



# Cumbria County Council

## UKGDPR Compliance Policy

February 2021

# 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.

## 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

## 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	<a href="#">2021-02-24</a>

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

## Introduction

Cumbria County Council supports the objectives of the UK General Data Protection Regulation (UKGDPR) and Data Protection Act 2018 (DPA) and seeks to ensure compliance with this data protection legislation. The processing of data by the council is essential to services and functions and will often involve the use of personal and/or 'special category' personal data. Compliance with the data protection legislation will ensure that such processing is carried out fairly and lawfully. The UKGDPR and the Human Rights Act (1998) (HRA) Article 8, make it clear that the processing of personal data must respect the rights and freedoms of the data subject (individual), but at the same time be adequate enough for the council to function effectively.

This policy should not be read in isolation and regard should be given to other related council policies, including (but not limited to) the Information Security Policy.

## Purpose

The purpose of this policy is to ensure that the provisions of the UKGDPR and DPA are adhered to whilst protecting the rights and privacy of living individuals; ensuring their personal data is not processed without their knowledge. In particular this policy will:

- assist the council to comply with all requirements of the UKGDPR and DPA,
- ensure that personal data is readily available on request and that requests from data subjects are dealt with in a timely manner,
- ensure adequate consideration is given to whether or not personal information should be disclosed,
- ensure increased awareness of data subjects to the amount of personal data processed and stored by the council about them and advise them of their rights under the data protection legislation.

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

## Aims

This policy sets out the council's commitment to upholding the data protection principles set out in the UKGDPR. It seeks to:

- strike a balance between the council's need to make use of personal data to manage services efficiently/effectively whilst respecting the privacy of individuals,
- support council employees to meet their statutory obligations under the UKGDPR/DPA, and
- provide guidance to the public on the council's' obligations regarding the processing of their personal data.

## Statement

This policy applies to the collection and processing of all personal data by the council and sets out how the council will ensure that individual rights and freedoms are protected.

- the council will comply with Article 8 of the HRA in respect of the processing of personal data,
- the council, as a Data Controller, will make individuals aware of the purpose(s) it is processing their personal data for and will seek consent for that processing where appropriate,
- ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her,
- the council will manage breaches of the UKGDPR in accordance with the Data Breach Reporting Policy and Procedure,
- the council will provide general information to the public about their statutory rights under the UKGDPR and DPA on its [website](#),
- the council will hold the minimum amount of personal data necessary to carry out its functions, and every effort will be made to ensure the accuracy and relevance of this data,
- the council will keep all electronic and manual records in accordance with its Records Management Policy,
- the personal data the council holds will be kept in accordance with the [six principles](#) of the UKGDPR and in line with the council’s Retention and Disposal Schedule,
- periodically a risk assessment will be undertaken, via audit reviews, for all data processing, and when inadequate controls are identified, technical and organisational security measures will be taken, appropriate to the level of risk identified,
- personal data will only be used for the direct promotion or marketing of goods or services with the explicit consent of an individual,
- elected members and staff will be trained to an appropriate level in the use and supervision of personal data,
- breaches of this policy may be subject to action under the council’s disciplinary procedure.

## Principles

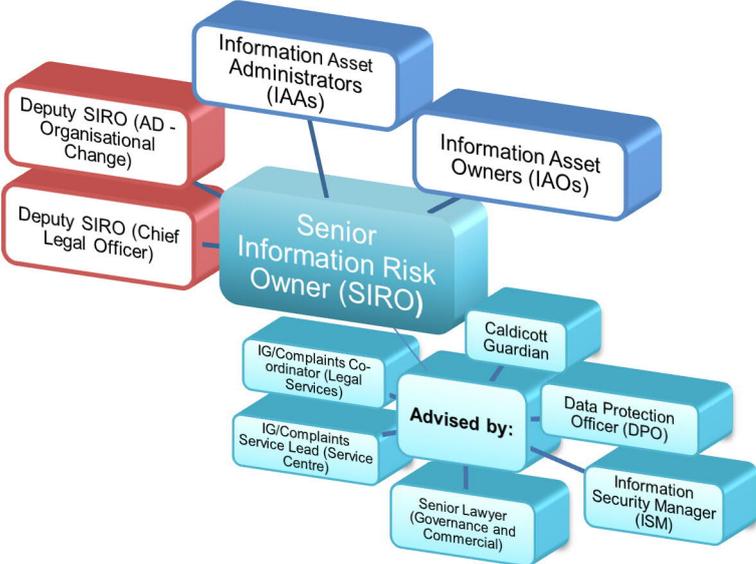
The council will comply with the following data protection principles, personal data shall be:

- 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’**)
- 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**')

### 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.



Role	Description
<b>Senior Information Risk Owner (SIRO)</b>	Responsible for: <ul style="list-style-type: none"> <li>acting as corporate champion for information governance,</li> <li>providing a focus for the management of information governance at a senior level,</li> <li>providing advice and reports in respect of information security incidents/risks,</li> <li>assessing how the council's strategic priorities may be impacted by these incidents/risks and how they can be managed, resourced and scrutinised effectively</li> </ul>
<b>Deputy Senior Information Risk Owners</b>	Are authorised either jointly or alone, to act in the absence of the SIRO to make decisions regarding referrals to the ICO, to chair the weekly SIRO Review Meeting and to consider the risks and activity contained in the SIRO Data Breach Report as supplied by the Data Protection Officer.
<b>Data Protection Officer (DPO)</b>	The council is required as a public authority to have a Data Protection Officer (DPO).  Responsible for: <ul style="list-style-type: none"> <li>monitoring data protection compliance,</li> <li>providing advice, guidance and training to employees and members,</li> <li>maintaining data protection documentation, and</li> <li>acting as the point of contact for data protection issues with the Information Commissioners Office.</li> </ul>
<b>Caldicott Guardian</b>	Supports the SIRO and acts as the conscience of the organisation and is responsible for protecting client and service-user confidentiality.

<b>Information Security Manager</b>	Responsible for: <ul style="list-style-type: none"> <li>Implementing an effective framework for the management of security,</li> <li>formulation, provision and maintenance of Information Security Policies.</li> </ul>
<b>Information Governance and Investigations Coordinator</b>	Responsible for: <ul style="list-style-type: none"> <li>receiving all data breaches and supporting the Senior Information Risk Owner (SIRO) in ensuring that appropriate action is taken.</li> </ul>
<b>IG/Complaints Service Lead</b>	Responsible for: <ul style="list-style-type: none"> <li>handling operational requests for information under the Freedom of Information Act/Environmental Information Regulations/Data Protection Act, and</li> <li>all statutory/corporate complaints.</li> </ul>
<b>Senior Lawyer (Governance and Commercial)</b>	Responsible for: <ul style="list-style-type: none"> <li>line management of Information Governance and Investigations Coordinator/Senior IG and Data Protection Officer</li> </ul>
<b>Disclosure Officer</b>	Responsible for: <ul style="list-style-type: none"> <li>supporting the Information Governance and Investigations Coordinator/Data Protection Officer to manage/ investigate of data breaches,</li> <li>maintaining the Data Breach Log</li> </ul>
<b>Information Asset Owners (IAOs)</b>	The nominated, senior owner of one of more organisational assets as listed in the council's Information Asset Register (IAR).  Responsible for: <ul style="list-style-type: none"> <li>supporting the SIRO to manage risks</li> <li>identification of assets</li> <li>managing data breaches/security incidents</li> <li>effective implementation of policies and procedures</li> </ul>
<b>Information Asset Administrators (IAAs)</b>	The nominated, administrator of one of more organisational assets as listed in the council's Information Asset Register (IAR).  Responsible for: <ul style="list-style-type: none"> <li>consulting with the SIRO/IAO/DPO/ISM</li> <li>updating policies/procedures</li> <li>identifying data breaches/ security incidents</li> <li>providing advice to asset users</li> </ul>
<b>Senior Managers</b>	Responsible for: <ul style="list-style-type: none"> <li>ensuring operational compliance with this policy within their own departments</li> <li>contributing to Data Breach Investigations in consultation with the Information Governance and Investigations Coordinator and/or Data Protection Officer where required.</li> </ul>
<b>All Employees</b>	Responsible for: <ul style="list-style-type: none"> <li>ensuring that Data Subject Access Requests and data breaches are dealt with in accordance with this policy,</li> <li>ensuring that personal data is processed appropriately i.e. that personal data supplied to the council is accurate, up-to-date and held securely.</li> </ul>

## Data Subject Access Requests (DSARs)

Article 15 of the UKGDPR 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).

Unlike the Data Protection Act 1998 where requests could be in writing, the UKGDPR permits applicants to make DSARs in recorded form i.e. email, letter and also by telephone or in person.

To support this the council will accept DSARs 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](mailto: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.

## 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. 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.

## Data Subject Rights

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

<b>Transparency</b>	Where the council is processing personal data it is required to communicate this to the individual's data is being processed about. For more information see the <a href="#">Corporate Privacy Notice</a> .
<b>Access</b>	See ' <a href="#">Data Subject Access Requests</a> '
<b>Rectification</b>	Individuals have the right to have personal data rectified if it is inaccurate or incomplete. Rectification requests should be made to the council's <a href="#">Data Protection Officer</a> in the first instance.
<b>Erasure</b>	Individuals have the right to have personal data deleted or removed where there is no compelling reason for its continued processing <sup>1</sup> . Erasure requests should be made to the council's <a href="#">Data Protection Officer</a> in the first instance.
<b>Restriction</b>	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

<sup>1</sup> 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.

	future should be retained. Restriction requests should be made to the council's <a href="#">Data Protection Officer</a> in the first instance.
<b>Portability</b>	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 <a href="#">Data Protection Officer</a> in the first instance.
<b>Object</b>	<p>The individual can object to processing in three areas and the council should have a process in place to respond to these objections.</p> <ol style="list-style-type: none"> <li>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.</li> <li>2) Direct marketing (including profiling) means that any direct marketing the Council does must stop if an individual objects.</li> <li>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.</li> </ol> <p>Objection requests should be made to the council's <a href="#">Data Protection Officer</a> in the first instance</p>

## 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)

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.

## 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 (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 to the council's [Data Protection Officer](#).

## 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.

Post: Information Commissioner's Office Wycliffe House, Water Lane Wilmslow  
Cheshire SK9 5AF

E-mail: [casework@ico.org.uk](mailto:casework@ico.org.uk)

Online: <https://ico.org.uk/make-a-complaint/your-personal-information-concerns/>

## 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](mailto:dataprotection@cumbria.gov.uk)

Post: Data Protection Officer, Legal and Democratic Services, 1<sup>st</sup> Floor - Cumbria House, 117 Botchergate, Carlisle, Cumbria CA1 1RD