



Cumbria County Council

Corporate Privacy Notice

Contents

INTRODUCTION.....	3
WHAT INFORMATION DOES THE COUNCIL COLLECT ABOUT ME?	3
WHY DOES THE COUNCIL COLLECT INFORMATION ABOUT ME?	3
WHO DOES THE COUNCIL COLLECT INFORMATION ABOUT?	4
WHO DOES THE COUNCIL SHARE INFORMATION WITH?.....	4
LAWFUL BASIS FOR PROCESSING DATA.....	5
PROTECTING YOUR INFORMATION.....	6
HOW CAN YOU REQUEST CORRECTION OF INACCURATE INFORMATION?	6
DATA TRANSFERS	6
BLUE BADGE APPLICATIONS.....	6
CCTV/SURVEILLANCE	7
CHILDREN AND FAMILIES SERVICES	7
EMPLOYMENT	8
DETECTION AND PREVENTION OF CRIME	8
HOUSEHOLD WASTE PERMIT SCHEME.....	9
HIGHWAYS SERVICE	9
PARKING	9
PUBLIC HEALTH	10
CONTACTING THE COUNCIL.....	12
YOUR RIGHTS	12
DATA PROTECTION OFFICER.....	13

Introduction

Cumbria County Council is a 'data controller' under the General Data Protection Regulation and is committed to protecting your privacy when you use its services. This notice explains what the council will collect, who it will be shared with, why we need it and how we will use it. The council will continually review and update this privacy notice to reflect service changes, feedback from customers and changes in the law.

What information does the council collect about me?

The council will collect information from you in a variety of formats:

- on a paper or online form
- by telephone
- by email
- recorded by CCTV cameras, or
- in person by a member of our staff or one of our partners

In the course of daily business the council collects the following information about you (dependent on the nature of the service(s) you are applying for or receiving):

- personal details
- family details
- lifestyle and social circumstances
- goods and services
- financial details
- employment and education details
- housing needs
- visual images, personal appearance and behaviour
- licenses or permits held
- student and pupil records
- business activities
- case file information

We also process sensitive classes of information that may include:

- physical or mental health details
- racial or ethnic origin
- trade union membership
- political affiliation
- political opinions
- offences (including alleged offences)
- religious or other beliefs of a similar nature
- criminal proceedings, outcomes and sentences
- sexual life

Why does the council collect information about me?

The council collects the information listed above to enable it to:

- support internal financial and corporate functions by maintaining accounts and records
- support and manage employees

- promote services and market local tourism
- conduct public/health awareness campaigns
- manage property
- provide leisure and cultural services
- provide education services
- carry out surveys and consultations
- administer the assessment and collection of taxes and other revenue i.e. benefits, grants
- carry out licensing and regulatory activities
- provide social services to adults and children
- assist with crime prevention and prosecution of offenders i.e. CCTV
- undertake research
- provide all commercial services i.e. administration and enforcement of parking regulations and restrictions
- provide non-commercial activities i.e. refuse collections from residential properties
- manage archived records for historical research
- match data under local and national fraud initiatives
- support public health services

Who does the council collect information about?

To provide services the council may need to collect information from or about the following:

- businesses, customers and suppliers
- staff, persons contracted to provide a service
- claimants
- complainants, enquirers or their representatives
- professional advisers and consultants
- students and pupils
- carers or representatives
- landlords
- recipients of benefits
- witnesses
- offenders and suspected offenders
- licence and permit holders
- traders and others subject to inspection
- people captured by CCTV images
- representatives of other organisations
- patients
- healthcare users

Who does the council share information with?

The council may share information with:

- business associates and other professional advisers
- courts, prisons and tribunals
- credit reference agencies
- current, past and prospective employers
- customers
- customs and excise
- data processors
- debt collection and tracing agencies

- educators and examining bodies
- employees and agents of the data controller
- family, associates or representatives of the person whose personal data we are processing
- financial organisations
- fire authorities
- healthcare, social and welfare organisations and professionals
- housing associations and landlords
- international law enforcement agencies and bodies
- law enforcement and prosecuting authorities
- legal representatives
- licensing authorities
- local and central government departments
- Local Government Ombudsman/Information Commissioner
- partner agencies, approved organisations and individuals working with the police,
- persons making an enquiry or complaint
- police complaints authority
- police forces
- political organisations
- press and the media
- private investigators
- professional advisers and consultants
- professional bodies
- providers of goods and services
- regulatory bodies
- religious organisations
- security companies
- service providers
- students and pupils including their relatives, guardians, carers or representatives
- survey and research organisations
- the disclosure and barring service
- trade unions
- voluntary and charitable organisations

Where information sharing is necessary we are required to comply with all aspects of the General Data Protection Regulation and the Data Protection Act 1998.

Lawful basis for processing data

There are a number of legal reasons why we need to collect and use your personal information.

Generally we collect and use personal information where:

- you, or your legal representative, have given consent
- you have entered in to a contract with us
- it is necessary to perform our statutory duties
- it is necessary to protect someone in an emergency
- it is required by law
- it is necessary for employment purposes
- it is necessary to deliver health or social care services
- you have made your information publicly available

- it is necessary for legal cases
- it is to the benefit of society as a whole
- it is necessary to protect public health
- it is necessary for archiving, research, or statistical purposes

If we have consent to use your personal information, you have the right to remove it at any time.

If you want to remove your consent, please [contact us](#) and tell us which service you're using so we can deal with your request.

Protecting your Information

We will take appropriate steps to make sure we hold records about you (on paper and electronically) in a secure way, and we will only make them available to those who have a right to see them. Our security includes: encryption, access controls on systems and security training for all staff. [View our Information Security policy](#).

If you access information online, the council website does not store or capture personal information, but merely logs a number called your IP address which is automatically recognised by the system. The system will record personal information if you:

- subscribe to or apply for services that require personal information
- report a fault and give your contact details for us to respond
- contact us and leave your details for us to respond

For further information visit our [Cookies](#) webpage.

How can you request correction of inaccurate information?

You should let us know if you disagree with some information we hold about you.

You may not always be able to change or remove the information; however, we will correct factual inaccuracies and may include your comments in the records. Please [contact us](#) to inform us of any inaccuracies.

Data Transfers

It may sometimes be necessary to transfer personal information overseas. When this is required information may need to be transferred to countries or territories outside of the European Economic Area (EEA). The council will ensure that all relevant safeguards are in place before this takes place and that all aspects of the Data Protection Act 1998 are complied with.

Blue Badge Applications

When you apply for a Blue Badge we will collect the following information from you:

- Name
- Postal address
- Date of birth
- Place of birth
- National Insurance number
- Driving licence number

- Proof of your address
- Proof of your identity
- A photograph
- Vehicle registration number(s)
- Evidence of eligibility relating to health conditions and/or disabilities
- Evidence of benefits received
- If you already have a Blue Badge, the number, expiry date and the name of the issuing local authority will be requested.

The purpose for collecting this information is to determine whether the applicant is eligible for a Blue Badge. We will share this information with third parties where necessary (including other internal service areas).

CCTV/Surveillance

We have installed CCTV systems in some of our premises used by members of the public, for the purposes of public and staff safety and the prevention and detection of crime. CCTV is also installed on the outside of some of our buildings for the purposes of monitoring building security and crime prevention and detection.

Images captured by CCTV will not be kept for longer than necessary. However, on occasions there may be a need to keep images for longer, for example where a crime is being investigated.

Civil Enforcement Officers (CEOs) who undertake the enforcement of parking restrictions, are each equipped with a Body Worn Video Device (BWVD) which has both video and audio recording capability.

During their work the CEOs are vulnerable to verbal and physical abuse. The BWVDs can act as a deterrent to abusive and aggressive behaviour and prevent a situation escalating and the recording can also be used as evidence in cases where a CEO has been assaulted or abused. It can also be used to investigate complaints about a CEO.

The council's [Body Worn Video Device and Hand Held Unit Policy \(PDF 289kb\)](#) details the operational procedures for using the devices, data storage and requests for access to footage.

Individuals can request a copy of the footage under the Data Protection Act using the [council's online form](#).

We will only disclose images and audio to other authorised bodies who intend to use it for the purposes stated above. Images and audio will not be released to the media for entertainment purposes or placed on the internet for public viewing. We operate CCTV and disclose in accordance with the codes of practice issued by the Information Commissioner and the Home Office.

Children and Families Services

Please refer to our Children and Families Services Privacy Notices:

- **Privacy Notice - Childrens Centres (752KB)**
- **Privacy Notice - Cumbria Information, Advice and Guidance (752KB)**

- **Privacy Notice - Children In Need, Children Looked After, Child Protection, Care Leavers (752KB)**
- **Privacy Notice - Citizens Portal (751KB)**
- **Privacy Notice - Focus Family (752KB)**
- **Privacy Notice - Multi Agency Safeguarding Hub (751KB)**
- **Privacy Notice - National Pupil Database (752KB)**
- **Privacy Notice - Pupils (751KB)**
- **Privacy Notice - Schools and Early Years (751KB)**
- **Privacy Notice - Short Breaks Autism Support (751KB)**
- **Privacy Notice - Strengthening Families (751KB)**
- **Privacy Notice - Targeted Youth Support (751KB)**
- **Privacy Notice - Youth Support Schools (546KB)**

Employment

Please refer to our employment privacy notices:

- **Privacy Notice - Employees, Candidates, Workers, Contractors and Volunteers (498KB)**
- **Privacy Notice – Schedules (24KB)**

Detection and Prevention of Crime

National Fraud Initiative

We participate in the [Cabinet Office's National Fraud Initiative](#): a data matching exercise to assist in the prevention and detection of fraud. We are required to provide particular sets of data to the Minister for the Cabinet Office for matching for each exercise.

The use of data by the Cabinet Office in a data matching exercise is carried out with statutory authority under Part 6 of the Local Audit and Accountability Act 2014. It does not require the consent of the individuals concerned under the Data Protection Act 1998.

Data matching by the Cabinet Office is subject to a [Code of Practice](#).

View further information on the [Cabinet Office's legal powers and the reasons why it matches particular information](#). For further information on data matching at this authority contact nfi@cumbria.gov.uk

Data Matching

This authority is required by law to protect the public funds it administers. It may share information provided to it with other bodies responsible for auditing, administering public funds or where undertaking a public function, in order to prevent and detect fraud.

The Cabinet Office is responsible for carrying out data matching exercises.

Data matching involves comparing computer records held by one body against other computer records held by the same or another body to see how far they match. This is usually personal information. Computerised data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it may indicate that there is an inconsistency which requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.

Household Waste Permit Scheme

When you apply for a Household Waste Recycling Permit we will collect the following information from you:

- Name
- Email address
- Telephone
- Address
- Permit requirements
- Vehicle details
- Waste information

The purpose for collecting this information is to allow the council to process your permit application. We will share this information with other third parties where necessary (including other internal service areas).

Highways Service

When you report a highways fault we will collect the following information from you:

- Name
- Email address
- Details of the fault

The purpose for collecting this information is to keep you informed about progress with reported highways defects i.e. potholes. No automated decisions are made using the personal data you supply to us for the above purposes.

We will share this information with other third parties where necessary (including other internal service areas).

Parking

Penalty Charge Notices

When we issue a penalty charge notice we collect the following information:

- Vehicle Registration Mark
- Vehicle make
- Vehicle location
- Photographs of vehicle and location

When you pay or challenge a penalty charge notice we will collect the following information:

- Penalty Charge Notice number
- Vehicle registration mark
- Name
- Postal address
- Contact details
- Payment details

The purpose for collecting this information is to allow the council to process payments or challenges. We will share this information with other third parties where necessary (including other internal service areas).

Apply for a parking permit

When you apply for a parking permit we collect the following information from you:

- Vehicle registration
- Name
- Postal address
- Contact details
- Proof of your address
- Proof of your identity
- Proof of vehicle ownership
- Specific supporting evidence for business and carer permits

The purpose for collecting this information is to allow the council to issue parking permits and operate the permit scheme in Cumbria. We will share this information with other third parties where necessary (including other internal service areas).

Public Health

Aggregated, anonymised or pseudonymised health data (including births and deaths data, and Hospital Episode Statistics) is used by Cumbria County

Council's Performance and Risk team in supporting the effective and efficient discharge of its statutory duty and wider responsibilities to improve and protect the health and wellbeing of the populations it serves, and reduce health inequalities. For more information of the role and duties of the Public Health function see: www.cumbria.gov.uk/publichealth

Purposes and Data Held

The Performance and Risk team will access health related information to analyse the health needs and outcomes of the local population and for monitoring trends and patterns of diseases and the associated risk factors.

All information accessed, processed and stored by the Performance and Risk team will be used to measure the health, mortality or care needs of the population; for planning, evaluating and monitoring health; protecting and improving public health. It is used to carry out and support:

- health needs assessments
- health equity analysis
- commissioning and delivery of services to promote health and prevent ill health
- public health surveillance
- identifying inequalities in the way people access services
- joint strategic needs assessment
- health protection and other partnership activities

To deliver public health, local authorities need to use available health data sources to get relevant health and social care information. This data can contain person identifiable data which may identify patients such as name, address, age, sex, ethnicity, disease, use of hospital services, and/or NHS Number.

The Performance and Risk team will have access to the following data:

- **Primary Care Mortality Database (PCMD)** - The PCMD holds mortality data as provided at the time of registration of the death along with additional GP details, geographical indexing and coroner details where applicable.
- **Births and Vital Statistics datasets** - Births files include date of birth, sex, birth weight, address, postcode, place of birth, stillbirth indicators and age of mother. Deaths data includes: deaths broken down by age, sex, area and cause of death sourced from the deaths register.
- **Hospital Episode Data (HES)** - is a data warehouse containing details of all admissions, outpatient appointments and A&E attendances at NHS hospitals in England. This data is collected during a patient's time at hospital and is submitted to allow hospitals to be paid for the care they deliver. HES data is designed to enable secondary use, that is use for non-clinical purposes, of this administrative data.

We are committed to using pseudonymised or anonymised information as much as is practical, and in many cases this will be the default position. Pseudonymisation is a procedure by which the most identifiable fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. There can be a single pseudonym for a collection of replaced fields or a pseudonym per replaced field. The purpose is to render the data record less identifiable and therefore lower customer or patient objections to its use.

Anonymisation is the process of removing identifying particulars or details from (something, especially medical test results) for statistical or other purposes.

Legal Basis

Any information held by the council about individuals will be held securely and in compliance with the Data Protection Act 1998. Information will not be held for longer than required and will be disposed of securely. The legal basis for the flow of data for the above purposes is set out in Section 42(4) of the Statistics and Registration Service Act (2007) as amended by section 287 of the Health and Social Care Act (2012) and Regulation 3 of the Health Service (Control of Patient Information) Regulations 2002. The council has a Data Access Agreement with NHS Digital and data is supplied in accordance with section 42(4) of the Statistics and Registration Service Act 2007 as amended by section 287 of the Health and Social Care Act 2012, and Regulation 3 of the Health Service (Control of Patient Information) Regulations 2002.

Your Rights

You have the right to opt-out of the Performance and Risk team receiving or holding your personal identifiable information. There are occasions where service providers will have a legal duty to share information, for example for safeguarding or criminal issues. The process for opting out will depend on the specific data and what programme it relates to. If you have any questions about our use of these data, wish to request a copy of the information we hold about you, or if you wish to discuss your rights in relation to opting-out from these processes, please contact the Performance and Risk team at pandi@cumbria.gov.uk

Contacting the Council

Emails

If you email us we may keep a record of your contact and your email address and the email for our record keeping of the transaction.

We suggest that you keep the amount of confidential information you send to us via email to a minimum and use our secure online forms and services.

You can sign up for email alerts for selected services using an external service from GovDelivery, with control over your preferences.

Telephone Calls

The council will inform you if your telephone calls are being recorded or monitored and will not record any financial card details if you make payments by telephone.

Your Rights

Access

Subject to certain conditions, you are entitled to have access to your personal data (this is more commonly known as submitting a "data subject access request"). If possible, you should specify the type of information you would like to see to ensure that our disclosure is meeting your expectations. We must be able to verify your identity. Your request may not impact the rights and freedoms of other people, eg privacy and confidentiality rights of other staff. Where you, the data subject, make a request by electronic form means, the information will be provided by electronic means where possible, unless otherwise requested.

Data Portability

Subject to certain conditions, you are entitled to receive the personal data which you have provided to us and which is processed by us by automated means, in a structured, commonly-used machine readable format. If you exercise this right, you should specify the type of information you would like to receive (and where we should send it) where possible to ensure that our disclosure is meeting your expectations. This right only applies if the processing is based on your consent or on our contract with you and when the processing is carried out by automated means (ie not for paper records). It covers only the personal data that has been provided to us by you.

Inaccurate or Incomplete Data

You may challenge the accuracy or completeness of your personal data and have it corrected or completed, as applicable. You have a responsibility to help us to keep your personal information accurate and up to date. We encourage you to notify us of any changes regarding your personal data as soon as they occur, including changes to your contact details, telephone number, immigration status. Please always check first whether there are any available self-help tools to correct the personal data we process about you. This right only applies to your own personal data. When exercising this right, please be as specific as possible.

Object to/Restrict Processing

Subject to certain conditions, you have the right to object to or ask us to restrict the processing of your personal data. As stated above, this right applies where our processing of your personal data is necessary for our legitimate interests. You can also object to our processing of your personal data for direct marketing purposes.

Erasure

Subject to certain conditions, you are entitled to have your personal data erased (also known as the "right to be forgotten"), eg where your personal data is no longer needed for the purposes it was collected for, or where the relevant processing is unlawful. We may not be in a position to erase your personal data, if for example, we need it to (i) comply with a legal obligation, or (ii) exercise or defend legal claims.

Withdrawal of Consent

As stated above, where our processing of your personal data is based on your consent you have the right to withdraw your consent at any time. If you withdraw your consent, this will only take effect for future processing.

You also have the right to complain with the Information Commissioner's Office (ICO), which is the UK data protection regulator. More information can be found on the Information Commissioner's website: www.ico.org.uk/concerns

Data Protection Officer

We have appointed a Data Protection Officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information. You can contact the DPO in the following ways:

Email: dataprotection@cumbria.gov.uk

Post:
Data Protection Officer,
c/o Information Governance Team,
Cumbria County Council,
Cumbria House,
117 Botchergate,
Carlisle
CA1 1RD

Last Updated: May 2018