



Allerdale Borough Council
Data Protection Act 1998
Policy and Guidance

Agreed: SMT April 2010

Data Protection Act 1998	3
Introduction:	3
Definitions:	3
Data Protection Principles:	5
Actions:	5
Guidelines on the gathering and processing of personal data	7
The Data Protection Principles	7
Principle One.....	7
Principle Two	8
Principle Three	9
Principle Four	9
Principle Five	10
Principle Six	10
Principle Seven	11
Principle Eight	11
Subject Access Requests	12
Further Information	13
Checklist	14
Appendix 2	15

Data Protection Act 1998 – Policy

Introduction:

The Council holds personal information on customers, staff, elected members and contractors among others. Everyone who represents the Council must protect this personal information and use it in accordance with the Data Protection Act.

Allerdale Borough Council is fully committed to compliance with the requirements of the Data Protection Act 1998 which came into force on 1 March 2000.

In order to operate effectively and comply with government legislation, Allerdale Borough Council needs to collect and use certain types of information about the people with whom it deals. The Council recognises that all personal information must be dealt with correctly. Under the Data Protection Act there is a duty to handle personal data properly and confidentially at all times, regardless of the format it is in. Allerdale Borough Council regards the lawful and correct treatment of personal information as vital to successful operation. The Council will ensure that it treats personal information properly.

Definitions:

Personal Data:

- Data relating to a living individual who can be identified from it, or from data combined with other information that is in the possession of, or is likely to come into the possession of the data controller. Personal data can include an expression of opinion about the individual, or is processed to learn, record, or inform something about an individual. The terms data and information have the same meaning and are interchangeable.

Sensitive Personal Data

- Data is considered to be sensitive personal data if it relates to racial or ethnic origin, political opinions, religious beliefs, membership in trade unions, physical or mental health, sexual life or criminal records.

Processing

- The obtaining, recording, using, sharing, or holding of information or data

Data Subject

- An individual who is the subject of the data.

Data Controller

- The organisation or individual who controls the contents and the use of personal data, in this case Allerdale Borough Council.

Subject Access Request

- Any person who believes that the Data Controller (Allerdale Borough Council) holds information about them can request to see this information, to learn the purpose for which it is held, and to have it corrected if they believe it to be inaccurate. This request is known as a Subject Access Request.

Information Commissioner (ICO)

- The independent supervisory authority over the Data Protection Act, and other legislation. This body has a duty to promote good data handling practices. The ICO can impose fines on those found to be in breach of the Act

Responsibilities:

Chief Executive: The Chief Executive will have overall responsibility for ensuring compliance with the Data Protection Act. They will be provided with details of all proposals to introduce new information systems, or to change existing ones. This will allow implications for personal data to be assessed and approved before implementation.

Human Resources: The HR department will ensure that all job descriptions and contracts for staff, whether permanent, temporary, agency or contractual, include clauses which relate to obligations of staff under the DPA. Clauses will also stipulate sanctions imposed in the event of misuse of personal data whilst in the employment of Allerdale Borough Council. All staff will undergo checks to assess their reliability in the workplace. HR will also oversee the induction training for new staff and undertake ongoing reviews of training requirements.

Service Area Managers: Service Managers are responsible for issues relating to Data Protection within their areas. This includes ensuring accuracy of data held in the department, for the disposal in an appropriate manner of confidential information when it is no longer needed and that contracts with other organisations contain adequate safeguards regarding access to personal data by those organisations. The eight data protection principles must be followed in all areas of Council business including fair processing, when collecting data and ensuring records are accurate, up to date and not excessive.

Information and Records Officer: The Information and Records Officer has day to day responsibility for data protection matters within the Council. This includes keeping the Notification up to date with the Information Commissioner's Office and producing procedures and advice as needed within the Council. Service managers should inform

the IRO of any changes to their services and/or the new processing of personal information.

All Staff: Everyone managing and handling personal information are responsible for following good data protection practices and the Council's procedures. All staff are obliged to complete the data protection e-training course available on the Intranet and further training provided by the Council. Employees are advised that wilful non-compliance with the data protection principles will be regarded as a disciplinary matter. Also employees are advised that breaches of the Data Protection Act can lead to prosecutions being brought by the Information Commissioner against them.

Data Protection Principles:

The DPA sets out eight principles that all organisations that hold personal information, including Allerdale Borough Council must adhere to. There is further explanation in the Guidance section of each of these as well as practical advice on what they mean to service areas within Allerdale. There is also a checklist in the Appendices that may be useful when evaluating how personal information in a particular area is kept. The eight principles state that personal data shall be:

- Processed fairly and lawfully
- Processed for specific purposes
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Not kept for longer than is necessary
- Processed in accordance with the rights of data subjects under this Act
- Kept secure
- Not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of data protection

Actions:

Through appropriate management and controls, Allerdale Borough Council will take action to make sure that the eight Data Protection principles are followed. We will:

- Only use personal information for lawful purposes
- Only use personal information for reasons which are not incompatible with why it was collected
- Be transparent with individuals about why we require their personal information and what it is used for
- Not ask for more information than we need, or that is relevant, but make sure that we have enough to carry out our duties
- Ensure the quality and accuracy of the information we hold
- Apply checks to determine the length of time information is held

- Ensure that the rights of people about whom the information is held are able to be fully exercised under the act, including giving access to the information held on them when requested
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred abroad without suitable safeguards and not beyond the EEA

More specific actions are listed in the Guidance section of this document.

Procedures

Allerdale Borough Council will apply the spirit of the Data Protection Act to the handling of all data. This includes non-personal data as this too could contain information sensitive for other reasons.

Data held by the Council is normally held solely for the use of the Council, where it may be shared between departments where legal to do so. The only exceptions to this rule are cases where data are intentionally stored for sharing with other agencies or where other agencies are working on behalf of the Council. In addition, when personal information is shared, there must be assurance from the third party involved that all information will be handled in accordance with the Data Protection Act. Conversely, when Allerdale Borough Council receives personal information from outside sources, we must get assurance that the information was obtained fairly and lawfully.

There will be someone with specific responsibility for day to day compliance with the Data Protection Act in the organisation. At this time it is the Information and Records Officer.

Methods of handling personal information will be clearly described and regularly assessed and evaluated. This policy will be built upon with further guidance and new procedures as the systems we have that hold personal information change. Everyone managing and handling personal information will be appropriately trained in these methods, and will be supervised as appropriate.

Deliberate unauthorised access, copying, alteration, deletion and interference with data held by the Council is prohibited. Wilful non-compliance with the Data Protection Act is a disciplinary matter.

Any breach of the Data Protection Act and/or loss, or potential loss, of personal data will need to be notified via the notification procedure as outlined in the relevant procedures and policies.

Procedures must be established for authenticating the identity of a person to whom data may be disclosed over the telephone. These will ensure that authentication takes place prior to the disclosure of the data.

Where contractual arrangements involves the sharing of personal information, the contract will include measures to ensure this is done safely and securely, and that information is disclosed and used for agreed purposes.

Guidelines on the Gathering and Processing of Personal Data

The Data Protection Principles

Principle One

Personal data should be processed fairly and lawfully and shall not be processed unless

- 1. at least one of the conditions in schedule 2 is met or**
- 2. in the case of sensitive personal data at least one of the conditions in Schedule 3 is also met.**

Explanation of Principal One:

The Data Protection Act has two schedules (Schedule 2 and Schedule 3) that set out preconditions for processing personal data. In addition, there is a requirement that all personal data should be processed fairly and lawfully at all times.

Schedule 2 provides a list of conditions, one of which must be met before personal data can be processed. These are:

- Consent of the Data Subject
- Necessary for the performance of a contract with the Data Subject
- Legal Obligation
- Necessary to protect the vital interests of the data subject
- Necessary to carry out public functions
- To pursue legitimate interests of the controller unless prejudicial to the interests of the data subject.

In the case of sensitive personal data, there are extra rules, one of which must be met in addition to meeting one in Schedule 2. See the Definitions section for more information on sensitive personal data. Schedule 3 conditions are:

- Explicit consent of the data subject
- To comply with the employers legal duty
- To protect the vital interests of the data subject or another person
- Carried out by certain non-profit bodies in the course of legislative bodies
- The information has been made public by the data subject
- In legal proceedings

- Exercising legal rights
- To carry out public functions
- For medical purposes
- For equal opportunity monitoring
- As specified by order

All Personal Data must be gathered and handled in such a way that it does not contravene the Act. This means that individuals must be told of the uses for the information they supply in accordance with the fair processing guidance. When this is obvious, for instance a name and address for correspondence, consent does not need to be specifically gained unless the data is sensitive. When in doubt it is best to inform the Data Subject of the reasons why personal details are being collected. Compliance with these principles will ensure fairness in processing of personal data.

Forms and Contracts: All forms used to obtain Personal Data, such as registration forms and contracts should state the purpose for which the information is being obtained and who the information will be shared with at the very least. More information on fair processing or privacy notices can be found in the procedural guidance.

External Agencies: Where Personal Data is obtained from an external organisation such as a private sector partner, there must be confirmation in writing (including email) that the data was obtained fairly and lawfully, according to the Data Protection Act principles.

Personal data obtained from subcontractors or volunteers: Where personal data (for example, CVs) are obtained for the purpose of placing a contract to which the data subject is party, this processing is considered to be fair, as the person providing the information will know the purpose already.

There are some exemptions on the non-disclosure provisions. These are Section 28, National Security; Section 29, Crime and Taxation; and Section 35 where disclosure is required by law or in connection with legal proceedings. Disclosures made under these sections can only be made to enquirers who can satisfy the council that the conditions held in these sections have been met. These will usually be police officers and taxation officials. However, it is the obligation of the enquirer to provide the relevant and satisfactory evidence before disclosure can be contemplated.

Principle Two

Personal data shall be obtained only for one or more specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose or those purposes

Explanation of Principle Two:

When we collect personal information we must tell the individuals we are collecting it from, the reason why it is being collected and who it may be shared with. We are then only allowed to use it for that specific reason. If later

we decide that the information would be useful in another way, fulfilling a different purpose which is incompatible with the original purpose, we must inform the data subject how we intend to use the data differently, and give individuals the chance to opt out.

Any new collection of data must have a legal basis and must be done in accordance with the Data Protection Act. A Privacy Impact Assessment may be necessary to help with planning the data collection process.

In addition, on a yearly basis, we must notify the Information Commissioner's office, the body which oversees the Act, of the purposes for which we hold information. Therefore, any changes in the purpose that personal data is kept or used, or any new data collection exercises, must be communicated to the Information and Records Officer in order that it can be included in our yearly notification to the Information Commissioner. The responsibility for keeping the registration up to date lies with the Information and Records Officer.

Principle Three

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

Explanation of Principle Three

When collecting personal data, Allerdale Borough Council must make certain that the right amount of Personal Data is collected, no more. We must only collect the minimum amount of information necessary to fill the purpose for which it was collected.

Therefore at Allerdale, we must only ask for personal information that is strictly necessary and adequate for the purpose it is to be used for. For example if you ask for a home address on a form, you must have a good reason for needing the information. But if you have no plans or reasons to contact that person at home, then you may not actually need the person's home address. Information can not be collected just in case it may be useful in the future. Any forms that are used should be regularly reviewed and updated if necessary to guarantee that the information collected is the minimum necessary.

Sensitive personal data can only be collected when absolutely necessary. It should not ever be part of a generally accessible record, such as a personnel file. If presented publicly, it should always be done in a de-personalised form and ideally stored without any link to the individual providing it.

Principle Four

Personal data shall be accurate and, where necessary, kept up to date.

Explanation of Principle Four

Allerdale Borough Council has a duty to take reasonable steps to make sure that the personal information we hold is accurate and up to date.

The Data Protection Act does allow individuals who are caused 'damage or distress' by the fact that we hold inaccurate personal data to appeal to the Information Commissioner. This could lead to fines or even in extreme cases the prosecution of individual officers. It is very difficult to guarantee that all of the personal information we hold is up to date, but services should endeavour to do as much as possible towards this and ensure compliance with the Data Quality Strategy. Therefore before significant decisions are made based on personal information, efforts must be made to ensure the accuracy of personal information. Inaccurate information should be destroyed.

Principle Five

Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose

Explanation of Principle Five

Information about an individual should be kept only as long as it is really necessary to the Council. After this it should be destroyed in a secure environment.

Disorganisation and lack of time to clear out old documents, or the thought that the information might be useful in the future, is not an excuse for holding personal data longer than is necessary. When implemented, retention times set out in the Allerdale Retention Schedule should be adhered to. In the meantime, guidance is available from the Information and Records Officer.

Principle Six

Personal data shall be processed in accordance with the rights of data subjects under the Act

Explanation of Principle Six

Under this principle, we must ensure that the rights of the people about whom information is held are able to be fully exercised. The rights that Data Subjects have under DPA are as follows:

- The right to be informed that processing is being undertaken
- The right of access to one's own personal information
- The right to prevent processing in certain circumstances, including if it is likely to cause damage or distress
- The right to seek compensation
- The right to have information which is regarded as wrong rectified, blocked or erased

In respect to the above rights of the Data Subjects, customers can be informed about their rights under the Act, and the right to make a Subject Access Request (subject to certain exemptions) in order that they may access their information either through our website or an information leaflet. When such requests are received the Information and Records Officer should be informed immediately, in order that we have the maximum amount of time to deal with the request (all requests must be answered within 40 days), and it can be forwarded to any other relevant service areas. It is imperative that the

identity and entitlement of the enquirer is checked before any information is disclosed.

In addition, if individuals or other organisations inform us that information we hold is incorrect, then we must change or erase it to keep our records up to date.

Complaints made to the Council with regard to Data Protection will be handled in accordance with our formal complaints policy.

Principle Seven

Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Explanation of Principle Seven

At Allerdale, we are the guardians of Data Subjects' Personal Data. Therefore we have a responsibility to put in place adequate precautions to avoid unauthorised access, changes to data, loss and damage.

Only members of staff who need access to files containing personal information will be allowed to view them with security levels dependent on the level of confidentiality of the information. All staff have a responsibility in protecting the data processed by the Council. In order to ensure that personal data is kept secure, security measures such as locking cabinets that hold personal information should be taken when offices are closed. Individuals' personal data should not be left on unattended desks and not downloaded onto mobile devices and local drives of computers. More advice and rules on the physical and technical security arrangements are outlined in the Information Security policy.

In situations where personal data is held by an external agency on behalf of Allerdale Borough Council, a guarantee should be obtained to ensure that the security measures in place are suitable, and included in any contractual arrangements.

Principle Eight

Personal data shall not be transferred to a territory or country outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Explanation of Principle Eight

When moving personal data, it is necessary to be cautious. The Data Protection Act states that information should not be moved out of the European Economic Area (EEA) (this includes all of the countries in the European Community as well as Iceland, Norway and Lichtenstein) unless certain safeguards have been put in place. While this is not an issue for

Allerdale most of the time, it should be remembered that information on the internet can be accessed by anyone in the world

If there is a situation where personal information is being transferred outside of the countries listed above, the Information and Records Officer should be consulted to make certain that checks are made regarding the security arrangements during the transfer and by the recipient

Subject Access Requests

If someone contacts the Council with a query about the personal information we hold about them, there are several steps that should be followed by Allerdale staff. They are as follows:

- When a customer asks to see information held on them, ask them to put the request in writing. There is a Subject Access Form both on the Intranet, and as an appendix to this guidance. Written enquiries should be addressed to the Information and Records Officer. Proof of identity must be provided before any personal information is released. There is also a £10 charge.
- When the actual request is received make sure a copy or the original is forwarded to the Information and Records Officer. That way they can make sure that it can be given to other areas if they need to be involved. All enquiries must be completed in 40 days, so it is imperative that these requests are forwarded promptly.
- If someone requests information on a third party, even if they are related, the information must not be given out unless the third party has given permission. If this is the case, we will require written permission from the third party as well as proof of identity from both parties. If permission has not been granted to share the information then the information must not be released.
- Individuals have the right to see all their personal information as defined by the Act, as well as explanations of any acronyms or terminology which isn't clear. They are also entitled to know who the information is shared with. Moreover, if they ask for it individuals should be given an explanation of any automated decisions made from the information held.
- There are certain exemptions to the right to information which include: information related to crime prevention and detection, confidential references made by the Data Controller, information related to management forecasts and management planning, information that relates to negotiations with the Data Controller, corporate finance information, legal professional privilege and self-incrimination
- All Subject Access Requests have to be signed off by at least a service manager before any information is disclosed

Further Information:

To make any further queries or for more information on the Data Protection Act, including exemptions that apply to various aspects of it, please contact Allerdale Borough Council's Information and Records Officer at: Allerdale Borough Council, Allerdale House, Workington, Cumbria, CA14 3YJ.

Policy Review

This policy will be reviewed on an annual basis and any changes made.

Other Policies

Other related documents and policies include:

- CCTV Policy
- Records Management Policy (draft)
- Data Protection Act procedural document
- Data Quality Strategy
- Freedom of Information Act policy and procedures
- Retention Schedule (draft)
- Information Sharing Protocols (draft)

Appendix I

Checklist

When dealing with personal data, it might be helpful to consider the following checklist:

Was the data obtained with the subject's consent? If the answer is no, then obtain consent in writing	
When the information was collected was it made clear what the data would be used for? If the answer is no then the data subject must be informed before the information can be used.	
Are you thinking of using the information for a different reason from which it was collected? If so, you must gain the permission of the individual involved.	
Is all of the personal information we are collecting absolutely necessary? If the answer is no then make sure that non-essential information is no longer collected, or destroyed.	
Is the personal information you hold kept up to date? If not, make sure that it is kept as accurate as possible.	
Do you dispose of personal information as soon as it is no longer needed? If not, measures need to be put in place to ensure that this type of information is disposed of as soon as is possible.	
If an individual made a request to see the information we hold on them, would you be able to provide that within 40 days? If not, the information in your service area needs to be kept in a more organised fashion.	
Is all personal information you hold kept secure? Is it only possible for staff members who need to see personal data to access it? If not, then further security measures should be put in place to make sure that personal data is protected.	
Does your service area send any personal information outside of the European Union, or publish it on the Internet? If so, security arrangements must be put in place to ensure the information is kept secure.	

Allerdale Borough Council must comply with the Data Protection Act. If you believe that your service is not in compliance with the Act, please contact the Information Officer so we can make sure that all of our practices get in line with current legislation. If the checklist raises any questions, please contact the Information Officer.

Appendix 2



Allerdale Borough Council

Data Subject Access Application Form

Under the terms of the Data Protection Act 1998, an individual is entitled to ask the authority for a copy of any personal information which it holds about him/her for the purposes of providing services to the individual. The additional information which the individual is entitled to receive from the authority includes a description of the purposes for which it is held, recipients to whom the data are disclosed and sources of the data. This entitlement is known as the "Right of Access to Personal Data". If you would like to access the personal data which the authority holds about you please answer the following questions:

A: Personal Details

Name	
Current Address	
Telephone Number	
Date of Birth	
No of Years at This Address	

B: Information Required

The authority uses personal data for many different purposes. Please tick the box if you would like to access personal data held about you in that area. For all information please tick the box marked all. If you believe that we hold information about you in another service please list in boxed marked 'Other.'

Council Tax Collection	
Planning	
Human Resources	
Environmental Health	
Leisure Services	

Benefits	
Other (please name)	

Please give any further details that would help us locate the information desired, including past addresses

C: Completing this form on behalf of someone else

This section should be completed ONLY if acting on behalf of the data subject.

I confirm that I am acting on behalf of the data subject and have submitted proof of my authority to do so.

Name	
Address	
Telephone Number	
Signature	
Date	

D: Declaration to be completed by all applicants

Please note that any attempts to mislead may result in prosecution.

I, certify that the information given on this Subject Access Request Form to Allerdale Borough Council is true. I understand that it is necessary for Allerdale Borough Council to confirm my/the Data Subject's identity and it may be necessary to obtain more detailed information in order to locate the correct data. The information given on this form may be passed to the relevant departments, in order to locate the data, but it will not be used for any other purpose.

Please note that there are certain exemptions to what can be released under the Act and Allerdale Borough Council has the right under the Data Protection Act to refuse requests for access when an exemption applies.

Where the data requested refers to a third party, the third party information may be removed.

Signature

Date

Please return this form to:

Information and Records Officer, Allerdale Borough Council, Allerdale House,
Workington, Cumbria, CA14 3YJ

Documents that must accompany this application:

1. Proof of identity of the Data Subject.
2. If acting on behalf of the Data Subject, proof of permission and proof of identity are required.