Foundations
What Works Centre for Children & Families

APPROPRIATE POLICY DOCUMENT

As part of Foundations' work with vulnerable individuals, we process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation ('UK GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Special Category Data

Special category data is defined at Article 9 of the UK 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; or
- Data concerning a natural person's sex life or sexual orientation.

Criminal Offence Data

Article 10 of the UK GDPR covers processing in relation 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'.

This Document

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in 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. This information supplements our Privacy Notice.

Our conditions for processing special category and criminal offence data

We process special categories of personal data under the following of the UK GDPR Articles:

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

Examples of our processing include staff sickness absences.

ii. Article 9(2)(j) – for archiving purposes in the public interest.

The relevant purpose we rely on is Schedule 1 Part 1 paragraph 4 – archiving.

An example of our processing is the transfers we make to the Office for National Statistics so that other organisations may access the information for their own studies.

iv. Article 9(2)(f) – for the establishment, exercise or defence of legal claims.

Examples of our processing include processing relating to any employment tribunal or other litigation.

v. Article 9(2)(a) – explicit consent

In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

Examples of our processing include staff dietary requirements and health information we receive from our employees who require a reasonable adjustment.

vi. Article 9(2)(c) – where processing is necessary to protect the vital interests of the data subject or of another natural person.

An example of our processing would be using health information about an employee in a medical emergency.

We process criminal offence data under Article 10 of the UK GDPR.

Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations. As Foundations carries on work with children and vulnerable individuals, we may carry on background and DBS checks concerning spent and unspent convictions, we do this under the following Schedule 1 conditions:

Vii Schedule 1. (1) – Employment, social security and social protection

Viii Schedule 1. (18) – Safeguarding of children and of individuals at risk

Ix Schedule 1, part 3 (31) – Processing by not-for-profit bodies

Processing requiring a policy document

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD (see Schedule 1 paragraphs 1 and 5).

This section of the policy is the APD for Foundations. It demonstrates that the processing of special category ('SC') and criminal offence ('CO') data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. It outlines our retention policies with respect to this data.

Description of data processed

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 their membership of any trade union. Further information about this processing can be found in our employee privacy notice.

Our processing for reasons of substantial public interest relates to the data we receive or obtain in order to fulfil our obligations towards our funders and conduct our research. Further information about this processing can be found in our privacy notice which can be found online.

We also maintain a record of our processing activities in accordance with Article 30 of the UK GDPR.

Schedule 1 conditions for processing

Special category data

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

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

We process SC 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 8(1)** equality of opportunity or treatment
- **Paragraph 9 (1)** racial and ethnic diversity at senior levels of an organisation
- **Paragraph 10(1)** preventing or detecting unlawful acts
- **Paragraph 11(1) and (2)** protecting the public against dishonesty

Criminal offence data

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

- **Paragraph 31** – Processing by not for profit bodies

How we comply with the privacy principles

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
- Maintaining documentation of our processing activities
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors as well as with joint controllers
- Implementing appropriate security measures in relation to the personal data we process
- Carrying out data protection impact assessments for our high-risk processing

We regularly review our accountability measures and update or amend them when required.

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, staff privacy notice and this policy document.

Our processing for purposes of substantial public interest is necessary for the exercise of our research activities

Our processing for the purposes of employment relates to our obligations as an employer.

Principle (b): purpose limitation

We process personal data for purposes of substantial public interest as explained above when the processing is necessary for us to fulfil our functions, where it is necessary for complying with or assisting another to comply with a regulatory requirement, as well as the reasons listed above.

We are authorised by law to process personal data for these purposes. We may process personal data collected for any one of these purposes (whether by us or another controller), for

any of the other purposes here, providing the processing is necessary and proportionate to that purpose.

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 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 retention policy. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention policy is reviewed regularly and updated when necessary.

Principle (f): integrity and confidentiality (security)

Electronic information is processed within our secure network. 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.

Retention and Erasure

Our retention and erasure practices are set out in our retention policy

Review date of this Appropriate Policy Document

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

This policy will be reviewed annually or revised more frequently if necessary.

Processing additional special category data

We process special category personal data in other instances where it is not a requirement to keep an appropriate policy document. Our processing of such data respects the rights and interests of the data subjects. We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice and employee privacy notice.