**Workforce Data Protection Policy**

***Version 2.0 (02 Dec 2019)***

[1. Introduction 2](#_Toc513115275)

[***Data protection definitions*** 2](#_Toc513115276)

[2. Data protection principles 3](#_Toc513115277)

[3. Individual rights 4](#_Toc513115278)

[***Subject access requests*** 4](#_Toc513115279)

[***Other rights*** 5](#_Toc513115280)

[4. Data security 5](#_Toc513115282)

[5. Impact assessments 6](#_Toc513115283)

[6. Data breaches 6](#_Toc513115284)

[7. International data transfers 6](#_Toc513115285)

[8. Individual responsibilities: how should you process personal data for the council? 6](#_Toc513115286)

[Appendix 1: Workforce Privacy Notice – Croydon Council 9](#_Toc513115287)

[1. Overview 9](#_Toc513115288)

[2. What information does the council collect? 9](#_Toc513115289)

[3. Why does the council process personal data? 11](#_Toc513115290)

[4. How does the council process special categories of personal data? 12](#_Toc513115291)

[5. Who has access to data? 13](#_Toc513115292)

[6. How does the council protect data? 14](#_Toc513115293)

[7. For how long does the council keep data? 14](#_Toc513115294)

[8. Your rights 14](#_Toc513115295)

[9. What if you do not provide personal data? 15](#_Toc513115296)

[10. Automated decision-making 16](#_Toc513115297)

1. **Introduction**

The council takes the security and privacy of data seriously and is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. We comply with our legal obligations under the Data Protection Act 2018 (the “2018 Act”) and the EU General Data Protection Regulation (“GDPR”). This policy sets out the council's commitment to data protection, and individual rights and obligations of its workforce in relation to personal data.

This policy applies to employees, workers, consultants, volunteers, interns, apprentices and former employees and their personal data referred to as ***HR-related personal*** data. If you fall into one of these categories then you are a ‘data subject’ for the purposes of this policy. The policy explains how the council will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of the council. This policy replaces the ‘Data Protection of Employment Related Personal Data Policy’ within the council’s HR handbook.

General concerns and queries relating to data protection and information management should in the first instance be directed to the Information Management Team [informationmanagement@croydon.gov.uk](mailto:informationmanagement@croydon.gov.uk). Questions about this policy, or requests for further information, should in the first instance be directed to Jennifer Sankar, Head of Human Resources at Jennifer.Sankar@croydon.gov.uk

## 

## ***Data protection definitions***

**"Personal data"** is any information that relates to a living individual who can be identified from that information (a “data subject”) on its own, or when taken together with other information which is likely to come into the council’s possession. It includes any expression of opinion about the person and indication of the intentions of the council or others, in respect of that person. It does not include anonymised data.

**"Special categories of personal data"** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic or biometric data.

**"Criminal records data"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

**“Data Processing”** means any use that is made of personal data, including collecting, recording, organising, combining, structuring, storing, amending, retrieving or consulting, disclosing (by transmission, dissemination or otherwise making available) or restricting or destroying data.

This includes processing personal data which forms part of a filing system and any automated processing**.**

1. **Data protection principles**

Personal data must be processed in accordance with six ‘data protection principles’ it must:

* Be processed fairly, lawfully and transparently;
* Be collected and processed only for specified, explicit and legitimate purposes;
* Be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
* Be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
* Not be kept for longer than is necessary for the purposes for which it is processed; and .
* Be processed securely. To that end the council adopts appropriate measures to make sure that personal data is secure and protected against unauthorised or unlawful processing and accidental loss, destruction or damage.

We are accountable for these principles and must be able to show that we are compliant.

The reasons for processing an individual’s personal data, how it uses such data and the legal basis for processing is explained in the ***Workforce Privacy Notice and Job Applicant*** ***Privacy Notice*** and within the ***HR Records Retention Policy***.

The council will not process personal data of individuals for other reasons. Where the council relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where the council processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with the details outlined in the ***Workforce Privacy Notice or Job Applicant Privacy Notice.***

The council will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate. Please refer to the ***Workforce Privacy Notice*** for further information on this process.

Personal data gathered during the employment or apprenticeship relationship, is held in the individual's personnel file (if the person is an employee) as well as in hard copy or electronic format, or both. Other categories of workers at the council may not have a ‘personnel file’ (although basic details for agency workers may be held on One Oracle). Additional information on other types of workers as well as employees may also be held on electronic systems such as My Resources and SharePoint. The periods for which the council holds HR-related personal data are contained in its ***HR Records Retention Policy.***

The council keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the GDPR.

1. **Individual rights**

As a data subject, individuals have a number of rights in relation to their personal data.

## ***Subject access requests***

Individuals have the right to request a copy of their personal data being processed by the council and on doing so, the council will signpost or supply the ***Workforce*** ***Data Protection Policy****,* ***HR Records Retention Policy*** and ***Job Applicant Privacy* Notice**. These documents stipulate the procedures around employee data processing within the council.

The council will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

A subject access request does not necessarily extend to all records or correspondence containing the individual’s name or personal identifier. To be included in a response to a subject access request, the information needs to relate to, be about or be linked to the individual. The council may ask the individual to specify the information to which the request relates.

To make a subject access request, the individual should send the request to [SAR@croydon.gov.uk](mailto:SAR@croydon.gov.uk). In some cases, the council may need to ask for proof of identification before the request can be processed. The council will inform the individual if they need to verify their identity and the documents which are required.

The council must respond within one month, unless the request is complex or numerous in which case the period in which the council must respond can be extended by a further two months. The council will write to the individual within one month of receiving the original request to explain why the extension is necessary.

If a subject access request is manifestly unfounded or excessive, the council is not obliged to comply with it. Alternatively, the council can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request.

A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the council has already responded. If an individual submits a request that is unfounded or excessive, the council will notify them that this is the case and whether or not the council will respond to it.

Where the council refuses to respond to a request, it must explain why to the individual, informing them of their right to complain to the Information Commissioner’s Office and to a judicial remedy without undue delay and at the latest within one month.

## ***Other rights***

Individuals have a number of other rights in relation to their personal data:

* Individuals have the right to information about what personal data the council processes, how and on what basis;
* Individuals can correct inaccuracies in their personal data;
* They have the right to request that the council stops processing or erases their personal data that is no longer necessary to process for the purpose it was collected;
* Individuals have the right to object to data processing or erase data if the individual's interests override the council's legitimate grounds for processing data (where the council relies on its legitimate interests as a reason for processing data);
* Individuals have the right to require the council to stop processing or erase data if processing is unlawful; and
* While they are requesting that their personal data is corrected or erased or are contesting the lawfulness of processing, individuals can apply for its use to be restricted
* Individuals have the right to object if the council processes their personal data for the purposes of direct marketing;
* Individuals have the right to receive a copy of their personal data and (excluding paper files) to transfer their personal data to another data controller;
* With some exceptions individuals have the right not to be subjected to automated decision making;
* Individuals have the right to be notified of a data security breach concerning their personal data where this will result in a high risk to your rights and freedoms;
* In most situations the council will not rely on an individual’s consent as a lawful ground to process their data. If we do however, request their consent to the processing of their personal data for a specific purpose, individuals have the right not to consent or to withdraw their consent later.

To ask the council to take any of these steps, the individual should send the request to [human.resources@croydon.gov.uk](mailto:human.resources@croydon.gov.uk).

1. **Data security**

The council takes the security of personal data seriously. The council has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. Information management policies are applicable to personal data and confirm the controls around data handling in the council.

The relevant ICT and security and information management policies including users’ responsibilities can be found here:

* [ICT and security and information management policies](https://intranet.croydon.gov.uk/lbc-policy-manager/acceptableuse.html)

Where the council engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data in accordance with GDPR standards.

1. **Impact assessments**

Some of the processing that the council carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the council will carry out a data protection impact assessment to determine the necessity and proportionality of processing.

This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

1. **Data breaches**

If the council discovers that there has been a breach of personal data (whether in respect of you or someone else) that is likely to be a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The council will record all data breaches in a register regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

**If you are aware of a data breach or a suspected data breach, you must immediately notify your manager and report it to the Information Management Team at** [**data.breach@croydon.gov.uk**](mailto:data.breach@croydon.gov.uk) **and keep any evidence you have in relation to the breach.**

1. **International data transfers**

The council will not transfer HR-related personal data to countries outside the EEA.

1. **Individual responsibilities: how should you process personal data for the council?**

Employees and workers for the council are responsible for helping the council keep their personal data up to date. Employees are responsible for reviewing and updating their personal records on the HR system through employee self-service facility for example if they move house or have changes to their bank details.

Everyone who works for or on behalf of the Council may have access to the personal data of other individuals and our customers/residents in the course of their employment, contract, volunteer period, internship or apprenticeship.

Where this is the case, the council relies on individuals to help meet its data protection obligations to other staff and to customers/residents. Everyone who works for, or on behalf of the Council has responsibility for ensuring data is collected, stored and processed appropriately, in line with this policy and the council’s data security and Data Retention policies.

**Individuals who have access to personal data are required:**

* To access only data covered by this policy if it is needed for the work they do and that they have authority to access. Data should only be used for the specific lawful purpose for which it was obtained;
* Not to disclose data except to individuals (whether inside or outside the council) who have appropriate authorisation;
* Not make any unnecessary copies of personal data;
* To keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
* Not to remove personal data, or devices containing or that can be used to access personal data, from the council's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
* Not to store personal data on local drives or on personal devices that are used for work purposes;
* To use only your council approved email account for email communications whilst working for the Council and not to send emails or transfer attachments using a personal email account;
* To lock drawers and filing cabinets. Do not leave personal data unattended;
* To dispose of personal data securely when finished with it by shredding or use of confidential waste bins;
* To report data breaches of which they become aware to the Information Management Team at [data.breach@croydon.gov.uk](mailto:data.breach@croydon.gov.uk) immediately;
* To ask for help if you are unsure about data protection or if you notice any areas of data protection or security which can be improved upon from the information management team at information.management@croydon.gov.uk.

Further details about the council's security procedures can be found in the information management policies on the intranet: <https://intranet.croydon.gov.uk/working-croydon/information-management/guidance-and-policy-documents>

**Everyone who works for the council has a responsibility to familiarise themselves with the information management policies and procedures (above) and undertake any data protection training that is provided.**

Failing to observe data protection requirements may amount to a disciplinary offence, which will be dealt with under the council's disciplinary procedure.

**Significant negligent or deliberate breaches of council policies, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.**

It is a criminal offence to conceal or destroy personal data which is part of a subject access request. This conduct would also amount to gross misconduct which could result in your dismissal without notice. Likewise under Section 170 of the Data Protection Act 2018 it is an offence for a person to knowingly or recklessly obtain or disclose personal data of another person without the consent of the Council. Where this occurs, the Council will refer the incident to the Information Commissioner’s Office for investigation and maybe prosecution.

End

**Appendix 1**:

**Workforce Privacy Notice – Croydon Council**

***Drafted: May 2018***

***Updated : Dec 2019***

**Data controller: Croydon Council**

**Data protection officer: Sandra Herbert**

[1. Overview 8](#_Toc512520438)

[2. What information does the council collect? 9](#_Toc512520439)

[3. Why does the council process personal data? 11](#_Toc512520440)

[4. How does the council process special categories of personal data? 12](#_Toc512520441)

[5. Who has access to data? 13](#_Toc512520442)

[6. How does the council protect data? 14](#_Toc512520443)

[7. For how long does the council keep data? 14](#_Toc512520444)

[8. Your rights 14](#_Toc512520445)

[9. What if you do not provide personal data? 15](#_Toc512520446)

[10. Automated decision-making 16](#_Toc512520447)

1. **Overview**

The council collects and processes your personal data, (including special categories of personal data) in accordance with our obligations under the Data Protection Act 2018 and the GDPR.

We will use your personal data for:

* Performing the contract of employment or contract for services between us;
* Complying with any legal obligation, or
* If it is necessary for our legitimate interests or of the legitimate interests of someone else. However, we can only do this if your interests and rights do not override ours or theirs. You have the right to challenge our legitimate interests and request that we stop this processing.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

General concerns and queries relating to data protection and information management should in the first instance be directed to the Information Management Team [informationmanagement@croydon.gov.uk](mailto:informationmanagement@croydon.gov.uk).

1. **What information does the council collect?**

The council collects and processes a range of information about you. This may include:

* Your name, address and contact details, including email address and telephone number, date of birth and gender;
* The terms and conditions of your employment or engagement;
* Details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the council;
* Information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
* Details of your bank/building society account and national insurance number;
* Information about your marital status, next of kin, dependants and emergency contacts;
* Information about your nationality and entitlement to work in the UK and information from related documents such as your passport or other identification information;
* Information about your criminal record where relevant to your employment;
* Details of your schedule (days of work and working hours) and attendance at work;
* Details of periods of leave taken by you, including holiday, sickness absence, family leave and unpaid leave, and the reasons for the leave;
* Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
* Assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
* Information about medical or health conditions, including whether or not you have a disability for which the council needs to make reasonable adjustments;
* Details of trade union membership where subscriptions are deducted from your salary;
* Information in applications you make for other positions within the council;
* Information about your use of the council’s IT, communication and other systems and other monitoring information;
* Details of your use of the council’s social media accounts;
* Your use of public social media, only in very limited circumstances (for example if you work in a politically restricted post) to check specific risks for specific functions within the council. You will be notified separately if this is to occur;
* Details in references about you that we give to others;
* Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief; gender re-assignment, marital status, caring commitments status.

Much of your personal data is provided by you and is collected through information you provide including:

* At the start of your working relationship e.g. Your application form or cv; identity documents such as your passport or your driving licence;
* During your work with the council e.g. When applying for employee benefits, maternity, adoption, or paternity leave, submitting fit notes, pension beneficiary nomination forms and online equalities disclosure;
* From correspondence with you; or through interviews, meetings or other assessments.

In some cases, the council (with your consent) will collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers, and information from criminal records checks permitted by law.

Data is stored in a range of different places, including in your personnel file (on SharePoint) and in the council's HR management system (My Resources) and in other IT systems (including the council's email system).

Certain of the categories above may not apply to you if you are a worker, agency worker, consultant, volunteer, apprentice or intern.

1. **Why does the council process personal data?**

The council needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with written details about your employment, to pay you correctly and to administer your terms and conditions of employment, any benefits, and pension and/or insurance entitlements.

In some cases, the council needs to process data to ensure that it is complying with its legal obligations, including with employment law, immigration law, health and safety law, tax laws and other laws which affect the council. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety requirements and to enable employees to take periods of leave to which they are entitled. For certain positions, it is necessary to carry out criminal record and/or professional registration checks to ensure that individuals are suitable to undertake the role in question.

In other cases, the council has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the council to:

* Run recruitment and promotion processes;
* Maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
* Monitor compliance by you, us and others with our policies and contractual obligations;
* Operate and keep a record of conduct and disciplinary and grievance processes raised by or involving you, to ensure acceptable conduct within the workplace;
* Operate and keep a record of employee appraisals and performance related processes, to plan for career development, and for succession planning and workforce management purposes;
* Operate and keep a record of absence and absence management procedures, to allow effective workforce management;
* Obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law,;
* Operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the council complies with duties in relation to leave entitlement;
* Operate our collective consultation and employee relations procedures which may involve your name and job title being shared with representatives of the trade unions recognised by the Council.
* Ensure that employees are receiving the pay, pension and/or other benefits to which they are entitled;
* Answer questions from insurers about any insurance policies which apply to you;
* Ensure effective general HR and business administration;
* Provide references on request for current or former employees;
* Prevent and detect fraud or other criminal offences;
* Respond to and defend the council in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure; and
* Monitor diversity and equal opportunities and maintain and promote equality in the workplace
* And any other reason which we may notify you of from time to time

Where the council relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

1. **How does the council process special categories of personal data?**

We will only process special categories of your personal data in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we ask for your consent to process a special category of personal data then we will explain the reasons for our request. You do not need to consent and can withdraw your consent later if you choose.

Criminal record checks and/or disclosure/barring information may be required for specific job roles. These checks will only be carried out with your consent.

We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

* Where it is necessary for carrying out rights and obligations under employment law;
* Where it is necessary to protect your vital interests or those of another person when you/they are physically or legally incapable of giving consent;
* Where you have made the data public;
* Where processing is necessary for the establishment, exercise or defence of legal claims; and
* Where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

Some special categories of personal data, such as information about health or medical conditions, is therefore processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes).

Information about trade union membership is processed when you authorise the council to deduct trade union subscriptions from your salary and to comply with our legal obligations in respect of trade union members.

Health and medical conditions information is processed to manage sickness absence and comply with any statutory pay and benefit requirements as well as helping the council manage its workforce. Employees can refuse to supply information about their health conditions which may mean decisions will be taken solely on available information.

Where the council processes other special categories of personal data and equalities data, such as information about ethnic origin, sexual orientation, religion or belief, gender re-assignment, marital status or caring commitments status, this is done for the purposes of equal opportunities monitoring within the context of the statutory public sector equality duty.

Data that the council uses for equality purposes is anonymised for any publication purposes and is collected with the express consent of employees, which can be withdrawn at any time. Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so. This data is kept in a secure online location with limited access only by specific HR individuals. Equality data cannot be seen by line management or other employees.

1. **Who has access to data?**

With the exception of equality information, your information will be shared on a need to know basis internally, including with members of the HR and recruitment team (including payroll), your line manager, managers in the business area in which you work, to carry out the council’s obligations under its contract with you, comply with legal obligations or for the council’s legitimate interests.

The council shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service. The council may also share your data with third parties in the context of a sale or transfer of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The council also shares your data with third parties that process data on its behalf, for example: the provision of workplace benefits (**Sodexo**); the provision of occupational health services (**Medigold**); the Employees Assistance Service (**Workplace Options**); job applications through the recruitment management system (**Lumesse**); out-placement support (**Hays);** employee benefits such as gym membership and travel season tickets (**Gymflex** and **Commuter Club;** disclosure and barring checks (**Atlantic Data**); andemployee administration through the human resources management system (**Evosys and Oracle**); pensions administration, processing and valuation (**Altair, Aquila Haywoods, Hymans, National Pensions Database and other pension funds).**

We require those third parties to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

The Council will not usually transfer your data to countries outside the European Economic Area, however we may provide visual access only (so a contractor may be able to view your data, but would be unable to process it in any other way) for system support purposes (and only where this is necessary and/or unavoidable), and when doing so we will ensure that that your data is appropriately protected and secured as required by GDPR.

1. **How does the council protect data?**

The council takes the security of your data seriously. The council has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Information management policies are applicable to HR- related data and confirm the controls around data handling in the council. The relevant ICT and security and information management policies including users’ responsibilities can be found here:

* [ICT and security and information management policies](https://intranet.croydon.gov.uk/lbc-policy-manager/acceptableuse.html)

Where the council engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

1. **For how long does the council keep data?**

The council will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment are set out via relevant retention periods in the ***HR Records Retention Policy.***

1. **Your rights**

As a data subject, you have a number of rights. You have the right to:

* Information about what personal data we process, how and on what basis (as set out in this policy);
* Access and obtain a copy of your data on request;
* Require the council to change incorrect or incomplete data;
* Require the council to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing for which it was collected;
* Require the council to delete or stop processing your data if processing is unlawful;
* Object to the processing of your data where the council is relying on its legitimate interests as the legal ground for processing; and
* Ask the council to restrict the use of data for a period if data is inaccurate or there is a dispute about whether or not your interests override the council’s legitimate grounds for processing data.
* Object if the council processes your personal data for the purposes of direct marketing;
* Transfer your personal data to another controller (excluding paper files);
* With some exceptions, not to be subjected to automatic decision making;
* Be notified of a data security breach concerning your personal data where there is a high risk to your the rights and freedoms;

In most situations, we will not rely on your consent as a lawful ground to process your data. If we do however, request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later.

If you would like to exercise any of these rights, please contact HR Consultancy via e-mail: [humanresources@croydon.gov.uk](mailto:humanresources@croydon.gov.uk)

You can make a subject access request by contacting the council via e-mail:[SAR@croydon.gov.uk](mailto:SAR@croydon.gov.uk)

If you believe that the council has not complied with your data protection rights, you can complain to the Information Commissioner. You can do this by contacting the Information Commissioner’s Office directly. Full contact details including a helpline number can be found on the Information Commissioner’s Office website [www.ico.org.uk](http://www.ico.org.uk).This website has further information about your rights and obligations.

1. **What if you do not provide personal data?**

You have some obligations under your employment contract to provide the council with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith.

You may also have to provide the council with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights. For example, by refusing to provide a fit note if you are absent for over seven days, may result in the council withholding sick pay for your absence from day eight onwards.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the council to enter a contract of employment with you. If you do not provide other information, this will hinder the council's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

1. **Automated decision-making**

Employment decisions are not based solely on automated decision-making.

1. **Further Information**

Further information can be obtained in our corporate wide Privacy Notice at <https://www.croydon.gov.uk/privacy>

End