Allerdale – a great place to live, work and visit


## **Data Protection Policy**

Aims to ensure a consistent approach to data protection within the Council

 Version 1.1

**Document Control**

|  |  |
| --- | --- |
| **Title** | Allerdale Borough Council – Data Protection Policy |
| **Document Type** | Approved Document |
| **Author** | Jo Doran – Information Governance and Data Protection Officer |
| **Owner** | SIRO |
| **Subject** | Information Governance |
| **Created** | March 2018 |

**Version Control Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Detail**  | **Author** | **Approver** |
| 1.0 | 05/04/18 | New document | J Doran | SMT |
| 1.1 | 26/02/19 | Appendix 1 – Law Enforcement Processing  | J Doran | Nik Hardy |
|  |  |  |  |  |
|  |  |  |  |  |
| Next review date: 05/04/19 |

**Table of Contents**

Introduction………………………………………………………………………………...[4](#_Toc456294029)

[1.0 Data Protection Principles 4](#_Toc456294030)

[2.0 Key definitions 5](#_Toc456294031)

[2.1 Personal Data 5](#_Toc456294032)

[2.2 Sensitive Personal Data 5](#_Toc456294033)

[2.3 Processing 5](#_Toc456294034)

[2.4 Data Controller 5](#_Toc456294035)

[2.5 Data Processor 5](#_Toc456294036)

[3.0 Personal data processed by the Council 6](#_Toc456294042)

4.[0 Lawful Basis for Processing 6](#_Toc456294048)

[4.1 Consent 6](#_Toc456294049)

[4.2 Contract 6](#_Toc456294050)

[4.3 Legal Obligation 7](#_Toc456294051)

[4.4 Vital Interests 7](#_Toc456294051)

[4.5 Public Task 7](#_Toc456294050)

[4.3 Legitimate Interests 8](#_Toc456294051)

[5.0 Individuals’ Rights 8](#_Toc456294052)

[5.1 Right to be informed 8](#_Toc456294053)

[5.2 Right to access 8](#_Toc456294054)

[5.3 Right to rectification 9](#_Toc456294055)

[5.4 Right to erasure 9](#_Toc456294056)

[5.5 Right to restrict processing 9](#_Toc456294057)

[5.6 Data Portability 9](#_Toc456294058)

[5.7 Right to object 10](#_Toc456294059)

[5.8 Rights related to automated decision making, including profiling 10](#_Toc456294060)

[6.0 Derogations/Exemptions 10](#_Toc456294062)

[7.0 Policies and Procedures 11](#_Toc456294062)

[8.0 Data Sharing 11](#_Toc456294062)

[9.0 Staff Training 11](#_Toc456294062)

[10.0 Sources of Information and Guidance 11](#_Toc456294062)

[Appendix 1 – Law Enforcement Processing 1](#_Toc456294062)3

**Introduction**

The processing of personal data is essential to many of the services and functions carried out by local authorities. Allerdale Borough Council (‘the Council’) recognises that compliance with prevailing data protection legislation will ensure that processing is carried out fairly, lawfully and transparently.

The Data Protection Act 1998 (DPA) will be replaced on 25 May 2018 by the General Data Protection Regulation (GDPR). Introduced to harmonise data protection across the European Union and to keep pace with modern digital advances, the GDPR is more extensive in scope and application than previous legislation. The Regulation extends the data rights of individuals, and requires organisations to develop clear policies and procedures to protect personal data, and adopt appropriate technical and organisational measures.

This policy applies to the collection and processing of all data held by the organisation, whether in paper or electronic format, that falls within the definition of ‘personal information’. It sets out how the Council adheres to data protection legislation and safeguards the rights and freedoms of all those utilising our services, including our staff.

**1.0 Data protection principles**

Under the GDPR, the data protection principles set out the main responsibilities for the Council. GDPR requires that personal data shall be:

* processed lawfully, fairly and in a transparent manner in relation to individuals;
* collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
* adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
* accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
* kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
* 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.

The Council must be able to demonstrate compliance with these principles.

**2.0 Key Definitions**

UnderGDPR the following definitions apply:

**2.1 Personal data**

*“…any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person* **Art.4(1)**

Personal data that has been pseudonymised, e.g. key-coded, can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

**2.2 Sensitive personal data**

*“…personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation;****genetic data or biometric data****. Data relating to criminal offences and convictions are addressed separately (as criminal law lies outside the EU's legislative competence)*. **Art.9(1)**

**2.3 Processing**

*"…any operation or set of operations performed upon personal data or 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.”* **Art.4(2)**

**2.4 Data Controller**

 *“… the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller (or the criteria for nominating the controller) may be designated by those laws.”* Art.4(7)

**2.5 Data Processor**

*"… a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.”* **Art.4(8)**

**3.0 Personal data processed by the Council**

The Council processes personal data for many reasons, in relation to both the services we provide and as an employer. A description of the types of personal data processed, together with the purposes of processing, is included in our Data Protection Registration entry (reference Z5680850) which is publicly available on the Information Commissioner’s Office website:<https://ico.org.uk/ESDWebPages/Entry/Z5680850>

**4.0 Lawful basis for processing**

The Council must process personal data to carry out our functions as a borough council, but we can only do this where there is a legal basis. This is known as the ‘lawful basis for processing’. There are six available lawful bases for processing and, whilst no single basis is ’better’ or more important than the others, before processing can begin we must decide which is most appropriate. This depends on our purpose and the relationship we have with the individual in question (known as the Data Subject).

In order to process sensitive personal data, the Council must not only have a lawful basis, but also an additional condition from Article 9 of the GDPR.

In order to process criminal conviction data/offences there must be a lawful basis plus an additional condition from Article 10.

Our lawful basis for processing is covered in our Privacy Notice.

* 1. **Consent**
* Requires positive opt-in
* Consent requests must be kept separate from other terms & conditions
* It must name any third parties who will also rely on the consent
* It should be easy for people to withdraw consent and we must tell Data Subjects how to do this
* The Council will keep a record who, when, how and what we told people
* Consent cannot be a precondition of a service
* It is only appropriate if we can offer real choice and control over how we use the data
* Where we are in a position of power over individuals we should avoid relying on consent unless we can demonstrate it is freely given.

**4.2 Contract**

This is the appropriate lawful basis where we need to process personal data:

* to fulfil our contractual obligations; or
* to do something before entering into a contract (e.g. provide a quote).

It does not apply if we need to process one person’s details but the contract is with someone else or if we take pre-contractual steps on our own initiative or at the request of a third party.

The contract does not have to be a formal signed document, or even written down, as long as there is an agreement which meets the requirements of contract law. Broadly speaking, this means that the terms have been offered and accepted, the Council and the other party/parties intend them to be legally binding, and there is an element of exchange (usually an exchange of goods or services for money, but this can be anything of value).

The processing must be necessary to deliver our side of the contract with a particular person. If the processing is only necessary to maintain our business model more generally, this lawful basis will not apply and we should consider another lawful basis.

* 1. **Legal obligation**

This is relevant if we need to process the personal data to comply with a common law or statutory obligation. We should be able to identify the obligation in question, either by reference to the specific legal provision or else by pointing to an appropriate source of advice or guidance that sets it out clearly. For example, we can refer to a government website or to industry guidance that explains generally applicable legal obligations

**e.g.**The Council needs to process personal data to comply with its legal obligation to disclose employee salary details to HMRC.

* 1. **Vital interests**

There is very limited scope to use this basis and it generally only applies to matters of life and death.

**4.5 Public task**

ICO guidance states that public authorities, such as the Council, need to consider the new ‘public task’ basis first for most of our processing:

 “*If you are a public authority and can demonstrate that the processing is to perform your tasks as set down in UK law, then you are able to use the public task basis.”* ICO

This includes:

* carrying out a specific task in the public interest which is laid down by law (statute or common law); or
* exercising official authority (for example, a public body’s tasks, functions, duties or powers) which is laid down by law

**What does ‘laid down by law’ mean?**

It includes clear common law tasks, functions or powers as well as those set out in statute or statutory guidance.

**4.6 Legitimate interest**

This is the most flexible basis for processing and is most likely to be an appropriate basis where we use data in ways that people would reasonably expect and that have a minimal privacy impact. However, public authorities can only rely on legitimate interests if we are processing for a legitimate reason other than performing our tasks as a public authority.

Before we can use this lawful basis we need to carry out a 3-part test to assess whether legitimate interests applies:

1. Purpose test: are we pursuing a legitimate interest?
2. Necessity test: is the processing necessary for that purpose?
3. Balancing test: do the individual’s interests override the legitimate interest?

**5.0 Individuals’ rights**

The GDPR provides several rights for individuals in terms of the processing of their personal data. However, the lawful basis for processing determines which of these rights are available to our customers and staff. This means that, due to the nature of our business, not all of the individuals’ rights listed below are applicable. For example:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lawful Basis** | **Right to Erasure** | **Right to Portability** | **Right to Object** |
| **Consent** | ✓ | ✓ | 🗶 |
| **Contract** | ✓ | ✓ | 🗶 |
| **Legal Obligation** | 🗶 | 🗶 | 🗶 |
| **Vital Interests** | ✓ | 🗶 | 🗶 |
| **Public Task** | 🗶 | 🗶 | ✓ |
| **Legitimate Interests** | ✓ | 🗶 | ✓ |

The Council must comply with any exercise of individuals’ rights within one month of receiving the request, or up to two months on grounds of complexity (the data subject must be told of the further time required within the initial one-month period).

**5.1 Right to be informed**

The GDPR sets out the information that we must supply and when individuals must be informed. We do this through a ‘Privacy Notice’. The notice also provides more details on which lawful basis for processing we use.

**5.2 Right to access**

The reason for allowing individuals to access their personal data is so that they are aware of what we hold and can verify that we have a valid lawful basis to process it. We will usually supply this information free of charge unless the request is manifestly unfounded or excessive. As we must verify the identity of the person making the request individuals will be asked to provide two proofs of identity, including confirmation of their current address. Copies will be accepted if posted but we reserve the right to have sight of original documentation. A signed letter of authority from the data subject will be required if someone else is acting as their agent.

Normally we will disclose the requested information but on occasion it may not be possible to do so if supplying it would be likely to, for example, compromise the way a crime is detected/prevented.

**5.3 Right to rectification**

Individuals can ask us to rectify any inaccuracies in the personal data we hold about them e.g. incomplete data. Where we’ve disclosed the personal information to a third party we must also inform them of the rectification where possible. If we do not take any action in response to a request for rectification we will notify the individual and inform them of their right to complain to the ICO.

**5.4 Right to erasure** (Formerly the Right to be forgotten)

Individuals can ask us to do this where there is: a problem with the underlying legality of processing; consent is withdrawn; the data is no longer necessary for the purpose for which it was collected or processed; or there is no overriding legitimate interest for continuing the processing. The Council will also inform any third parties to whom we have already disclosed the personal data, unless it is impossible or involves a disproportionate effort.

**5.5 Right to restrict processing**

This is where data is held in limbo whilst challenges to its processing are resolved. The right is only relevant where: an individual disputes the accuracy of the personal data; where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our organisation’s legitimate grounds override those of the individual; where processing is unlawful but the individual objects to erasure; or where we’ve no further use for the data but an individual requires it for legal claims. In these circumstances the Council may store the personal data but not process it further. However, we will retain just enough information about the individual to ensure that the restriction is respected in the future.

**5.6 Data portability**

This right allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way. However, it only applies to personal data which the individual has provided to us, where processing is based on consent or in performance of a contract and when processing is carried out by automated means.

If the individual requests it, and it is technically feasible, we may transfer data directly to another organisation. If we are unable to comply we will let the individual know and inform them of their right to complain to the ICO.

**5.7 Right to object**

This right only covers specific types of processing, i.e. direct marketing or processing carried out in performance of our public task (in the exercise of our official authority). If the Council are using public task as the lawful basis for processing, we must cease processing unless we can demonstrate: compelling legitimate grounds which override the interests, rights and freedoms of the individual; or where processing is required for legal claims.

Please note, this does not give individuals the right to object to processing in general. The only absolute right to object is to direct marketing.

On-line systems must offer an automated method of objecting.

**5.8 Rights related to automated decision making, including profiling**

Automated individual decision-making is a decision made by automated means without any human involvement. Information is analysed to classify people into different groups or sectors, using algorithms and machine-learning. This analysis identifies links between different behaviours and characteristics to create profiles for individuals.

We must tell our customers about the profiling and automated decision-making we carry out, what information we use to create the profiles and where we get this information from.

**6.0 Derogations/Exemptions**

As with the previous data protection legislation Article 23 of the GDPR allows member states to introduce derogations to data protection law in certain situations. This means that the UK can introduce derogations from transparency obligations and data subject rights, but only where the measure “*respects the essence of … fundamental rights and freedoms and is … necessary and proportionate … in a democratic society*”.

An example of this is Section 29 of the DPA which currently provides an exemption to data processing rules for the purposes of the prevention or detection of crime, or the apprehension or prosecution of offenders. As the GDPR does not cover the processing of personal data for law enforcement purposes, the UK will implement The Data Protection Law Enforcement Directive into UK law allowing data processing for the “*prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.”*

This section will be updated as more detail becomes available.

**7.0 Policies and procedures**

The Council has approved and adopted several relevant Information Governance policies and procedures. The approval of this documentation by the Senior Management Team provides formal evidence of ownership and accountability for information.

Key policies:

* Information Governance Policy
* Information Security Policy
* Records Management Policy
* Freedom of Information Policy
* Email Policy
* Mobile Devices Policy
* Data Breach Notification Procedure
* Privacy Impact Assessment Procedure

We have ensured that appropriate physical, technical and organisational measures are in place and that employees comply with the aforementioned policies.

**8.0 Data sharing**

Any sharing of personal data with external partners, for the purposes of service provision, must comply with all statutory requirements and corporate policies. Further details are available in the Council’s ‘Information Governance Policy’.

**9.0 Staff training**

The Council’s data protection framework is supported by adequate skills, knowledge and experience across the organisation. The level of competency is in line with the duties and responsibilities of particular posts or staff groups in order to provide an adequate level of assurance.

As a minimum ALL staff must complete mandatory e-learning modules in Data Protection and GDPR. Both modules include a general overview of the subject followed by a small test which they must pass. Further details are available in the Councils ‘Information Governance Policy’.

**10.0 Sources of information and guidance**

The Council will review and supplement this policy as more legislation is enacted into UK law and relevant guidance from the ICO and the Article 29 Working Party is issued.

For more information on data protection please contact the Councils Information Governance and Data Protection Officer:

Email – foi@allerdale.gov.uk

Phone – 01900 702898

Mail – Allerdale House, Workington, Cumbria, CA14 3YJ

You can also contact the ICO at:

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF,

Phone: 0303 123 1113

[www.ico.gov.uk](http://www.ico.gov.uk)

**Appendix 1 – Law Enforcement Processing**

**Introduction**

Law Enforcement processing - Part 3 of the Data Protection Act 2018 (DPA).

The way we handle personal data; how we collect, store, use and dispose of it, is coming under growing scrutiny. Part 3 of the DPA sets out the requirements for the processing of personal data for criminal ‘law enforcement purposes’. It covers processing for the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties. Any other processing of personal data (including where processing relates to civil offences and penalties) comes under GDPR/DPA Part 2. Please refer to our main Data Protection Policy for more details.

**1.0 Is Allerdale Borough Council a competent authority?**

A ‘competent authority’, for the purposes of law enforcement, means a person specified in Schedule 7 of the DPA and any other person if, and to the extent that, the person has statutory functions to exercise public authority or public powers for the law enforcement purposes, or where the authority have a legal power to process personal data for law enforcement purposes. For example, the Council will be a competent authority when processing data relating to noise nuisance, planning enforcement and other environmental offences as it holds statutory powers to enforce criminal law.

**2.0 Key Definitions**

Underthe DPA/GDPR the following definitions apply:

**2.1 Personal data**

Personal data means “…*any information relating to an identified or identifiable living individual*”

This includes information such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

**2.2 Sensitive personal data**

*“…personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.”*

**2.3 Data Controller**

In Part 3 “controller” means *“…the competent authority which, alone or jointly with others—*

*(a) determines the purposes and means of the processing of personal data, or*

*(b) is the controller by virtue of subsection (2).*

*(2) Where personal data is processed only—*

*(a) for purposes for which it is required by an enactment to be processed, and*

*(b) by means by which it is required by an enactment to be processed,*

*the competent authority on which the obligation to process the data is imposed by the enactment (or, if different, one of the enactments) is the controller.”* s32 DPA

**2.4 Data Processor**

In this Part, “processor” means “…*any person who processes personal data on behalf of the controller (other than a person who is an employee of the controller).”* s32 DPA

**3.0 Principles**

* 1. **Overview**

The six law enforcement principles under Part 3, Chapter 2 of the DPA are the main responsibilities we follow when processing personal data for law enforcement purposes. The principles are broadly the same as those in the GDPR, and are compatible across the two regimes. However, there are no principles relating to individuals’ rights or overseas transfers of personal data (these are addressed in the DPA separately). Transparency requirements are not as strict, due to the potential to prejudice an ongoing investigation in certain circumstances.

**3.2 Data Protection Principles**

Part 3 of the DPA requires that:

* Processing be lawful and fair - s35(1)
* The purposes of processing be specified, explicit and legitimate – s36(1)
* Personal data be adequate, relevant and not excessive – s37
* Personal data be accurate and kept up to date – s38(1)
* Personal data be kept for no longer than is necessary – s39(1)
* Personal data be processed in a secure manner – s40

We must be able to demonstrate overall compliance with all of the law enforcement principles.

**4.0 Processing conditions (sensitive personal data)**

Processing of sensitive data for a law enforcement purpose will be lawful only if:

* explicit consent has been gained from the subject, or
* the processing is ‘strictly necessary’ for the law enforcement purpose and meets one of the further conditions from schedule 8 DPA.

‘Strictly necessary’ in this context means that the processing has to relate to a pressing social need, and we can’t reasonably achieve it through less intrusive means. Conditions for sensitive processing under Part 3 include:

**4.1 Statutory purposes**

Processing is necessary for:

* the exercise of a function conferred on a person by an enactment or rule of law, and
* reasons of substantial public interest.

**4.2 Administrations of justice**

Processing is necessary for the administration of justice

**4.3 Safeguarding of children and of individuals at risk**

**4.4 Personal data is already in the public domain**

The data subject has deliberately made the information public

**4.5 Legal claims**

Processing is necessary for:

* the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
* the purpose of obtaining legal advice; or
* the purposes of establishing, exercising or defending legal rights.

**4.6 Judicial acts**

Whenever a court is acting in its judicial capacity

**4.7 Preventing fraud**

NB. if it involves sharing data with organisations that do not fall within the definition of a competent authority, the processing needs to comply with the applied GDPR elements in the DPA, and we need to have lawful basis for sharing the data.

**4.8 Archiving**

Processing is necessary for archiving in the public interest, for scientific or historical research purposes or for statistical purposes. However, we can’t use it if it will result in decisions being made that affect a particular individual, or is likely to cause substantial damage or substantial distress to an individual.

**5.0 Rights of the Data Subject**

This section only applies to processing of personal information for a law enforcement purpose. Part 3 still imposes the following:

**5.1 General duties on the controller to make information available (s44)**

We must tell data subjects:

* who we are & our contact details (including contact details for the DPO where appropriate)
* the purpose for which we will process their data
* the existence of their rights
* the existence of their right to lodge a complaint with the ICO
* information about the legal basis for processing
* Retention periods
* Recipients of the personal data

**5.2 Right of access by the data subject (s45)**

This includes information about the data processing (including the legal basis for processing, the type of data held, to whom the data has been disclosed, the period for which it will be held and the right to make a complaint

**5.3 Right to rectification (s46 & s48)**

The Council must rectify inaccurate personal data or complete incomplete personal data relating to the data subject

**5.4 Right to erasure or restrict processing (s47 & s48)**

These rights exist where the processing of the data would infringe the data protection principles and we have a legal obligation to erase the data. NB: Where the Council has been asked by the data subject to erase personal data but it is required as evidence, the Council must restrict, rather than erase, its processing.

**5.5 Right not to be subject to automated decision-making (s49)**

i.e. decision making that has not involved human intervention

**6.0 Restrictions on Individuals’ Rights**

Part 3 places restrictions on the rights referred to in section 5.0, but only where necessary and proportionate in order to:

* Avoid obstructing an investigation or enquiry;
* Avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
* Protect public security;
* Protect national security; and
* Protect the rights and freedom of others

**7.0 Privacy by Design**

We will implement technical and organisational measures to show that we have considered and integrated data protection into our processing activities. When processing personal data for law enforcement purposed, we will implement these measures by default, to ensure that we only process personal data for a specified and necessary purpose.

As a minimum a Privacy Impact Assessment will contain:

* A general description of the processing operations and the purposes;
* As assessment of the risk to the rights and freedoms of individuals;
* The measures envisaged to address those risks;
* The safeguards, security measures and mechanisms in place to ensure we protect personal data; and
* A demonstration of how we are complying with Part 3 of the DPA, taking into account the rights and legitimate interests of the data subjects and any other people concerned.

For further information see the Council’s ‘Privacy Impact Assessment Procedure’.

**8.0 Data sharing**

Any sharing of personal data with external partners, for the purposes of service provision, must comply with all statutory requirements and corporate policies. Further details are available in the Council’s ‘Information Governance Policy’.

**9.0 Sources of information and guidance**

The Council will review and supplement this policy as more legislation is enacted into UK law and relevant guidance from the ICO is issued.

For more information on Law Enforcement (data protection) please contact the Councils Information Governance and Data Protection Officer:

Email – foi@allerdale.gov.uk

Phone – 01900 702898

Mail – Allerdale House, Workington, Cumbria, CA14 3YJ