

# **DATA PROTECTION OF STAFF RECORDS POLICY**

## **1.0 Aim and scope of policy**

1.1 This policy applies to the processing of personal data in manual and electronic records kept by the Council in connection with its employees as described below. It also covers the Council's response to any data breach and other rights under the UK General Data Protection Regulation and Data Protection Act 2018.

1.2 This policy also applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as "relevant individuals".

1.3 The Clerk is the person responsible for managing the Council's data compliance.

## **2.0 Definitions**

2.1 "Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

2.2 "Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

2.3 "Criminal offence data" is data which relates to an individual's criminal convictions and offences.

2.4 "Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

## **3.0 Council commitment**

3.1 The Council makes a commitment to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with GDPR and English law and all its employees conduct themselves in line with this, and other related, policies. Where third parties process data on behalf of the Council, the Council will ensure that the third party takes such measures in order to maintain the Council's commitment to protecting data. In line with current data protection legislation, the Council understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

## **4.0 Types of data held**

4.1 Personal data is kept in personnel files or any of the Council's HR systems. The following types of data may be held by the Council, as appropriate, on relevant individuals:

- name, address, phone numbers - for individual and next of kin
- application forms, CVs and other information gathered during recruitment
- references from former employers
- National Insurance numbers
- job title, job descriptions and pay grades
- conduct issues such as letters of concern, disciplinary proceedings
- holiday records
- internal performance information
- medical or health information
- sickness absence records
- tax codes
- terms and conditions of employment
- training details.

4.2 The Council will tell relevant individuals of the personal data it processes, the reasons for processing their personal data, how it uses such data, how long it will retain the data, and the legal basis for processing in its privacy notices.

4.3 The Council will not use personal data of relevant individuals for an unrelated purpose without telling them about it and the legal basis that it intends to rely on for processing the data. The Council will not process their personal data if it does not have a legal basis for processing.

4.4 The Council keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

4.5 Relevant individuals should refer to the Council's privacy notice for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

## **5.0 Data protection principles**

5.1 All personal data obtained and held by the Council will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes of processing
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- not be kept for longer than is necessary for its given purpose
- be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- comply with the relevant data protection procedures for international transferring of personal data.

5.2 In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict the processing of the data
- the right to portability

- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

## 6.0 Processing data

### *Personal data*

6.1 The council will process the personal data of relevant individuals (that is not classed as special categories of personal data) for one or more of the following reasons:

- it is necessary for the performance of a contract, e.g., a contract of employment (or services); and/or
- it is necessary to comply with any legal obligation; and/or
- it is necessary for the council's legitimate interests (or for the legitimate interests of a third party), unless there is a good reason to protect personal data which overrides those legitimate interests; and/or
- it is necessary to protect the vital interests of a data subject or another person; and/or
- it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

6.2 If the Council processes the personal data of relevant individuals (excluding special categories of personal data) in line with one of the above bases, it does not require a consent from the individual. Otherwise, the council is required to gain their consent to process their personal data. If the council asks for their consent to process personal data, then it will explain the reason for the request. Consent does not have to be given or can be withdrawn later.

6.3 The Council will not use the personal data of relevant individuals for an unrelated purpose without telling them about it and the legal basis that it intends to rely on for processing it.

6.4 Personal data gathered during employment is held in individual personnel files in hard copy and may also be held in electronic format on HR and IT systems and servers. The periods for which the council holds HR-related personal data are contained in the privacy notices to individuals.

6.5 Sometimes the Council will share the personal data of relevant individuals with contractors and agents to carry out its obligations under a contract with the individual or for its legitimate interests. The Council requires those individuals or companies to keep this personal data confidential and secure and to protect it in accordance with Data Protection law and the Council's policies. They are only permitted to process that data for the lawful purpose for which it has been shared and in accordance with our instructions.

6.6 The Council will update HR-related personal data promptly if a relevant individual advises that their information has changed or is inaccurate (e.g. a change of address). The relevant individual may be required to provide documentary evidence in some circumstances.

6.7 The Council keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

### *Special categories of data*

6.8 The Council will only process special categories of personal data (see above) on the following basis in accordance with legislation:

- where it is necessary for carrying out rights and obligations under employment law or a collective agreement
- where it is necessary to protect the vital interests of a relevant individual or those of another person where the individual is physically or legally incapable of giving consent

- where a relevant individual has made the data public
- where it is necessary for the establishment, exercise or defence of legal claims
- where it is necessary for the purposes of occupational medicine or for the assessment of the working capacity of a relevant individual
- where it is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates to only members or former members provided there is no disclosure to a third party without consent
- where it is necessary for reasons for substantial public interest, on the basis of law, which is proportionate to the aim pursued and which contains appropriate safeguards
- where it is necessary for reasons of public interest in the area of public health; and
- where it is necessary for archiving purposes in the public interest or scientific and historical research purposes.

6.9 If the Council processes special categories of the personal data of relevant individuals in line with one of the above bases, it does not require the individual's consent. In other cases, the Council is required to gain consent to process any special categories of personal data. If the council asks for consent to process a special category of personal data, then we will explain the reason for the request. Relevant individuals do not have to consent or can withdraw consent later.

## 7.0 Access to data

7.1 Relevant individuals have a right to be informed whether the Council processes personal data relating to them and to access the data that the Council holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

- request must be made by letter or email to the Clerk
- the Council will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request
- the Council will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.

7.2 Relevant individuals must inform the Council immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. The Council will take immediate steps to rectify the information.

## 8.0 Data disclosures

8.1 The Council may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- any employee benefits operated by third parties
- disabled individuals - whether any reasonable adjustments are required to assist them at work
- individuals' health data - to comply with health and safety or occupational health obligations towards the employee
- for Statutory Sick Pay purposes
- HR management and administration - to consider how an individual's health affects his or her ability to do their job
- the smooth operation of any employee insurance policies or pension plans.

These kinds of disclosures will only be made when strictly necessary for the purpose.

## **9.0 Data security**

9.1 The Council adopts procedures designed to maintain the security of data when it is stored and transported.

9.2 In addition, employees must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- refrain from sending emails containing sensitive work-related information to their personal email address
- check regularly on the accuracy of data being entered into computers
- always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them
- use computer screen blanking to ensure that personal data is not left on screen when not in use.

9.3 Where personal data is recorded on laptops, portable drives, USB sticks or similar devices be kept or transported on laptops, USB sticks, or similar devices, it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary
- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
- ensuring that laptops or USB drives are not left lying around where they can be stolen.

9.4 Failure to follow the Council's rules on data security may be dealt with via the Council's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

## **10.0 Breach notification**

10.1 Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of the Council becoming aware of it and may be reported in more than one instalment.

10.2 Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.

10.3 If the breach is sufficient to warrant notification to the public, the Council will do so without undue delay.

## **11.0 Training**

11.1 New employees must read and understand the policies on data protection as part of their induction.

11.2 All employees will receive training covering confidentiality, data protection and the actions to take upon identifying a potential data breach, and in understanding the consequences of any potential lapses and breaches of the Council's policies and procedures.

## **12.0 Records**

12.1 The Council keeps records of its processing activities including the purpose for the processing and retention period. These records will be kept up to date by the Clerk.