date: Information Governance Steering Group (Jan 2023), Groups for Policy Consultation under People and Culture Committee (March-May 2023) IGCSDR (November 2023)				
EIRA stage One Completed Stage Two Many special category data describe protected characteristics under equalities law. This Policy provides control over the processing of these data, with reliance on other protective training and other practices to prevent relevant data being misused. EIRA has been completed.				
Approving Body and Date Approved			Trust Delivery Group - January 2024	
Date of Issue			January 2024	
Review Date and Frequency			November 2026 and then 3 yearly	
Contact for Review			Head of Information Governance/DPO	
Executive Lead				

	Will Monaghan, Executive Chief Digital Information Officer
--	--

Background

There are particular legal requirements for processing special category data and criminal offence data in accordance in Article 9 and 10 of the General Data Protection Regulation as applied in the UK ('GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Some of the Schedule 1 conditions for processing special category and criminal offence data require controllers to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in GDPR Article 5 and policies regarding the retention and erasure of such personal data.

This document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018. The information supplements UHDB's employment privacy notice, which can be found on UHDB's public website.

To introduce the Policy below, there are three considerations for anyone proposing to use special category data to ascertain if it is necessary, lawful, and managed appropriately:

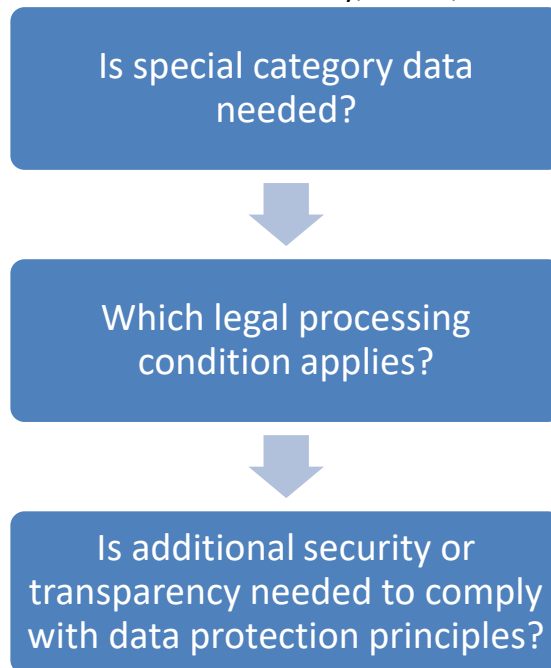


Figure 1 Flow diagram for main checks to make before using special category data. Seek advice from the Data Protection Officer if you are unsure.

Definitions

Data subject - the term in data protection law for the person the data relates to

Personal data - data that relates a data subject

Special category data - types of personal data that can only be used under special conditions and require a higher level of protection

Types of data

Special category data is 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.

Criminal conviction data is personal data relating to criminal convictions and offences or related security measures. In addition, section 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'. We process criminal offence data under Article 10 of the GDPR. Examples of UHDB processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations.

Conditions for lawful processing under GDPR

Conditions for processing special category data are from GDPR Article 9:

a: the data subject has given explicit consent

b: the processing is necessary for the purposes of exercising its obligations e.g.: employment

c: processing is necessary to protect the vital interests if the data subject e.g.: processing health information in a medical emergency

d: processing is carried out for a not-for-profit organization e.g.: union

e: the data has been made public by the data subject

f: for the establishment, exercise or defence of legal claims e.g.: litigation or employment tribunal

g: substantial public interest. If relying on substantial public interest then a condition of this is for the controller to have an appropriate policy document in place.

h: the data is being processed for health and social care purposes

i: public interest in public health and is carried out under the supervision of a health professional

j: archiving, research and statistics

Conditions for lawful processing under Schedule 1 of the Data Protection Act

We process special category data for the following purposes in Part 1 of Schedule 1:

- Paragraph 1(1) employment, social security and social protection.

We process special category data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:

- Paragraph 6(1) and (2)(a) statutory, etc. purposes
- Paragraph 10(1) preventing or detecting unlawful acts
- Paragraph 11(1) and (2) protecting the public against dishonesty
- Paragraph 12(1) and (2) regulatory requirements relating to unlawful acts and dishonesty
- Paragraph 24(1) and (2) disclosure to elected representatives

We process criminal offence data for the following purposes in parts 1 and 2 of Schedule 1:

- Paragraph 1 – employment, social security and social protection
- Paragraph 6(2)(a) – statutory, etc. purposes

Description of data processing

We process the special category data about our employees that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, photographs and trade union activity to ensure fair pay (for example involvement on strike days).

We process the special category data about health as necessary to fulfil our obligations as a health and social care provider and as part of the occupational health service. Some of these obligations are met by external providers, such as the Employee Assistance Program. There are other obligations on NHS organisations that can involve external scrutiny of staff information, for example regarding fraud.

Our processing for reasons of substantial public interest relates to the data we receive or obtain to fulfil our statutory function as a health care provider. This may be health data, evidence provided to us as part of a complaint, or intelligence information we gather for our investigations or investigations conducted by other bodies e.g. the police. It may also be in surveys issued by external data processors where we monitor staff wellbeing and aspects of our equalities duty.

Further information about this processing can be found on our website or the intranet. We also maintain a record of our processing activities in accordance with Article 30 of the GDPR.

We also process special category personal data in other instances where it is not a requirement to keep an appropriate policy document.

Compliance with the data protection principles.

UHDB has a range of procedures for ensuring special category and criminal offence data are protected when they are processed.

- **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 reports directly to our highest management level.
- Taking a 'data protection by design and default' approach to our activities and carrying out data protection impact assessments for high-risk processing.
- Maintaining documentation of our processing activities and producing training materials.
- 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 reviewing those measures when incidents occur.
- We regularly review our accountability measures and update or amend them when required, including assessing our special category processing against regulatory checklists and undertaking audits.

Processing will be in accordance with the principles and framework outlined in UHDB's Information Governance Policy. How special category data are processed in accordance with the data protection principles from GDPR are outlined below:

- **Principle (a): lawfulness, fairness and transparency**

Processing personal data must be lawful, fair, and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.

- We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice and this policy document.
- Our processing for purposes of substantial public interest is necessary for the exercise of a function conferred on the Trust by the legislation
- Our processing for the purposes of employment relates to our obligations as an employer.
- We also process special category personal data to comply with other obligations imposed on the Trust in its capacity as a public authority e.g., the Equality Act.

- **Principle (b): purpose limitation**

We will process data for the purpose it was provided to us as a health care provider or employer. If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose. We will keep a record of all data sharing. We will not process personal data for purposes incompatible with the original purpose it was collected for.

- **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.

- **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.

- **Principle (e): storage limitation**

All special category data processed by us for the purpose of employment or substantial public interest is, unless retained longer for archiving purposes, retained for the periods set out in our Records Management Policy. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs.

- **Principle (f): integrity and confidentiality (security)**

Electronic information is processed within our secure network and on secure cloud services provided to the NHS, for example by Microsoft. Hard copy information is processed in line with our security procedures. 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 appropriate.