



Privacy Statement

REF: HR/Privacy statement
Oct 2022

Introduction:



The Council is entitled to hold and process personal data electronically and manually for compliance with its legitimate interests and in order to perform its legal obligations. The Council acts as a Data Controller and Data Processor. The Council ensures it complies with its obligations to ensure the personal data it retains is accurate and necessary and is stored in compliance with its legal obligations towards all data subjects.

Scope:

The privacy statement applies to applicants and former applicants (successful and unsuccessful), employees, agency workers, casual workers, contract workers (current and former), volunteers including elected representatives of the Council and work experience placements.

Transfer of Data:

In accordance with its rights to process personal data, the Council may at any time and without the knowledge of the Data Subject, transfer personal data about the Data Subject to third party service providers in order to meet its contractual or legal obligations and/or as part of the means by which the Council organises its operations. The Council will use its best endeavours to ensure that any data it transfers is accurate and complete at the point of transfer.

The Council will transfer data to such third-party agencies to enable such third parties to carry out processing activities defined and prescribed by the Council. Such third parties will carry out such activities under the direction and control of the Council and will comply with the Council's data protection policies and procedures. The Council may use third parties who are based outside of the European Union, and where this is the case, the Council will use its best endeavours to ensure the security of data.

The Council may also be required to transfer personal data about a data subject to other agencies to fulfil its legal obligations and for health and safety reasons.

Such agencies may include but are not limited to HMRC, benefit providers, and law enforcement agencies, medically trained professionals for the purpose of protection and conserving the Data Subject's health and wellbeing and others who may be required to provide treatment and guidance in the event of a medical incident. The Data Subject will not necessarily be notified that the Council has been required to submit information to such agencies.



The Council will use its best endeavours to advise third parties of any requirements to erase or restrict or make corrections to the processing of personal data normally within one month of any change being agreed.

Data the Council may Collect, Retain, Process and Analyse:

The Council will require the Data Subject to provide information and the Council may obtain information about the Data Subject from third party providers and subject information will be retained, processed and analysed as considered necessary by the Council for its legitimate purposes. The information the Council may collect, retain, process and analyse may vary from time-to-time and will be considered on a case-by case basis but may include and is not limited to a data subject's:

- Names, address, contact details, date of birth, national insurance number, right to work evidence, email address, phone numbers, gender, next of kin, protected characteristics, unspent criminal convictions, results of DBS checks, emergency information including medical practitioner, medical screening data, banking information for payment of salary and expenses, pay and pay rates bonus and commission and overtime rates and payments, hours of work, tax codes, student loan information, records of orders for deductions from pay in regard to deductions from pay the Council is required to make for statutory purposes, qualifications, membership of enrolment in benefit and training programmes provided by the Council, absence records including self-certification and fitness certificates, medical reports holiday requests and other holiday tracking, references, disclosures of conflicts of interest and personal relationships, CV and letters of application and associated recruitment tests and scores, records of application and previous work history, records in relation to roles undertaken within the Council, performance evaluations, improvement plans, disciplinary warnings and investigations, periods of suspension appeals retained in accordance with the Council procedure, records and requests in relation to the family friendly policies operated by the Council, records in relation to grievances and other matters in relation to actioning statutory rights of enacting the policies operated by the Council, credit checks and other security checks, driving licence data and accident investigations and other data the Council requires for compliance with its health and safety obligations, information in relation to use of and access of the Council's information and communication systems and equipment, photographs and videos featuring the Data Subject, CCTV footage and other information obtained through electronic means such as swipe card records.

Data subjects are required to cooperate fully with the Council's reasonable requests for such information and to use their best endeavours to ensure the responses that the Data Subject supplies are accurate. In the event that a Data Subject unreasonably refuses to comply with the Council's reasonable requests for the Data Subject to supply personal data or to update personal data, the Employee will be deemed to be in breach of his/her obligations and the contractual relationship will terminate.

The Council may analyse data about data subjects either on an individual basis or as subsets of groups for management purposes.

Access to Personal Information:



Information will normally be stored by manual and electronic means. The Council will store personal information in a manner which minimises the risk of unauthorised or unlawful processing, accidental loss, destruction or damage, and a data access breach. Those entrusted with access to personal information will be required to adopt measures when accessing or using personal data which minimises the risk of a data access breach.

Access to personal information will be restricted to a need-to-know basis.

Keeping Information up-to-date and Accurate:

The Council will use its best endeavours to ensure the information it holds in relation to data subjects is valid and complete. The Data Subject is required to notify the Council of changes to his/her personal information and the Council will update such information on its systems and records, normally within one month of such notification. From time-to-time the Council will conduct measures to verify the data it holds is accurate. Where data subjects are asked to verify the information the Council holds about them, the Data Subject is required to cooperate fully with such requests. Updates from such verification procedures will normally be made as soon as reasonably practical and normally within one month.

The Council will use its best endeavours to correct any errors or omissions in its data about a data subject. Where information which is inaccurate or contains omissions has been passed to a third-party, the Council will use its best endeavours to correct the information which has been submitted to a third-party within one month of becoming aware of the error or omission.

Right to Rectify Inaccurate or Incomplete Data:

The Council will endeavour to ensure the data it uses is complete and accurate. Where for whatever reason data is not accurate or complete, the Data Subject should notify the Council, normally via a Manager. The Council will endeavour to make any corrections as soon as reasonably practical, normally within one month. If a Data Subject is not satisfied with the Council's responses, the Data Subject should submit a complaint using the procedure below.

Obligations for those who have Access to Personal Data:

From time-to-time data subjects and other third parties will be entrusted with access to personal data including sensitive data. Those entrusted with such information must ensure any data is stored appropriately to protect its confidentiality and must not disclose such information to any other person or organisation unless authorised to do so. Those entrusted with access to such data agree to apply their best endeavours to ensure any personal data they become party to remains confidential.

When data, which includes personal data, is due to be transferred to third parties, prior to any transfer taking place those transferring such information will carry out checks to verify the request is genuine and for a legitimate purpose and the information being transferred is necessary and in accordance with the Council's rights and will verify that the recipient has provided assurance that the information once transferred will be treated in a confidential manner.

Restrictions on the Processing of Personal Data including Erasure:



A data subject may request that data is not processed or is erased or 'forgotten'. The Council will consider such requests. The Council will normally notify the Data Subject of the outcome of any request within one month.

Retention of Information:

Information will normally be retained by the Council for as long as necessary. This may vary on a case-by-case basis. In general, detailed records will be retained for a maximum of seven years after the Data Subject's engagement has terminated. After this time only a record of the Data Subject's record for reference purposes will be retained.

Disposal of Manual Records and Devices used to store Personal Data:

The Council will ensure when disposing of manual records containing personal data that such records are treated to protect the confidentiality of such personal data. When disposing of devices which have been used for the storage of personal data, the Council will ensure such devices are wiped clean.

Automated Decision Making The Council does not routinely apply automated decision-making mechanisms such as profiling in order to make decisions. Where some automation is applied, any outcomes are reviewed by the Chairperson of the Council.

Use of Close Circuit Television (CCTV):

CCTV may be used in areas of the Council premises and from time-to time in vehicles to monitor compliance with the Council's rules for operation, for keeping data subjects safe and secure by preventing crime, ensuring health and safety compliance, for communication, for monitoring and verifying activity, performance and conduct and for security purposes. Evidence gathered from surveillance cameras may also be passed to legal enforcement agencies as evidence to support prosecutions for wrongdoing. The Council may locate covert surveillance cameras from time-to time at locations around the premises of the Council where the Council has a reasonable belief of wrongdoing, however such surveillance equipment will not be located in areas which constitute areas of high risk of infringing a data subject's right to privacy such as toilets, and facilities used for changing and showering.

Complaints:

In the event a data subject has a concern in regard to the manner in which personal data is controlled or processed, the Data Subject should notify the Council's nominated Data Controller, which is the Clerk or in the absence of a nominated Data Controller the Chairperson of the Council. In the event a data subject still has concerns, a data subject has a statutory right to make a complaint to a supervisory authority.

*Proposed ordinary council meeting
11 October 2022*