Cumbria County Council

UKGDPR Compliance Policy

Version 3.0
March 2022

Document History and Authorisation

Related Documents

Title	Author	Version/Date
Information Security Policy	Information Security Manager	1.7/January 2020

Document Revision

Release Date	Revision Version	Summary of Changes
2020-01-16	0.1	Content review/update by DPO
2020-01-22	1.0	Version reviewed by SIRO PRG
2020-06-04	1.1	Document reviewed by DPO, and typos corrected. No material change to content. As approved by SIRO.
2021-02-24	2.0	Document updated based on recommendations from Internal Audit.
2022-03-07	3.0	Content review/update by DPO

Document Review

This document (or component parts) has been reviewed by the following:

Officer Name/Position	Revision Version	Circulation Date
SIRO Performance Review Group	1.0	2020-01-22
SIRO Performance Review Group	2.0	2021-02-24
SIRO Performance Review Group	3.0	2022-03-17

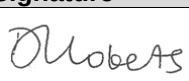
Document Approval

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

Version	Approval Date
1.0	2020-01-22
2.0	2021-02-24
3.0	2022-03-17

This Policy will be reviewed by the Data Protection Officer at on an annual basis from the date of formal approval.

Authorised Signatory

Officer Name	Position	Version	Signature	Date
Dawn Roberts	Executive Director - Corporate Customer and Community Services/Senior Information Risk Owner (SIRO)	3.0		2022-03-17

Policy Statement

Cumbria County Council is a *data controller*[1] for the purposes of the UK General Data Protection Regulation (UKGDPR) and Data Protection Act 2018 (DPA), but also has specific responsibilities under the Human Rights Act (1998) (HRA).

This policy applies to the processing[2] of all data relating to identifiable, living individuals (data subjects) and sets out how the council will comply with organisational and technical requirements.

The council is committed to complying 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] UKGDPR Article 4(7): '…means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data…'

[2] UKGDPR Article 4(2) '…means 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
- 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
- it has a clear procedure for handling personal data breaches and security incidents
- information is provided to the public about their statutory rights i.e., Data Subject Access
- at a **minimum** data collection has a purpose/legal basis to comply with core principles
- current 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 Senior Information Risk Owner (SIRO) is responsible for the council's approach to managing information risk. This includes 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 these risks the SIRO is supported by a group of professionals, who can provide advice on the operational and technical aspects of effect data management.

Deputy Senior Information Risk Owners

Authorised either jointly or alone, to act in the absence of the SIRO to:
- 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.

Data Protection Officer (DPO)

The council is required as a public authority to have a Data Protection Officer (DPO).
Responsible for:
- monitoring data protection compliance,
- providing advice, guidance and training to employees and members,
- maintaining data protection documentation, and
- acting as the point of contact for data protection issues with the Information Commissioners Office.

Caldicott Guardian

Supports the SIRO and acts as the conscience of the organisation and is responsible for protecting client and service-user confidentiality.

Information Security Manager

Responsible for:
- implementing an effective framework for the management of security
- formulation, provision and maintenance of Information Security Policies

Information Governance/ Investigations Coordinator

Responsible for:
- monitoring data breaches and
- supporting the Senior Information Risk Owner (SIRO) in ensuring that appropriate action is taken

Disclosure Officer

Responsible for:
- supporting the Information Governance and Investigations Coordinator/Senior IG and Data Protection Officer to manage/investigate data breaches
- maintaining the Data Breach Log

Other critical roles include:

IG/Complaints Service Lead
Responsible for: • handling operational requests for information under the Freedom of Information Act/Environmental Information Regulations/Data Protection Act, and all statutory/corporate complaints.
Information Asset Owners (IAOs)
The nominated, senior owner of one of more organisational assets as listed in the council's Information Asset Register (IAR). Responsible for: • supporting the SIRO to manage risks • identification of assets • managing data breaches/security incidents • effective implementation of policies and procedures
Information Asset Administrators (IAAs)
The nominated, administrator of one of more organisational assets as listed in the council's Information Asset Register (IAR). Responsible for: • consulting with the SIRO/IAO/DPO/ISM • updating policies/procedures • identifying data breaches/ security incidents • providing advice to asset users
Senior Managers
Responsible for: • ensuring operational compliance with this policy within their own departments • contributing to Data Breach investigations (where required)
All Employees
Responsible for: • ensuring that Data Subject Access Requests and data breaches are dealt with in accordance with this policy • ensuring that personal data is processed appropriately i.e. that personal data supplied to the council is accurate, up-to-date and held securely.

Data Protection Officer

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

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

The Data Protection Officer can be contacted by:

Online: Contact the DPO
Email: dataprotection@cumbria.gov.uk
Post: Data Protection Officer, Legal and Democratic Services, 1st Floor - Cumbria House, 117 Botchergate, Carlisle, Cumbria CA1 1RD

Data Subject Access Requests (DSARs)

UKGDPR Article 15 provides individuals with the right to access information the council, as a public authority holds about them. This is commonly referred to as a Data Subject Access Request (DSAR). Requests can be made in the following ways:

Online: Make a Request
Post: Information Governance Team, Corporate, Customer & Community Services –Cumbria County Council, Parkhouse, Baron Way, Carlisle, CA6 4SJ
Email: information.governance@cumbria.gov.uk
Phone: (01228) 221234

Upon receipt of a **valid request** the Information Governance Team will:

- provide advice to assist individuals to formulate requests
- verify data subject identity where they are unknown to the council or have not used council services for a significant period
- seek additional clarification where the information sought is not described in a way that would enable the council to identify and locate the requested material, or the request is ambiguous
- seek evidence of consent from an individual where a third party has requested access to their personal data
- provide a response within one month
- inform individuals if an extension may be required
- make reasonable efforts to comply with the format of the request
- confirm if the request is going to be refused or a charge is payable[3]

Timescales and Extensions

The council is committed to dealing with requests for information promptly and no later than the statutory guideline of **one calendar month**.

The council would not expect every application for information 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 months[4]. 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 shall be realistic and reasonable taking into account the circumstances of each particular case.

[3] UKGDPR Article 12(5)
[4] UKGDPR Article 12(3)

Other Rights

As well as access rights data subjects also have the rights below:

Rectification	Individuals have the right to have personal data rectified if it is inaccurate or incomplete. Rectification requests should be made to the council's Data Protection Officer in the first instance.
Erasure	Individuals have the right to have personal data deleted or removed where there is no compelling reason for its continued processing[5]. Erasure requests should be made to the council's Data Protection Officer in the first instance.
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. Restriction requests should be made to the council's Data Protection Officer in the first instance.
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. Portability requests should be made to the council's Data Protection Officer in the first instance.
Object	The individual can object to processing in three areas and the council should have a process in place to respond to these objections. 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. Objection requests should be made to the council's Data Protection Officer in the first instance

Exemptions

The UKGDPR is designed to prevent access by third parties to a data subject's personal data. However, under the DPA there are circumstances which allow disclosure of a data subject's personal data to a third party, or for it to be used in a situation that would normally be considered to breach the UKGDPR.

The council will only use an exemption where it is in the public interest to do so, i.e. prevention of crime, or where the functioning of the council requires the processing of personal information to be exempt so that it can provide statutory services to members of the public.

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)

[5] If the council has a legitimate legal basis for processing personal data i.e. a legal obligation, this will be deemed to be a compelling reason.

The council considers that when a valid reason, which is both robust and legally defendable, 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.

Data Breaches

The UKGDPR places a duty on the council to report certain types of personal data breaches to a supervisory authority - the Information Commissioner's Office (ICO). When a personal data breach happens and 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)

To comply with the above requirements the council maintains breach detection, investigation and internal reporting procedures. These procedures reflect changes to the law and will enable the council to keep a record of all personal data breaches, whether they are reportable or not.

Data breaches can be reported via the council's Data Breach Reporting Form.

Appeals and Complaints

Where an applicant is dissatisfied with the level of service they have received, they are entitled to complain about the actions of the council through the Internal Review Procedure. Further details can be found at: Internal Reviews and Complaints

The applicant will receive a response to their correspondence within twenty working days. If the applicant remains dissatisfied with the council's reply, they have the option of taking their complaint to the Information Commissioner (at the address below) who will independently adjudicate each case and make a final decision.

Telephone: 0303 123 1113
Live Chat: https://ico.org.uk/global/contact-us/live-chat
Online: https://ico.org.uk/global/contact-us/