



Privacy Notice Blue Badges

When processing personal data, the council is required under Articles 13 and 14 of the UK General Data Protection Regulation (UKGDPR) to provide individuals with the information contained in this document.

Data Ownership

Name	Cumbria County Council
Address	Cumbria House, 117 Botchergate, Carlisle, Cumbria CA1 1RD
Registration Number	Z5623112

This information is also available via the Information Commissioner's Register of Fee Payers at: <https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/>

Data Protection Officer

The council's Data Protection Officer is Claire Owen and can be contacted by:

Email: dataprotection@cumbria.gov.uk
Post: Cumbria County Council, Legal and Democratic Services, 1st Floor, Cumbria House, 117 Botchergate, Carlisle, Cumbria CA1 1RD
Online: [Contact Form](#)

Purpose

We are Cumbria County Council's Blue Badge Team, and we are responsible for providing the following services:

- Administration of the Disabled Persons Blue Badge scheme on behalf of the Department for Transport

Data Collection

Your data will be collected in the following ways:

- Through the completion of an application form either online, by post or by email
- Supporting evidence may be collected either online, by post, by email, by telephone or by accessing our Health and Care Records
- A face-to-face Mobility Assessment may be necessary if applying under the "Walking Disabilities criteria

Data Types

The Blue Badge Team is required to process either your personal, special category/sensitive or criminal/law enforcement data to meet legal obligations and make robust recommendations and decisions.

The **Personal Data** requirements are:

- Name (including surname at birth/or adoption)
- Address (including previous addresses in the last 3 years)
- Contact Details (including email address)
- Town of Birth
- Country of Birth
- Date of Birth
- Driving License Number
- Passport Number
- National Insurance Number
- Proof of Identity (e.g. birth/adoption certificate, marriage/civil partnership certificate, Driving License, Passport, Identity Cards)
- Proof of address from an official source (e.g. local authority correspondence, benefit award letters, utility bills etc)
- Payment details may be taken if you pay by card

The **Special Category Data** requirements are:

- Health and information including details of medical conditions affecting mobility, pain medication and assessment of walking ability.
- Evidence to support automatic eligibility for a Badge (e.g. blind registration, payment of Personal Independence Payment (PIP), Disability Living Allowance, War Pensions etc)
- Evidence to support those applicants applying under the hidden illness criteria (e.g. supporting evidence from a health care professional independent of the applicant e.g. OT, Physio, Psychologist, Psychiatrist)

The **Criminal/Law Enforcement Data** requirements are:

- **Not Applicable**

Legal Basis for Processing Data

Where the [Insert Service or Project Name] identifies the requirement to process personal, special category/sensitive or criminal/law enforcement data, depending on the specific data being shared, it must have at least one of the following:

- for personal data, a legal basis under **UKGDPR Article 6**,
- for special category/sensitive data, a condition under **UKGDPR Article 9**
- for criminal/law enforcement data, a purpose under **UKGDPR Schedule 8**

The following **legal bases** apply to the processing of your personal data:

- **UKGDPR Article 6(1) (a) Consent**
- **UKGDPR Article 6(1) (c) Legal Obligation**
- **UKGDPR Article 6(1) (e) Public Task/Public Interest/Official Authority**

Where the LGR Programme is relying on UKGDPR Article 6(1)(c) all [Relevant Legislation](#) should be listed below.

The following **conditions** apply to the processing of your special category/sensitive data:

- **UKGDPR Article 9(2) (a) Explicit consent**
- **UKGDPR Article 9(2) (b) Employment/social security and social protection**
- **UKGDPR Article 9(2) (i) Public health**

The following **purposes** apply to the processing of your criminal/law enforcement data:

- **Not Applicable**

Relevant Legislation

- Chronically Sick and Disabled Persons Act 1970
- Disabled Person (Badge for Motor Vehicles) (England) Regulations 2000
- Disabled Person (Badge for Motor Vehicles) (England) (Amendment) Regulations 2019

Automated Decision-Making/Profiling

Automated individual decision-making is a decision made by automated means without any human involvement. Automated individual decision-making does not have to involve profiling, although in some cases it might.

A definition of Profiling can be found in: [UK GDPR - Article 4\(4\)](#) and further information can be found at: [ICO - Automated Decision Making and Profiling](#)

We **do not** use your information for automated decision-making or profiling purposes.

Data Transfers

Your personal data **is not** transferred to a third country or international organisation.

Redaction

We operate a policy where we routinely redact the following details before making forms and documents available online:

- contact details e.g. telephone numbers, email addresses
- signatures
- personal or special category data
- information agreed to be confidential or commercially sensitive

Occasionally it may be considered necessary, justified and lawful to disclose data that appears in the list above. In these circumstances the council will make all reasonable efforts to contact you if this processing is going to have an impact on your rights or privacy.

Data Sharing

To achieve the [purpose](#) laid out above, the Blue badge Team will share [specific data](#) with:

- Northgate Public Services, Valtech UK Limited and Allied Publicity Services (Manchester) Limited as part of a contract for the production of the blue badge
- Various charities acting on your behalf including Age UK, Citizens Advice Bureau, Copeland Age and Advice Service, Barrow and District Disability Advice Association etc.
- The Council's parking enforcement team – this includes routine sharing of information on lost and stolen badges.
- Other local authority Blue Badge enforcement teams
- Police for parking enforcement
- Your name, address, date of birth, contact information and blue badge details will be shared with the Cabinet Office for data matching under the National Fraud Initiative

While responding to your enquiries or complaints it may be necessary to share your personal data with other parts of the council or other public bodies or organisations. All reasonable efforts will be made to contact you if this processing is going to have an impact on your rights or privacy.

National Fraud Initiative (NFI)/Data Matching

The Council participates 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 processing of data by the Cabinet Office in a data matching exercise is carried out with statutory authority under its powers in Part 6 of the Local Audit and Accountability Act 2014. It does not require the consent of the individuals concerned under the data protection legislation or the UK General Data Protection Regulation (UKGDPR).

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

The Council 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.

Data Security and Retention

The data, collected from or supplied by you, will be kept on a secure system and can only be accessed by authorised employees in the Blue Badge Team.

A range of encryption and security policies are in place to ensure the safety of your data. All debit and credit card payment transactions are encrypted to comply with relevant statutory and financial requirements.

Cumbria County Council will only store your information for as long as is legally required in accordance with the council's [Retention and Disposal Schedule \(EXCEL 267KB\)](#) or in situations where there is no legal retention period established best practice will be followed.

To help you understand the Schedule the council has published a [Retention Schedule - Quick User Guide \(PDF 787KB\)](#). If you have any questions about the Schedule or the Quick User Guide, please contact: recordcentre@cumbria.gov.uk.

If you experience any problems in relation to your personal data or you see something that doesn't look right, get in touch to report it as a [Data Breach](#).

Please note: Privacy Notices cannot be finalised and published without identifying the correct retention period.

Your Rights - Data Subject Access

The UKGDPR provides you with the right to access information the council, as a public authority holds about you. Upon receipt of a valid request the council will:

- provide you with a response within one month
- let you know if your request is subject to an extension
- make reasonable efforts to comply with the format of your request
- inform you if your request is going to be refused or a charge is payable.

You can make a Data Subject Access Request (DSAR) by contacting:

Email: information.governance@cumbria.gov.uk
Post: Cumbria County Council, Information Governance Team
Parkhouse, Baron Way, Carlisle CA6 4SJ
Telephone: (01228) 221234
Online: [Contact Form](#)

Your Rights - Other

In addition to your right of access the UKGDPR also gives you the following rights:

- the right to be informed via the council's Privacy Notice
- the right to withdraw your consent. If we are relying on your consent to process your data, then you can remove this at any point
- the right of rectification, we must correct inaccurate or incomplete data within one month
- the right to erasure. You have the right to have your personal data erased and to prevent processing unless we have a legal obligation to process your personal information
- the right to restrict processing. You have the right to suppress processing. We can retain just enough information about you to ensure that the restriction is respected in future
- the right to data portability. We can provide you with your personal data in a structured, commonly used, machine readable form when asked
- the right to object. You can object to your personal data being used for profiling, direct marketing or research purposes
- you have rights in relation to automated decision making and profiling, to reduce the risk that a potentially damaging decision is taken without human intervention.

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 do decide to withdraw your consent, we will stop processing your personal data for that purpose, unless there is another lawful basis we can rely on – in which case, we will let you know. Your withdrawal of your consent won't impact any of our processing up to that point.

Where our processing of your personal data is necessary for our legitimate interests, you can object to this processing at any time. If you do this, we will need to show either a compelling reason why our processing should continue, which overrides your

interests, rights and freedoms or that the processing is necessary for us to establish, exercise or defend a legal claim.

Unless otherwise stated above you can exercise any of these rights by contacting:

Email: dataprotection@cumbria.gov.uk
Post: Cumbria County Council, Legal and Democratic Services, 1st Floor,
Cumbria House, 117 Botchergate, Carlisle, Cumbria CA1 1RD
Online: [Contact Form](#)

Verifying Your Identity

When exercising the rights mentioned above, please be aware that under UKGDPR Article 12(6) additional information can be requested to verify that you are the data subject if your identity is unconfirmed. Please note that:

- additional documentation is only required when the council cannot verify your identity using internal council systems that relate to the service you are requesting information about
- the council will contact you for this documentation prior to processing your request
- the statutory deadline for responding to your request will start when you have provided the additional documentation
- failure to provide additional documentation may lead to the council rejecting your request.

Complaints

If you have any concerns about the information contained in this Privacy Notice, please contact: blue.badges@cumbria.gov.uk.

If you have concerns about the way the council has processed your data, please contact the council's Data Protection Officer via:

Email: dataprotection@cumbria.gov.uk
Post: Cumbria County Council, Legal and Democratic Services, 1st Floor,
Cumbria House, 117 Botchergate, Carlisle, Cumbria CA1 1RD
Online: [Contact Form](#)

If you are not satisfied with our response or believe we are not processing your personal data in accordance with the law you can complain to the Information Commissioner's Office (ICO): <https://ico.org.uk/make-a-complaint/your-personal-information-concerns/>

Reviews and Updates

In accordance with UK GDPR Article 13(3) where either, the extent of the data being collected or the purpose for collecting it changes this notice should be updated and republished, to ensure that data subjects are properly informed