



Data Protection Policy

Version: 1.0
Policy Date: 1 April 2023

Document Version Control

Organisation	Cumberland Council
Document Title	Data Protection Policy
Filename	Cumberland Council_Data Protection Policy
Document Status	Final
Author	LGR Legal and Democratic Services – Data Assurance Group
Document held by (name/section)	Legal and Democratic Services
Contact	dataprotection@cumberland.gov.uk
Date of publication	1 April 2023
Next review date	1 April 2024
Version Number	1.0
Approval date and by who (delegated/ committee)	Delegated – Chief Executive and Senior Information Risk Owner
For internal publication only or external also?	Both
Document stored on Council website or Intranet?	Intranet

Change History

Version	Date reviewed	Reviewed by	Description of revision
0.1	06/12/2022	LGR Legal and Democratic Services – Data Assurance Group	Draft policy based on existing CCC policy
0.2	08/02/2023	LGR Legal and Democratic Services – Data Assurance Group	Corporate branding applied
0.3	15/02/2023	LGR Legal and Democratic Services – Data Assurance Group	Changes required by Service Manager – Records Management Service
0.4	20/03/2023	Senior Information Governance and Data Protection	Updated Roles and Responsibilities

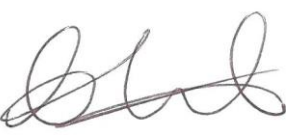

Document Approval

This document requires approval by the council's Senior Information Risk Owner (SIRO):

Version	Approval Date
1.0	14/04/2023

This Policy will be reviewed by the Data Protection Officer on an annual basis from the date of formal approval by the Authorised Signatory (below).

Authorised Signatory

Officer Name	Position	Version	Signature	Date
Andrew Seekings	Chief Executive	1.0		14/04/2023
Simon Higgins	Director – Resources Senior Information Risk Owner	1.0		14/04/2023

Contents

Introduction	4
Scope	4
Policy Statement	4
Roles and Responsibilities	5
Data Protection Officer (DPO)	8
Rights - Subject Access	8
Rights - Other	9
Timescales and Extensions	10
Consent	10
Refusing Requests	10
Verifying Your Identity	11
Data Breaches	11
Complaints	11

Introduction

Cumberland Council as a public authority, processes¹ large volumes of personal, sensitive personal or criminal/law enforcement data about employees, customers, clients, residents and visitors, and as a result is required to comply with data protection legislation including:

- [UK General Data Protection Regulation](#) ('**UKGDPR**')
• [Data Protection Act 2018](#) ('**DPA 2018**')
• [Human Rights Act 1998](#) ('**NRA 2008**')

Effective service delivery and compliance with legal obligations is dependent on the lawful collection, use and disposal of data that identifies people, this includes personal, sensitive personal or criminal/law enforcement data ('person identifiable data').

The purpose of this policy is to:

- provide an explanation of the council's obligations under data protection legislation
- help data subjects understand their rights and how to exercise them
- ensure adequate consideration is given to the disclosure of person identifiable data

The council aims to promote greater openness, provide increased transparency of data processing and build trust and confidence in the way personal data is managed.

Further information on how the council processes personal data can found in the [Corporate Privacy Notice](#).

This policy should be read alongside the following:

- Information Security Policy
- Records Management Policy
- Data Breach Reporting Policy, Procedure and FAQs

Scope

This policy applies to the processing of all data relating to identifiable, living individuals ('**data subjects**') and sets out how the council will comply with the obligations laid out in the UKGDPR/DPA 2018. Data processing is defined in [UKGDPR Article 4\(2\)](#).

Policy Statement

The council is committed to actively demonstrating compliance with core [data protection principles](#) and therefore, personal data shall be:

- 1) processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**')
- 2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('**purpose limitation**')

¹ Processing is defined by [UKGDPR Article 4\(2\)](#) as: '...any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction...'

- 3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**)
- 4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay (**'accuracy'**)
- 5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed (**'storage limitation'**)
- 6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**'integrity and confidentiality'**)

As a responsible Data Controller, the council will ensure that:

- the fee, as required by the [Data Protection \(Charges and Information\) Regulations 2018](#) is paid on an annual basis (Registration will cover corporate operations, with separate applications being made for the Electoral Registration Officer, Superintendent Registrar and Returning Officer)
- once confirmed, the name of the Data Protection Officer is recorded with the [Information Commissioner's Office](#) and published on the council's website
- openness and transparency requirements are met via the publication of a Privacy Notice, that covers both general and service specific data processing
- it has a clear procedure for handling personal data breaches and security incidents
- information is provided to the public and employees about their statutory rights i.e., Data Subject Access
- at a **minimum** data collection has a clear business purpose and lawful basis
- organisational records are managed in accordance with the Records Management Policy
- records with limited business use are **either** retained for archival/research purposes or destroyed in accordance with the council's Retention and Disposal Schedule
- all elected members, employees and contractors are informed about their responsibilities via a programme of training and regular/thematic communications

Roles and Responsibilities

There are a number of officers and teams across the Council that have professional expertise relating to data protection and information security.

However, it is important that anyone with legitimate access to council data understands their responsibility to ensure information and data is held securely, processed appropriately.

The Chief Executive as Accounting Officer has delegated the overall security responsibility for security, policy and implementation to the Senior Information Risk Owner (SIRO).

The Senior Information Risk Owner (SIRO) is responsible for the council's approach to managing information risk, including:

- acting as corporate champion for information governance including security and data protection
- providing a focus for the management of information governance at a senior level
- ensuring that a Data Protection Officer is identified
- ensuring that the council has identified an Information Security Manager

- ensuring that the council has appropriate information security policies in place
- providing advice and reports in respect of information security incidents/risks
- assessing how the council's strategic priorities may be impacted by these incidents/risks and how they can be managed, resourced and scrutinised effectively

To manage identified risks the SIRO is supported by a group of professionals, who can provide advice on the operational and technical aspects of effect data management

The Senior Information Risk Owner is required to be registered with the [NHS Digital - Organisation Data Service](#)

This includes the appointment of one or more Deputy SIROs, usually the Chief Legal and Monitoring Officer or Assistant Director - ICT.

To manage identified risks the SIRO is supported by a group of professionals, who can provide advice on the operational and technical aspects of effect data management.



Role	Responsibilities
Deputy Senior Information Risk Owner(s)	Authorised either jointly or alone, to act in the absence of the SIRO to: <ul style="list-style-type: none"> • make decisions regarding referrals to the ICO, • chair the weekly SIRO Review Meeting • consider the risks and activity contained in the SIRO Data Breach Report as supplied by the Data Protection Officer.
Chief Legal and Monitoring Officer	The council's Chief Legal and Monitoring Officer is responsible for providing legal opinion as requested by the Chief Executive or SIRO.
Data Protection Officer(s)	The council is required as a public authority to have a Data Protection Officer (DPO) who is responsible for: <ul style="list-style-type: none"> • monitoring data protection compliance • providing advice, guidance and training to employees and members • maintaining data protection documentation • acting as the point of contact for data protection issues with the Information Commissioners Office • working alongside the Information Security Manager to ensure the organisational and technical requirements of the UK General Data Protection Regulation (UKGDPR) are fully implemented
Caldicott Guardian	Supports the SIRO and acts as the conscience of the organisation and is responsible for protecting client and service-user confidentiality. The Caldicott Guardian is required to be registered with the NHS Digital - Organisation Data Service .

Information Security Manager	<p>The Information Security Manager is responsible for:</p> <ul style="list-style-type: none"> • working alongside the Data Protection Officer to ensure the organisational and technical requirements of the UK General Data Protection Regulation (UKGDPR) are fully implemented • acting as a central point of contact on information security within the organisation, for both users and external organisations • implementing an effective framework for the management of security • the formulation, provision and maintenance of Information Security Policies • advising on the content and implementation of the Information Security Programme • producing and supporting the production of organisational standards, procedures and guidance on Information Security matters for review by the SIRO, Section 151 Officer, Data Protection Officer, Caldicott Guardian and other senior staff • co-ordinating information security activities particularly those related to shared information systems or IT infrastructures • liaising with external organisations on information security matters, including representing the organisation in cross-community issues • ensuring that contingency plans and disaster recovery plans are reviewed and tested on a regular basis • representing the organisation on internal and external bodies that relate to security • ensuring the systems, application and/or development of required policy standards and procedures in accordance with needs, policy and guidance set centrally • approving system security policies for the infrastructure and common services • providing an incident and alert reporting system • providing advice to employees on: <ul style="list-style-type: none"> ○ compliance ○ incident investigation ○ awareness/training ○ system accreditation ○ external service provision
Service Manager - Records Management Service	<p>The County Records Management Service (RMS) is responsible for providing advice and guidance for managing council records. It maintains, updates, and answers enquiries on the Retention and Disposal Schedule, which details how long to keep records. RMS also manages paper records for services that came under Cumbria County Council prior to April 2023 (storage, retrieval, and disposal of records). These are records that are no longer needed for day-to-day business activities but are still required to meet legal and ongoing business requirements.</p>
Information Governance/ Investigations Coordinator	<p>Responsible for:</p> <ul style="list-style-type: none"> • monitoring data breaches and • supporting the Senior Information Risk Owner (SIRO) in ensuring that appropriate action is taken
Disclosure Officer	<p>Responsible for supporting the Information Governance and Investigations Coordinator/Data Protection Officer to manage/ investigate data breaches and maintain the council's data Breach Reporting System.</p>
Information Asset Owners (IAOs)	<p>The nominated, senior owner of one of more organisational assets as listed in the council's Information Asset Register (IAR). Responsible for:</p> <ul style="list-style-type: none"> • supporting the SIRO to manage risks • identification of assets • managing data breaches/security incidents • effective implementation of policies and procedures
Information Asset Administrators (IAAs)	<p>The nominated, administrator of one of more organisational assets as listed in the council's Information Asset Register (IAR). Responsible for:</p> <ul style="list-style-type: none"> • consulting with the SIRO/IAO/DPO/ISM • updating policies/procedures • identifying data breaches/ security incidents • providing advice to asset users

Executive Directors/Line Managers	<p>Executive Directors and Line Managers are responsible for:</p> <ul style="list-style-type: none"> ensuring that all employees complete mandatory Information Security and Data Protection eLearning on an annual basis ensuring that the security of the organisation's information assets (e.g., information, hardware and software used by staff and, where appropriate, by third parties) is consistent with legal and management requirements and obligations ensuring that employees, temporary and contracted staff, contractors, elected members and third parties acting for the council conform with System Security Policies and Security Operating Procedures understanding and reducing risk to information risk within the directorate assigning ownership to information assets ensuring that their employees are aware of their security responsibilities ensuring directorate arrangements are in place to manage information risk provide assurance that information assets are protected against security risks and threats
Employees	<p>All council employees, temporary and contracted staff, contractors, elected members and third parties acting for the council have a statutory duty of confidentiality to protect information and only use it for the purposes for which it was intended.</p> <p>All users have a duty to:</p> <ul style="list-style-type: none"> complete mandatory Information Security and Data Protection eLearning on an annual basis conform to System Security Policies and Security Operating Procedures be aware of their security responsibilities safeguard hardware, software and information in their care prevent the introduction of malicious software on the organisation's IT systems report on any suspected or actual breaches in security be aware that any breach of confidentiality is a serious matter which may result in disciplinary action by the council or the appropriate professional regulatory body

Data Protection Officer (DPO)

Under the UKGDPR, the council is required to appoint a Data Protection Officer (DPO) as:

- it is a public authority or body
- core activities require large scale, regular and systematic monitoring of individuals
- core activities consist of large-scale processing of special categories of data

The Data Protection Officer can be contacted at:

Email: dataprotection@cumberland.gov.uk

Post: Cumberland Council, Cumbria House, 117 Botchergate, Carlisle, Cumbria CA1 1RD

Rights - Subject Access

The UKGDPR provides you with the right to access the personal, special category personal or criminal/law enforcement data 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

We will not disclose:

- any information that relates to a third party as this will breach their rights under UKGDPR/Data Protection Act 2018
- where a professional thinks disclosure would cause serious harm to you or someone else
- information that may hinder the prevention or detection of crime.

Please note: From 1 April 2023, for a transitional period, individuals wishing to submit a Data Subject Access Request should do so via legacy websites, as listed below:

- [Cumbria County Council](#)
- [Allerdale Borough Council](#)
- [Carlisle City Council](#)
- [Copeland Borough Council](#)

Once new systems and processes have been agreed and implemented, they will be made available via the Cumberland Council website.

Rights - Other

In addition to the right of access, the council is also required to comply with the additional rights contained [UKGDPR Articles 16-22](#):

Rectification	Individuals have the right to have personal data rectified if it is inaccurate or incomplete.
Erasure	Individuals have the right to have personal data deleted or removed where there is no compelling reason for its continued processing ⁴ .
Restriction	Individuals have a right to 'block' or suppress processing of personal data depending on whether the information is collected by statute or consent. When processing is restricted, the Council can store the personal data, but not further process it. Just enough information about the individual to ensure that the restriction is respected in future should be retained.
Portability	In specific situations, an individual can request a copy of their personal data in a format that they can take to another provider. This is rare in local government as it relies on automated processing in which no person is involved in the processing.
Object	The individual can object to processing in three areas and the council should have a process in place to respond to these objections. <ol style="list-style-type: none"> 1. Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling). This means processing where it is done in the public interest and the individual disagrees that the public interest has been assessed correctly. 2. Direct marketing (including profiling) means that any direct marketing the Council does must stop if an individual objects. 3. Processing for purposes of scientific/historical research and statistics. In certain circumstances, an individual can object to having their personal data included in some scientific/historical research and statistics.

Unless stated otherwise, individuals can exercise any of these rights by contacting:

Email: dataprotection@cumberland.gov.uk
Post: Cumberland Council, Cumbria House, 117 Botchergate, Carlisle, Cumbria CA1 1RD

Timescales and Extensions

The council is required to process Data Subject Access Requests, and any other rights-based requests, promptly within the statutory timescale of **one calendar month**.

The council would not expect every request to take one calendar month and will endeavour, where possible, to provide the requested information at the earliest opportunity from the date of the request.

However, if the council considers the request to be complex, they may extend the time by up to two extra calendar months². In this instance the council will notify the applicant in writing that the DSAR requires further time and will provide an estimate of a 'reasonable time' by which they expect a response to be made. These estimates must be realistic and reasonable taking into account the circumstances of each particular case.

Consent

Where the council is relying on [UKGDPR Article 6\(1\)\(a\)](#) or [Article 9\(2\)\(a\)](#) to process any personal identifiable data, the individual who has provided their consent has the right [UKGDPR Article 7\(3\)](#) to withdraw their consent at any time.

If consent is withdrawn, the council must stop processing data for the identified purpose, unless there is an alternative lawful basis available. Where an individual withdraws their consent any data processing that has occurred prior to the objection being received will not be affected. Individuals must be advised of the impact of withdrawing consent, specifically where they are in receipt of essential services.

Individuals wishing to withdraw their consent should, in the first instance contact the service responsible for collecting their data. Specific questions or concerns can be sent to dataprotection@cumberland.gov.uk.

Refusing Requests

The council will not supply information to a data subject if:

- the request is not clear enough for the council to conduct an effect search
- the identity of the data subject cannot be identified
- responding to the request will inadvertently disclose personal information relating to another individual without their consent
- the same or similar information has been requested within the last 3 months (dependent on nature of data)

The council considers that when a valid reason, which is both robust and legally defensible, exists for refusing the disclosure of information to either the data subject or a third party, the information should be withheld.

When information is withheld, full explanations of the reasoning behind the refusal must be provided to the applicant. This explanation must also include the details of how the applicant can complain about the council's decision.

² [UKGDPR Article 12\(3\)](#)

Verifying Your Identity

When exercising the rights mentioned above, the council is permitted under [UKGDPR Article 12\(6\)](#) to request additional information where the identity of data subjects cannot be confirmed. Please note that:

- additional documentation will only be required when the council cannot confirm the identity of data subjects using internal systems and/or data sources
- documentation from data subjects should be requested prior to processing requests
- the statutory deadline for responding to requests will only start when additional documentation is provided
- failure to provide additional documentation may lead to the council rejecting requests

Data Breaches

The Council is legally required under the UK General Data Protection Regulation ("UKGDPR") to ensure the security and confidentiality of the data it holds.

The council is required to maintain data breach detection, investigation and internal reporting procedures to ensure that risks are identified, contained and managed effectively.

These procedures include the requirement under UKGDPR Article 33 to report certain types of personal data breaches to a supervisory authority - the [Information Commissioner's Office](#) (ICO).

In the event of a significant data breach that is likely to affect individuals' rights and freedoms, the council will:

- report it to the ICO within 72 hours of becoming aware of it (where relevant); and
- tell the individuals concerned (where required)

Data breaches can be reported using the [Data Breach Online Reporting Form](#) or by email to dataprotection@cumberland.gov.uk.

Complaints

There are two separate areas where individuals can raise complaints:

- responses received to Data Subject Access Requests
- handling of personal, special category or criminal/law enforcement data

Where an individual has received a response to a Data Subject Access Request and they believe, for example that it is incomplete, they should raise this with the relevant council via the Internal Review Procedure.

- [Cumbria County Council](#)
- [Allerdale Borough Council](#)
- [Carlisle City Council](#)
- [Copeland Borough Council](#)

Complaints submitted for consideration under the Internal Review Procedure will be processed in most cases within twenty working days. If an extension is required individuals will be informed directly.

Where an individual is dissatisfied with the handling of their personal data, they should in the first instance contact the service responsible for the provision or management of their data. Advice can be requested from dataprotection@cumberland.gov.uk.

In both instances, although the council should be given the opportunity to address areas of concern directly, individuals have the right to complain to the Information Commissioner (ICO) at any time. The ICO can be contacted by:

Telephone: 0303 123 1113

Online: <https://ico.org.uk/make-a-complaint/>

Live Chat: <https://ico.org.uk/global/contact-us/contact-us-public/public-advice/>