

Appropriate Policy Document

Data Protection

September 2025



Contents

Introduction	2
Purpose	2
Definitions and Scope	2
Conditions	3
Compliance with Data Protection Principles	6
Accountability and Governance	6
Lawfulness, Fairness and Transparency	6
Purpose Limitation	7
Data Minimisation	7
Accuracy	8
Storage Limitation	8
Integrity and Confidentiality	8
Document Administration	10

Introduction

This Policy is part of Health and Safety Executive's (HSE) policy suite, to which all personnel and the functions provided by HSE are required to adhere.

Purpose

The Data Protection Act (DPA) 2018 states that data controllers should have an Appropriate Policy Document (APD) in place that documents the safeguards in place for the sensitive processing that is used for law enforcement purposes, where the processing is reliant on consent or a condition specified in Schedule 8 of DPA 2018.

When processing special category data under the UK General Data Protection Regulation, (UK GDPR), the DPA Schedule 1, Part 2, Paragraph 5, states that data controllers should have an APD in place when relying on substantial public interest conditions.

This document will demonstrate that the processing of Special Category data by HSE, based on these specific Schedule 1 and Schedule 8 conditions is compliant with the requirements of the Data Protection Principles. Its purpose is to explain what special category personal data is processed by HSE, the various reasons for which we use this data, and how we ensure it is handled in accordance with the core data protection principles.

Definitions and Scope

Special Category data (defined by Article 9 of the UK GDPR) is personal data which reveals:

- 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

Sensitive Processing (defined by section 35 of the DPA 2018) is the processing of:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
- data concerning health;
- data concerning an individual's sex life or sexual orientation.

Article 10 of the UK GDPR covers processing in relation to criminal convictions and offences or related security measures. Section 11(2) of the DPA 2018 states that criminal conviction data includes data which relates to the alleged commission of offences and related proceedings and sentencing.

Conditions

HSE is an executive non-departmental public body established under section 10 of the Health and Safety at Work etc. Act 1974 (HSWA), as amended. We are also listed as a Competent Authority under Section 28(7) of DPA 2018.

HSE processes special category data and criminal offence data under the following DPA 2018, Schedule 1 conditions;

Reference	Title
Part 1(1)	Employment, Social Security and Social Protection
<i>HSE may process data concerning racial or ethnic origin, religious or philosophical beliefs, trade union membership, sexual orientation, health and criminal offence data for the purposes of performing its obligations or rights as an employer, or for ensuring the social protection of individuals.</i>	
Part 2(6)	Statutory etc. and government purposes
<i>HSE may process data concerning health, trade union membership, and criminal offence data for the purpose of exercising its statutory obligations under HSWA 1974.</i>	

Reference	Title
Part 2(8)	Equality of Opportunity
<i>HSE may process data concerning racial or ethnic origin, religious or philosophical beliefs, sexual orientation and health for the purposes of monitoring equality of opportunity or treatment between groups of its employees with a view to enabling such equality to be promoted or maintained.</i>	
Part 2(9)	Racial and ethnic diversity at senior levels in HSE
<i>HSE may process data concerning racial or ethnic origin for the purposes of promoting and maintaining diversity in the racial and ethnic origins of individuals who hold senior positions in our organisation.</i>	
Part 2(10)	Preventing or detecting unlawful acts
<i>HSE may process data concerning health and criminal offences for the purposes of preventing and detecting crimes.</i>	
Part 2(11)	Protecting the public against dishonesty etc.
<i>HSE may process data concerning criminal convictions for the purpose of protecting the public from serious harm caused by dishonest or non-compliant working practices.</i>	
Part 2(12)	Regulatory requirements relating to unlawful acts and dishonesty
<i>HSE may process data concerning health and criminal offences for the purposes of its core regulatory functions as defined under HSWA 1974. This includes (but is not limited to) investigations into workplace health and safety incidents or instances of occupational ill health, and for the prosecution of serious criminal breaches of health and safety law.</i>	
Part 2(13)	Journalism etc. in connection with unlawful acts and dishonesty etc.
<i>HSE may publish personal data concerning criminal offences associated with the commission of unlawful acts by a person or dishonesty, malpractice or other seriously improper conduct by a person where HSE believes that publication is in the public interest</i>	

HSE also processes special category data and criminal offence data under the following DPA 2018, Schedule 8 conditions;

Reference	Title
Paragraph 1	Statutory etc purposes
<i>HSE may process data concerning racial or ethnic origin, religious or philosophical beliefs, trade union membership, sexual orientation, health and criminal offence data for the purposes of exercising a function conferred by law, and where it is necessary for reasons of substantial public interest.</i>	
Paragraph 4	Safeguarding of children and of individuals at risk
<i>HSE may process data concerning health and criminal offences for reasons of substantial public interest, to protect them from harm or to protect their well-being.</i>	
Paragraph 5	Data already in the public domain
<i>HSE may process any of the special category data for law enforcement purposes where the data subject has deliberately made the information public.</i>	
Paragraph 6	Legal claims
<i>HSE may process data concerning criminal convictions for the purpose of establishment, exercise or defence of a legal claim.</i>	
Paragraph 8	Preventing fraud
<i>HSE may publish personal data concerning criminal offences associated with the commission of unlawful acts by a person or dishonesty, malpractice or other seriously improper conduct by a person where it is necessary for the purposes of preventing fraud. If it involves sharing data with organisations that do not fall within the definition of a competent authority, the processing needs to comply with the UK GDPR, and we need an Article 6 lawful basis for sharing the data.</i>	
Paragraph 9	Archiving etc
<i>HSE may archive special category data collected for law enforcement purposes where it is in the public interest, for scientific or historical research purposes or for statistical purposes. However, HSE cannot use it if it will result in decisions being made that affect a particular individual, or is likely to cause substantial damage or substantial distress to an individual.</i>	

HSE does not process genetic data, or biometric data for the sole purpose of identifying a natural person. Furthermore, HSE does not process personal data concerning political opinion.

Compliance with Data Protection Principles

HSE follows the data protection principles set out in Article 5 of the UK GDPR, and Part 3, Chapter 2 of the DPA 2018 for law enforcement processing, as follows.

Accountability and Governance

In accordance with the accountability principle, HSE maintains Records of Processing Activities (ROPA) under Article 30 of the UK GDPR and section 61 of the DPA 2018.

Nominated Information Asset Owners (IAOs) must identify their information assets, and specifically those which contain sensitive processing. IAOs are required to complete an annual Assurance Statement for their assets. The assurance statement contains questions that refer to the data protection principles and ask the IAO to provide evidence and assurances as to how they are ensuring compliance with these statements. Any concerns raised within these assurance statements are brought to the attention of relevant stakeholders, i.e. IAO, system owners, IT, Information Security, Information Management Team, Data Protection Officer and the Senior Information Risk Owner (SIRO).

We carry out data protection impact assessments (DPIAs) where appropriate in accordance with Articles 35 and 36 of the UK GDPR and section 64 of the DPA 2018 to ensure data protection by design and by default. We have documented procedures in place whereby DPIAs must be completed by relevant business areas when processing meets certain criteria. These mirror those criteria documented within the legislation and on the Information Commissioner's Office (ICO) website. This process is also embedded with the Project and Procurement Processes.

In accordance with UK GDPR Article 37 and based on its status as a UK public authority, HSE has appointed a permanent Data Protection Officer (DPO).

In addition, we have effective breach notification systems and procedures in place that ensure timely reporting to the ICO (where necessary) and appropriate actions are taken to limit the impact of the breach on the affected data subjects.

Lawfulness, Fairness and Transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

HSE will;

- ensure that personal data is only processed where it is lawful to do so
- ensure a lawful basis for processing personal data is identified against each business function, and set out within our ROPA
- ensure that data subjects are appropriately informed of all processing activities performed by HSE on their personal data (excluding certain areas of law enforcement processing). This will be achieved through the use of privacy notices published on our website.

Purpose Limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

HSE will;

- only collect personal data for specified, explicit and legitimate purposes
- inform data subjects of those purposes via the published privacy notice and other notification mechanisms
- not use personal data for purposes that are incompatible with the purposes for which it was collected.
- Inform the data subject before using personal data for a new purpose that is not compatible with the original purpose.

Data Minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

HSE will;

- only process the minimum personal data needed for the purpose for which it is collected
- ensure that the data we collect is adequate and relevant
- ensure the least intrusive personal data processing method is adopted in each instance

- Periodically review data held and delete anything no longer required

Accuracy

Personal data shall be accurate and, where necessary, kept up to date.

HSE will;

- Ensure appropriate processes are in place to check the accuracy of the data we create and collect, and to maintain that accuracy for the duration of the processing
- Ensure the sources of the personal data we create and collect are reliable
- Ensure the individual's right to rectification is observed and applied in a timely manner

Storage Limitation

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

HSE will;

- be aware of the personal data held and why it is needed
- give due consideration and justification for the retention of personal data
- ensure personal data is destroyed in accordance with HSE's business classification scheme and disposal [policy](#)
- regularly review and erase or anonymise personal data no longer required
- ensure processes are in place that observe and enforce the data subjects' right to erasure

Integrity and Confidentiality

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

HSE will;

- ensure that there appropriate organisational and technical measures in place to protect personal data
- maintain Cyber Essentials security accreditation at all times
- provide annual data protection training to all staff
- employ technical security controls to secure sensitive information within systems
- implement role-based access controls to restrict access to sensitive data

Other appropriate safeguards in place to secure compliance with data protection principles include:

- Policies, procedures, guidance, roles and responsibilities, and mechanisms of reporting to the SIRO and accountable officer
- Assurance check processes in place to monitor compliance with policies and procedures
- Training and awareness provision
- Data Processing Contracts with third parties undertaking processing on our behalf
- Information Sharing Agreements with regular recipients of data.

Document Administration

First published: August 2022

Revised: September 2025

Version no. 1.2

Version	Date	Amendment	Author
1.0	17 August 2022	First draft	S Eagan
1.1	30 August 2024	Review. The following additions have been made: Schedule 8 conditions Governance and Accountability considerations Other appropriate safeguards in place to secure compliance with data protection principles.	M Leszczynska
1.2	4 September 2025	Transferred on to HSE's corporate template.	M Leszczynska

Further information

For information about health and safety, or to report inconsistencies or inaccuracies in this guidance, visit [the HSE website](#).

You can order HSE priced publications at [the HSE books website](#).

HSE priced publications are also available from bookshops.

This publication is available on the HSE website [here](#)

© Crown copyright If you wish to reuse this information visit [the HSE website](#) for details. First published 08/22.

Published by the Health and Safety Executive 09/25.