

What is the purpose of this document?

Nottingham City Council is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation ("GDPR").

It applies to all employees, workers and consultants.

Nottingham City Council is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and consultants. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.

It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are certain types of more sensitive personal data which require a higher level of protection, such as information about a person's health or sexual orientation. Information about criminal convictions also warrants this higher level of protection.

We will collect, store, and use the following categories of personal information about you:-

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits (including salary sacrifice) information.
- Start date and, if different, the date of your continuous employment.
- Leaving date and your reason for leaving.
- Location of employment or workplace.
- Copy of driving licence.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).
- Compensation history.
- Performance information.
- Disciplinary and grievance information.
- CCTV footage and other information obtained through electronic means such as swipe card records and e-mails/ WhatsApp messages.

- Information about your use of our information and communications systems.
- Photographs.
- Results of Her Majesty's Revenue & Customs ("HMRC") employment status check, details of your interest in and connection with any intermediary through which your services are supplied.

We may also collect, store and use the following more sensitive types of personal information, known as special category personal data under the GDPR: -

- Information about your race or ethnicity, religious beliefs, sexual orientation, disability and political opinions (information about political opinions will only be collected, stored and used when: information comes to light that a post-holder of a politically-restricted post may be in breach of the requirements of the Local Government & Housing Act 1989 and subordinate legislation regarding political restriction of officers and staff; where an individual's political opinions conflict with our equality and diversity policies and/or our Code of Conduct for Employees; or where an individual's political opinions are, or may be, proscribed by law).
- Trade union membership.
- Information about your health, including any medical condition, health and sickness records, including: -
 - where you leave employment and the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision;
 - details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; and
 - where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions purposes.
- Genetic information and biometric data.
- Information about criminal convictions and offences.

How is your personal information collected?

We collect personal information about employees, workers and consultants through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies. We also obtain data from Occupational health and other providers such as opticians, pension administrators and other government departments for example HMRC, Trade Unions, Car parking scheme, providers of staff benefits such as Works perks. We may also collect information from categories of data subjects for example whistle blowers.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.
2. Where we need to comply with a legal obligation.
3. Where processing is necessary for the purposes of the legitimate interests

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).
2. Where it is needed in the public interest or for official purposes.

Situations in which we will use your personal information

We need all the categories of information in the list above primarily to allow us to perform our contract with you *, to enable us to comply with legal obligations ** and where we need to protect your interests (or someone else's interests) ***. The situations in which we will process your personal information are listed below. We have indicated by asterisks the purpose or purposes for which we are processing or will process your personal information.

- Making a decision about your recruitment or appointment. *
- Determining the terms on which you work for us. *
- Checking you are legally entitled to work in the United Kingdom. **
- Maintaining 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, worker and consultant contractual and statutory rights. * **
- Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions ("NICs"). * **
- Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties. * **
- Liaising with the trustees or managers of your pension provider and any other provider of employee benefits, such as Works Perks. * **
- Administering the contract we have entered into with you. *
- Monitoring your use of our information and communication systems to ensure compliance with our IT policies. * **
- Conducting performance reviews, managing performance and determining performance requirements. *
- Education, training and development requirements. *

- Making decisions about salary reviews and compensation. *
- Assessing qualifications for a particular job or task, including decision about promotions. *
- Managing any sickness absence. * ***
- Ascertaining your fitness to work. * ***
- Making decisions about your continued employment or engagement. *
- Making arrangements for the termination of our working relationship. *
- Providing references on request for you. ***
- Business management and planning, including accounting and auditing. * **
- To gather evidence in internal grievance or disciplinary processes. * ***
- To deal with legal disputes involving you, or other employees, workers and consultants, including accidents at work. * **
- To comply with health and safety obligations. ** ***
- To prevent fraud. **
- To operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace. * ***
- To operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled. * ***
- To obtain occupational health advice, to ensure that we comply with duties in relation to individuals with disabilities, meet our obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled. * ** ***
- To 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 we comply with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled. * ** ***
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution. **
- To conduct data analytics studies to review and better understand employee retention and attrition rates. *
- To maintain and promote equality and diversity in the workplace. ** ***

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

Monitoring of staff

All of NCC ICT systems, CCTV systems and swipe access system for the entry and exit of our premises are auditable and can be monitored although we don't do so routinely.

The Council are committed to respecting individual user's reasonable expectations of privacy concerning the use of its ICT systems and equipment. However, the Council reserves the right to log and monitor such use in line with the IT acceptable use policy, CCTV policy and Telematics policy.

Covert monitoring of staff can take place without the employee's knowledge or consent where it is necessary for the prevention and detection of criminal activity or other serious equivalent malpractice breaches of the disciplinary policy. This will take place only where it is necessary and proportionate to do so. Where covert monitoring is to take place because criminal activity is suspected and a criminal investigation is being considered then the RIPA policy must also be followed.

Monitoring can also take place without the consent of the employee for business continuity reasons where the employee cannot reasonably give consent or it is not appropriate to do so (for example where the employee is ill or has left the organisation).

Monitoring can take place for health and safety reasons in line with NCC policies and guidance.

If you fail to provide personal information

Certain information, such as contact details, your right to work in the United Kingdom and payment details, have to be provided to enable us to enter into a contract of employment or contract for services with you and maintain that contract. If you do not provide other information, this will hinder our ability to administer the rights and obligations arising as a result of the working relationship efficiently. In addition, we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

You have some obligations under your contract with us to provide us 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 us 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.

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations or exercise rights in connection with employment.
3. Where it is needed in the public interest, such as for equal and diversity monitoring or in relation to public sector occupational pension schemes.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay and pensions.
- If you apply for an ill-health pension under a public sector pension scheme, we will use information about your physical or mental health in reaching a decision about your entitlement.
- We will use information about your race or national or ethnic origin, religious or philosophical beliefs, or your sexual orientation, to ensure meaningful equality and diversity monitoring and reporting.
- We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in

the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences in the following ways:-

- Where we are legally required by a professional regulatory body to carry out criminal records checks for those carrying out a role you are being considered for or work in;
- Your role is one which is listed in the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (SI 1975/1023) (as amended) and is also specified in the Police Act 1997 (Criminal Records) Regulations 2002 (SI 2002/233) (as amended) so is eligible for a standard or enhanced check from the Disclosure and Barring Service (“DBS”);
- Your role requires a high degree of trust and integrity since it involves dealing with vulnerable citizens or high value funds and so we would like to ask you to seek a basic disclosure of your criminal records history;
- Where a criminal conviction or offence may also be evidence of a breach of Nottingham City Council’s equality and diversity policies, the Code of Conduct for Employees and/or your contract of employment or contract for services with us.

We are allowed to use your personal information in this way to carry out our obligations to vulnerable citizens and, in some instances, our duty of care to other colleagues. We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you 21 days to request a reconsideration.
2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

Some of our decisions are based solely on automated decision-making. This relates solely to eligibility to receive salary sacrifice scheme entry, ensuring that you are entitled to apply and that there will be no adverse implication, namely taking your monthly salary below the National Minimum Wage.

Data sharing

We may have to share your data with third parties, including third-party service providers.

We require third parties to respect the security of your data and to treat it in accordance with the law.

As part of work being done by us to replace our Human Resources, Finance and Payroll systems, we will transfer some personal information we collect about you to India, which is outside the European Economic Area ("EEA"), in order to perform our contract with you. There is not an adequacy decision by the European Commission in respect of India. This means that the country to which we transfer your data is not deemed to provide an adequate level of protection for your personal information. However, to ensure that your personal information does receive an adequate level of protection we have put in place the following appropriate measures to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects European Union and United Kingdom laws on data protection: we will put in place the standard data protection clauses adopted by the European Commission in our contract with our provider that will, in effect, secure compliance with the GDPR.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law or where it is necessary to administer the working relationship with you.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents). The following activities are carried out by third-party service providers: payroll; pension administration; benefits provision and administration.

Where we engage third parties to process personal data on our 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. Nottingham City Council and Leicestershire County Council have an Information Sharing Agreement in relation to East Midlands Shared Services (“EMSS”) processing data.

We will share personal data regarding your participation in any public sector pension scheme with the relevant pension scheme administrator (e.g. Nottinghamshire County Council for the Local Government Pension Scheme or Teachers’ Pensions for the Teachers’ Pension Scheme).

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible outsourcing of a service area. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share your personal data with the other parties if and to the extent required under the terms of the transaction.

We may also need to share your personal information with a regulator or to otherwise comply with the law. This may include making returns to HMRC, disclosures to the DBS and/or to professional regulators such as the Teaching Regulation Agency.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available on the intranet.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

Once you are no longer an employee, worker or consultant of Nottingham City Council we will retain and securely destroy your personal information in accordance with the applicable period for which data is held after the end of a working relationship with us. These periods are set out in the Information Asset Register, which is available to view on the Nottingham City Council intranet (<http://ims.nottinghamcity.gov.uk/iar/InformationAssets/Directorate/18>)

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:-

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Contact

If you would like to exercise any of the rights of access, correction, erasure and restriction, or to withdraw your consent for specific processing, please contact the Information Compliance Team, (email: Data.Protection@nottinghamcity.gov.uk; tel: 0115 87 63855). You can also make a subject access request by completing our form for making a subject access request, which is available on Nottingham City Council's intranet.

Data protection officer

If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO at the above address.

Information Commissioner's Office

You have the right to make a complaint at any time to the Information Commissioner's Office ("ICO"), the United Kingdom supervisory authority for data protection issues.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact the DPO, Nottingham City