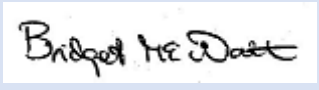
The Meadows

Data Protection Policy

Approved by:	IEB	**Date:** 5.11.2024	
Signed by:			(Chair)
Last reviewed on:	Autumn 2024		
Next review due by:	Autumn 2025		

Contents **Page**

1. Introduction

The Data Protection Policy sets out the Council's approach to handling personal information in all activities and decisions of Durham County Council (hereinafter referred to as 'the Council') in accordance with the Data Protection Act 2018. The Data Protection Act 2018 (DPA) is one of several pieces of legislation that deal with individual rights and information policy. The Human Rights Act 1998 (HRA) and the Freedom of Information Act 2000 (FOIA) are two other statutes that are closely related. An indicative list of related legislation that needs to be considered when handling personal information can be found in **Appendix A.**

The Data Protection Act 2018 seeks to balance the rights of individuals and the sometimes-competing interests of those with legitimate reasons for using the personal information, like the Council. Its aim is to prevent organisations (such as the Council) from holding and using inaccurate information about individuals. This applies to information regarding both the individuals private lives and their business lives. Its purpose is to give the public confidence about how organisations can use their personal information.

The DPA sets out a number of standards and rules and places obligations on those who process information (like the Council) while giving rights to those who are the subject of the data (data subjects). As personal information covers both facts and opinions about the individuals, the rules and procedures cover the collection and use of information, the quality and security of the information and the rights of individuals regarding the information about themselves. As the Act and the guidance contains specific terms that have a particular meaning, a glossary of the terms within the DPA is located in **Appendix F.**

The policy sets out a framework for understanding the requirements under the legislation. At the same time, it provides an overview of the main obligations for officers and Members in dealing with personal information so they can comply with the Act and the 8 data protection principles. For more detailed advice and guidance, the Information Management Team (IMT) is available.

2. Statement of policy

The Council collects and uses information about people with whom it works to operate and carry out its functions. In some cases, the Council is required by law to collect and use information to comply with central government requirements.

Durham County Council is committed through its policy, procedures and guidelines to ensure that it will:

- comply with both the law and good practice
- respect individuals' rights
- be open and honest with individuals whose data is held
- provide training and support for staff who handle personal data, so that they can act confidently and consistently

At the heart of the Act is the need to protect personal information otherwise known as personal data (Seen Annex F for the definition) and sensitive personal data.
What this means is when the Council collects and uses personal information, it must be sure to handle it and deal with it according to the 8 enforceable principles of good information handling practice.

3. The Six Principles of Data Protection

If the Council or the individual follows these six principles, they will be acting in accordance with the Act. The principles set the framework for the legitimate reasons for which an organisation may process or use personal information. These Principles are legally enforceable which means that if you have not processed personal information in accordance with them, you and the Council can be considered in breach of the Data Protection Act.

The six principles, which form the basis of the Act, state that data must be:

1. **Fairly, transparent and lawfully processed**
Nobody should be deceived or misled about the purpose for which their data is to be processed.

2. **Processed for limited purposes**
Personal data can only be obtained for specified and lawful purposes with permission from the data subject for each purpose.

3. **Adequate, relevant and not excessive/ data minimisation**
The data must be sufficient to meet their purpose but not provide more information than the purpose requires or provide information outside the scope of the purpose.

4. **Accurate**
The personal data must be accurate when recorded, and accuracy must be maintained throughout the life cycle of the data.

5. **Not kept for longer than is necessary/ storage limitation.**
Personal data must not be kept for any longer than is necessary for the purpose for which it was obtained. If data are kept for too long, the accuracy and relevance may be compromised.

6. **Stored and processed securely**
All necessary measures must be taken to prevent unauthorised or unlawful processing of personal data and to protect personal data against loss, damage or destruction.

Addition to these principles data must not be transferred to countries without adequate protection (Chapter 5 DPA) - Personal data must not be transferred to a country outside the UK unless that country has in place a level of data protection comparable to that in the UK. Advice should be sought from the Information Management Team.

The Council must also respect the specific data protection rights for all individuals, **(see Annex H)** this includes staff as well as the public. Each of these rights creates responsibilities for the Council that are met by adhering to the six data protection principles as well as the provisions of this policy.

4. Scope

The policy applies equally to full time and part time employees on a substantive or fixed-term contract and to associated individuals who work for the Council including agency staff, contractors and others employed under a contract of service. The policy also applies to individuals in their role as a Member of the Council.

The policy covers all personal information that the Council holds in either electronic or paper format or file system. The policy applies throughout the life cycle of the information from the time it is created or arrives within the Council to the time it is either destroyed or preserved permanently within the County Durham Record Office.

The Policy fits within an information governance policy framework (**Appendix E).** The framework lists the procedures, and guidelines that will support the data protection policy. Many are already in place, and some are being developed. The most up-to-date versions of these policies will be available on the Intranet.

5. Roles and Responsibilities

Members
All elected members are to be made fully aware of this policy and of their duties and responsibilities under the Act.

When Members handle personal information in their role as politicians or in their role as elected members, they are covered by their party or the Council's notification. As such, they have to handle personal information in line with the requirements of the eight data protection principles.

If Members use (process) personal information in their constituency work, they will have to notify with the Information Commissioner's Office as a separate data processor.

Corporate Management Team (CMT)
The Corporate Management Team has overall responsibility for ensuring that the Council, as a data controller under the Data Protection Act, and its staff complies with the Council's legal obligations regarding the handling of personal information.

In discharging this duty, CMT will approve the corporate framework for data protection within the Council as set out in this policy to protect personal information/

By demonstrating the Council's commitment to accountability and promoting good governance, CMT have the lead role in developing a data protection culture within the Council.

Information Governance Group

- Will advise services and departments on developing service specific procedures and applying the Data Protection Policy;
- Will ensure that staff have access to support in terms of training and development in adhering to the Data Protection Policy and procedures;
- Will review and update the Data Protection Policy and procedures when changes occur.

Heads of Service (HOS)
Heads of Service have responsibility for seeing that their service complies with the principles of the data protection act when processing personal data. Their responsibility includes ensuring that their staff are aware of their responsibilities under the Data Protection Act and trained to discharge those responsibilities. They will ensure that good Data Protection practice is established and followed by:

- Ensuring that appropriate staff are appointed as Data Protection Champions as they are required to assist with subject access requests (see **Appendix B**).
- Ensure employees, including contractors, consultants and volunteers employed to undertake Council business follow the data protection policy and procedures. This will include developing verification procedures for monitoring compliance with procedures.
- Ensure appropriate resources are in place to enable compliance with the data protection policy.

The Information Management Team
The Information Management Team are responsible for:

- Briefing senior managers on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising staff on Data Protection issues such as data protection statements on any forms collecting personal information
- Notification with the Information Commissioner's Office
- Handling subject access requests
- Approving, in consultation with the Monitoring Officer, unusual or controversial disclosures of personal data

Specific other staff:
Information Security Manager
The Information Security Manager has responsibility, in conjunction with the Head of ICT, for the security of electronic systems and electronic information.

Corporate Procurement Manager
The Council has a standard clause in Council contracts, which requires the other party to comply with the requirements of the Data Protection Act. If the contract you are considering involves specific personal information handling requirements, please alert the Corporate Procurement Manager so that specific contractual language can be prepared as needed.

Caldicott Guardians
A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Guardian plays a key role in ensuring that the Council and partner organisations satisfy the highest practical standards for handling patient identifiable information.

Acting as the 'conscience' of an organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information. Their remit covers all social care records for children and adults.

As they have responsibilities relating to confidential information and information sharing, the Caldicott Guardians also have a strategic role, which involves representing and championing Information Governance requirements and issues at management team level and, where appropriate, at a range of levels within the organisation's overall governance framework.

The Caldicott Guardian makes sure that where confidential personal information is shared, for example with local NHS or other care partners, this is done properly, legally and ethically in line with the following principles.

The Caldicott Guardians in Durham County Council are:

Jane Robinson
Head of Service - Policy, Planning and Performance
Adult Wellbeing and Health
0191 383 3628

Martin Stenton
Head of Access and Inclusion Services
Children and Young People's Services
0191 383 6481

6. Development of Service and Corporate Procedures

From this policy, additional procedures and guidance notes will be developed. Each service will want to consider what specific guidance it may need to have in place to meet the data protection principles. The following five areas cover the main areas for officers in their day-to-day work when dealing with personal information under the Data Protection Act. Please be aware that there will technical areas within the DPA that are not relevant to the day-to-day work. If an issue, not covered in this document, arises please contact the Information Management Team for advice and assistance. The following procedures address the main issues that will arise for staff in dealing with personal information under the Act:

1. How we use personal information
2. How we store it
3. How we keep it secure
4. How we respond to subject access requests, and
5. How we share it

The five areas cover the most likely ways in which staff will have responsibility for processing (using) personal data.

6.1 How to process or use personal data

The definition of processing (using) data is very broad in the Data Protection Act. If the Council obtains, holds, files, organises, transmits, retrieves, disseminates, discloses or destroys data, it has processed data. When officers and Members want to use personal information, they have to make sure that it is done fairly and lawfully (Principle 1).

The main requirements for processing (using) personal information is that the process meets the conditions for the processing (use) of personal information or sensitive personal information are set out in **Appendix G**. In practical terms, this means the Council needs to be clear when it collects personal or sensitive personal information what it will do with the information and whether the use is in line with the conditions. at they have the permission of the person providing the information.

The Council's paper or electronic forms, such as application forms or registration forms, should seek the applicant's consent, where possible, to use the information as well as:

- State the purpose or purposes for which the information is required
- Be reviewed regularly to check that all of the information asked for is still required and necessary.
- Be checked for the accuracy of the data before they are used for any processing. If in doubt about the accuracy of the data they should be referred back to the data subject for confirmation

In addition to understanding these points regarding the processing of personal information, some additional steps to do and some to avoid are the following:

Do:

- Think of personal data held about individuals as though it were held about you;
- Get permission from the data subject to hold their personal data unless consent is obviously implied;
- Be particularly careful about sensitive data: concerning race, political opinion, religious belief, trade union membership, physical or mental health, sexual life, criminal offences;
- Hold personal data about people only when necessary;
- Ensure personal data is kept accurate and up to date;
- Tell people you hold personal data about them and tell them why you need to do so (fair processing);
- Be very careful about passing personal data to third parties;
- Respect confidentiality and the rights of the data subject (the person whose information you hold);

- Review personal data kept in files from time to time and at least annually;
- When writing documents, bear in mind that the data subject (any person who is mentioned in the document) has a right to see information relating to them;
- Realise emails may be retrieved and revealed to those about whom they are written;
- Direct any official requests to see personal data to the Information Management Team at **dataprotection@durham.gov.uk**

Avoid:

- Worrying about the complexities of the Act - the Data Protection Act principles are simple
- Revealing personal data to third parties without the data subject's permission or justification
- Disclosing any personal data over the telephone unless the person has been identified appropriately
- Holding sensitive data about a person without their explicit consent or seeking advice from the Information Management Team (for example CRB forms)
- Leaving personal data insecure in any way, whether it is physical files or information held electronically; (keep a clean desk) ▪ Taking personal data home that is unencrypted.
- Use personal data held for one purpose for a different purpose without permission from the data subject

6.2 How to hold personal information (records management)

The Data Protection Act puts a responsibility on organisations to maintain a focus on keeping personal information accurate and up to date. The Council's corporate records management policy provides guidance on how the Council manages its records and sets out the retention guidelines so that information is up to date and not held longer than needed by the Council.

As part of the Corporate Records Management Policy, Heads of Service have a responsibility to review their service procedures for ensuring that they maintain accurate and consistent records. In doing so, they will take the necessary steps to ensure that any personal data they hold or process as part of their service will be accurate and stored securely and appropriately in line with the Act. The following are some of the actions that may be required to make sure data is stored accurately and is up to date.

Updating

Each service, as part of their responsibilities under the Corporate Records Management Policy will have created a process for regularly checking, updating or discarding old data.

Storage
In most instances, keeping personal information under lock and key is sufficient to meet the requirements of the Data Protection Act. However, in some instances, extra security measures must be followed. For example, sensitive personal data will require a higher level of security and authorisation in line with the seventh data protection principle.

Retention periods
Different records will have different retention periods. To comply with the fifth data protection principle the Council has to make sure that it has clear retention periods for the various types of personal information it holds. The retention period for different types of records may vary. For example, adoption records have to be held for 100 years. For more information on retention guidelines please see the Corporate Records Management Policy.
https://www.durham.gov.uk/media/1628/Corporate-Records-Management-Policy/pdf/CorporateRecordsManagementPolicy.pdf?m=637164113527600000

If personal information is to be disposed, it must be disposed securely and confidentially. The Council has a contract with a secure shredding service. Each Head of Service will want to make sure they have appropriate secure shredding facilities set up within their service to handle the disposal of any personal or sensitive personal information.

Archiving
In some cases, the personal information the Council holds may have a permanent retention period. In these instances, the County Durham Record Office will retain the material. The procedures for determining whether the record is to be retained permanently are found within the Corporate Records Management Policy.
If you have any questions about transferring records to the County Durham Record Office, you can contact them at the following:

Durham County Record Office
County Hall
Durham
DH1 5UL
03000 267619, record.office@durham.gov.uk.

6.3 How to keep personal information secure

Security is more than a Data Protection issue because it covers the wider security of all Council facilities. There are direct linkages with the information security policy within ICT as it relates to all Council facilities and systems.

The Council is required to take all reasonable measures to ensure the personal information is held securely (Principle 6). To meet the principle, security in some instances may involve encrypted and password protected devices or files. In other instances, it may

require paper files to be kept in locked cabinets. As a basic rule of thumb, personal information should not be left on an unattended desk or overnight.

When Members, employees and others acting on behalf of the Council access or use personal data, they must only have access or use personal data that are necessary to carry out their duties and responsibilities.

Further procedures on keeping personal information secure will be provided on the intranet and staff are reminded to check the ICT information security policy for further information relating to wider information security questions.

Confidentiality
Confidentiality applies to a much wider range of information than Data Protection. There are **three** elements to be considered for something to be confidential.:

- First, the information itself must have the necessary quality of confidence
- Second, that information must have been imparted in circumstances that oblige confidence
- Third, disclosure must harm the party communicating it

Some of the things that are likely to be confidential, but may well not be subject to Data Protection, include:

- Information about the organisation (and its plans or finances, for example)
- Information about other organisations, since Data Protection only applies to information about individuals
- Information which is not recorded, either on paper or electronically

6.3a What to do about a data breach? If we lose personal information or it is stolen

On occasion, personal data may be lost, stolen, or compromised. When this happens, it is important to notify the designated officers as set out in the Data Breach Procedures document **(Appendix I)** as well as find out what data has been lost, mitigate the loss, contact the people whose data was lost, and, if serious notify the Information Commissioner's office.

A data breach is any incident involving the loss of personal information that could lead to identity fraud or have other significant impact on individuals should be considered as serious. The data breach includes both electronic media and paper records it can also mean inappropriate access to information.

A data breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored

- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

As a general approach, when a breach occurs, the following four steps are to be followed. The full data breach response procedure is available separately to this summary in (**Appendix I**).

Initial reporting

The first person to inform, upon discovering a data breach, is your line manager. They will then contact the Caldicott Guardian or the Information Management Team (IMT) depending on the issues. You will then want to report it to databreach@durham.gov.uk**.** In deciding whom to contact, it might be helpful to ask the following questions:

- What data is involved?
- Who are the individuals affected?
- How sensitive is it?

At the reporting stage, it is important to consider the possible consequences for individuals. Are these serious or substantial and how likely they are to happen? For example, is it someone's full care file or is it someone's leisure centre membership registration card? The data can be sensitive because of what might happen if it is misused (bank account details)

- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate

Finally, at the reporting stage, it will be important to consider whether the information can be recovered if it has been lost or stolen, or contained in any way, if the information has been disclosed in some way.

Managing the incident

Once a breach has been reported to databreach@durham.gov.uk, a reference number will be issued by the IMT so that it can be tracked and managed. The Caldicott Guardian will consult with the IMT and, if needed, the Information Security Manager, to determine the lead investigating officer for the breach. The service involved will need to ensure the investigating officer has the appropriate resources. Further guidance is available in the

data breach procedure document. In brief the following are some of the actions required in Managing the incident:

- Establish what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes for a door.
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Where appropriate, inform the police

Investigating

Once an investigating officer has been appointed, they will need to consider whether appropriate specialist help (IMT, ICT, Security, Records Management) is required.

The Investigating Officer will need to document the details of the investigation by following the Data Breach Procedure which will contain the forms and the investigation checklist.

A data breach investigation needs to answer four interrelated questions.

- What caused or allowed the breach to occur?.
- Do the people affected by the breach need to be informed?
- Does the ICO need to be notified?
- What are the lessons to be learned to avoid a similar breach in the future?

Final Evaluation and response

The investigation report (a narrative summary as well as the completed form and checklist) will contain recommendations on notifying the ICO as well as lessons learned. The document will need to be circulated to the Head of Service affected, as well as the Caldicott Guardians and the HOS for Policy and Planning.

The investigating manager will have a time-scale for completing investigation and finalising reports. For the final evaluation and response, they will prepare a report in line with the report template and the report will be evaluated by the relevant persons or appraisal group. A key part of the response will be to identify who is responsible for disseminating the lessons learnt as described in the report.

Once the final evaluation has been submitted, following the review by the relevant senior officers, the incident will be closed on the data breach log.

6.4 What to do if someone requests their personal information (Subject Access Request)

Responsibility

One of the main data protection rights is for an individual to be able to obtain a copy of any of their personal information held by an organisation. When someone requests his or her own information, this is called a Subject Access Request (SAR). The Council has to provide the information within 40 calendar days. Although there are some exceptions to this right, it is rare that these exceptions are used.

When a request is made formally to the Council for personal information it is usually done through the online form on the Data Protection Access page or within one of the service specific requests for access to care records. Both the Children and Young Peoples' Service and Adults, Wellbeing and Health have specific processes by which people in care may request their personal information. However, a person may request their personal information in the course of business as usual requests so officers need to be alert to these types of requests.

The checklist in **Appendix C** will help you identify a request for personal information and help you to respond appropriately. If you are in doubt, please contact the Information Management Team who can advise you on the appropriate response.

Each service grouping will need a data protection champion to handle requests for personal information to that service. A statutory fee of £10 is required before a formal Subject Access Request can be processed. In some exceptional circumstances, this fee may be waived or refunded, for example in cases of financial hardship. However, this will depend on circumstances that need to be reviewed on a case by case basis.

6.5 What to do if you want to share personal information with a partner organisation

Information sharing is key to the Council's ability to deliver better, more efficient public services that are coordinated around the needs of the individual. It is essential to enable early intervention and preventative work and in some cases for safeguarding and promoting welfare and for wider public protection. Information sharing is a vital element in improving outcomes for all.

At the same time, the Council is aware that the public want to be confident that their personal information is kept safe and secure. Council officers have to maintain a balance between the privacy of the individual, whilst sharing information to deliver better services.

For those who have to make decisions about information sharing on a case-by-case basis, the following checklist gives an introduction to sharing under the data protection. The corporate information sharing protocol, which is referenced in Appendix D, is available as a separate procedural document.

1. **Remember that the Data Protection Act is not a barrier to sharing information.** It provides a framework to ensure that personal information about living persons is shared appropriately.

2. **Be open and honest.** Let the person (and/or their family where appropriate) from the outset know about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. **Seek advice**. If you are in any doubt, seek advice about the data sharing. Contact the Information Management Team if you have any questions, without disclosing the identity of the person where possible.

4. **Share with consent where appropriate.** Where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case. If in doubt, seek advice from the Information Management Team.

5. **Consider safety and well-being:** Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

6. **Necessary, proportionate, relevant, accurate, timely and secure.** Remember that the data protection principles still apply. You will need to ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

7. **Keep a record of your decision to share information.** Remember to record the reasons for sharing whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Although the principles cover sharing of information with anyone or any organisation, staff should ensure that if they are sharing information on a regular basis with an organisation that they have an agreed information sharing protocol in place. (See **Appendix D** for the corporate approach to setting up an information sharing protocol).

If you are sharing or disclosing personal information to a third party, please ensure that you have proper authorisation to do so either as part of your normal working practice or as a result of a subject access request where someone makes a formal request for their

personal information. **If you are in any doubt whether you can share information or disclose it to a third party, please contact the Information Management Team.**

7. Training and Awareness

All staff and Councillors will need to be aware of the Council's data protection policy. To help staff understand the basic principles within this policy a shorter guide will be prepared. For some posts within the Council, additional training and guidance will be required. Those posts will be identified through their work and any additional training and guidance will need to be discussed with the line manager in the first instance.

Induction
When staff and Councillors join the Council, it is important that they are introduced to their basic responsibilities under the Data Protection Act. For most staff and
Councillors, this level of understanding will be met by reading this policy. However, staff may need additional awareness based upon any specific induction requirements within their service groupings.

Continuing training
If additional Data Protection training or awareness is required beyond this policy, staff are encouraged to raise it during staff training, team meetings, supervisions. In the first instance, please contact your line manager or Corporate HR. If you require specific training relating on particular data protection issue, please contact the Information Management Team.

8. Enforcement

Significant intentional breaches of this policy will be handled under the Council's disciplinary procedures. If criminal activity is in evidence, then the police will be informed.

The Act removes the corporate protection of individual employees or agents from prosecution should they breach the conditions imposed by the Act. What this means is that staff are individually responsible for compliance with the provisions of the Act. The unauthorised accessing or processing of personal data is a criminal offence under s.55 of the DPA. For example, the accessing of someone else's files or information, even a close family member, can be a breach of the Data Protection Act. In accessing the files without authorisation, the person may have committed a criminal office. If you access personal information and disclose it to someone else then you will have breached the Act and be liable for a criminal prosecution.

The misuse of public information has been prosecuted under the offence of Misconduct in Public Office.

9. Performance Management

The Information Management Team will monitor performance with regard to the data protection policy indicators to monitor the performance on data protection are set out on the table below and will be reported as part of Corporate and Service Grouping performance management frameworks.

Performance Measure	Target	When
Response time on SARs	Less than 40 days	Reported quarterly

No adverse judgements from the Information Commissioner's Office linked to Data Protection issues.

10. Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. Durham County Council is registered as such. The Data Protection Act 2018 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

The Information Management Team will review the Data Protection Registration with Information Governance Group annually, prior to notifying the Information Commissioner.

Any changes to the register must be notified to the Information Commissioner, within 28 days. Therefore, any changes made between reviews will be brought to the attention of the Information Management Team immediately.

11. Policy Review

This policy will be reviewed at least once every three years and if appropriate, amended to maintain its relevance.

12. Contacts

The Information Management Team or guidance via the Intranet available at:

Lawrence Serewicz
Information And Records Manager

Tel: 03000 268038/ 07979 593074

Lynn Nash
Records Management Officer
Tel: 0191 372 8372 VPN 7777 8372

Julie Johnson
Freedom of Information officer / Data Protection
Tel: 03000 268073

Chris Paciorek
Freedom of Information officer / Data Protection
Tel: 03000 268036

Julie Purser
Freedom of Information officer / Data Protection
Tel: 03000 268037

Julie Hodgson
Freedom of Information Officer / Data Protection
Tel: 0191 372 8377 / 7777 8377
NB* Wed - Friday

Tracy Millmore
Information Management Assistant
Tel: 0191 372 8376 / 7777 8376

Neale Boswell
Admin Assistant Information Management
Tel: 0191 372 8373 / 7777 8373

Appendix A

Related Legislation

- Common Law Duty of Confidence
- The Human Rights Act 1998
- Computer Misuse Act 1990
- The Freedom of Information Act 2000 (FOI Act)
- The Regulation of Investigatory Powers Act 2000 (RIPA)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000 (SI 2000/2905)
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426)
- The Environmental Information Regulations 2004 (SI 2004/3391)
- The United Kingdom Data Protection (Processing of Sensitive Personal Data) Order 2006 (SI 2006/2068)
- The Criminal Justice and Immigration Act 2008
- The Data Protection (Notification and Notification Fees) (Amendment) Regulations 2009 (SI 2009/1677)
- The Data Protection (Processing of Sensitive Personal Data) Order 2009 (SI 2009/1811)
- The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 (SI 2010/31)
- The Data Protection (Monetary Penalties) Order 2010 (SI 2010/910).

Appendix B

Data Protection Champion

Role

- Contact for Information Management Team for Subject Access Requests
- Act as a point of contact on initial data protection issues

Responsibility

- Signpost other staff within the service to the Information Management Team
- Help locate personal information
- Coordinate response containing personal information to the Information Management Team

Appendix C

Checklist for when someone asks for their personal information (subject access requests)

Individuals have a right under the Act to make a request in writing for a copy of the information you hold about them on computer and in some manual filing systems. This is called a subject access request. They are also entitled to have a description of the information, what you use it for, who you might pass it on to, and any information you have about the source of the information.

The checklist should help you deal with subject access requests. Detailed guidance will be available from the Information Management Team.

1 Is this a subject access request?

Determine whether the person's request will be treated as a routine enquiry or as a subject access request. Any written enquiry that asks for information you hold about the person making the request can be a subject access request, but in many cases, there will be no need to treat it as such. If you would usually deal with the request in the normal course of business, do so. Examples of such requests might be:

- "I've forgotten the last date I made a payment to my account. Can you tell me what it is please?"
- "How many payments did I make from my account in the last 4 months?"

The following are likely to be treated as formal subject access requests.

- "Please send me a copy of my staff records."
- "I am a solicitor acting on behalf of my client and request a copy of his medical records. An appropriate authority is enclosed."

If you are in any doubt how to respond, go back to the individual or their representative and clarify the situation. It is important that you recognise requests that are formal. If you receive a formal request or are in any doubt whether the written request for personal information is a Subject Access Request, please contact the Information Management Team.

No Handle the query as part of your normal course of business it may be a request for information under the Freedom of Information Act or under the Environmental Information Regulations.

Yes, Go to **2**.

2 Do you have enough information to be sure of the requester's identity?
Often you will have no reason to doubt a person's identity. For example, if a person with whom you have regular contact sends a letter from their known address it may be safe to assume that they are who they say they are.

No. If you have good cause to doubt the requester's identity you can ask them to provide any evidence, you reasonably need to confirm it. Once satisfied, go to **3**.

Yes, Go to **3**.

3 Do you need any other information to find the records they want? No Go to **4**.

Yes, You will need to ask the individual promptly for any other information you reasonably need to find the records. You might want to ask them to narrow down their request. However, they do have the right to ask for everything you have about them and this could mean a very wide search. You have 40 calendar days to respond to a subject access request. The clock only starts after you have received any further information you need, and the statutory £10 fee has either been paid or waived. Go to **4**.

4 Are you going to charge a fee? No Go to **5**.

Yes, If you need a fee you must ask the individual promptly. Please consult with the Information Management Team if you have any questions about the statutory fee. The maximum you can charge is £10. The 40 calendar days clock only starts when you have all necessary information to help you find the records and you have received or waived the statutory fee. Go to **5**.

5 Do you hold any information about the person?

No if you hold no personal information at all about the individual, you must tell them this.

Yes, Go to **6**.

6 Will the information be changed between receiving the request and sending the response?

No Go to **7**.

Yes, You can still make routine amendments and deletions to personal information after receiving a request. However, you must not make any changes to the records as a result of receiving the request, even if you find inaccurate or embarrassing information on the record. Go to **7**.

7 Does it include any information about other people? No Go to **8**.

Yes, You will not have to supply the information unless the other people mentioned have given their consent, or it is reasonable to supply the information without their consent. Even when the other person's information should not be disclosed, you should still supply as much as possible by editing the references to other people. For more information and help, please contact the information management team. Go to **8**.

8 Are you obliged to supply the information?
There may be circumstances in which you are not obliged to supply certain information.

Please contact the Information Management Team for more on any exemptions. **No** If all the information you hold about the requester is exempt, then you can reply stating that you do not hold any of their personal information that you are required to reveal.

Yes, Go to **9**.

9 Does it include any complex terms or codes?

The information may include abbreviations or terms that the individual will not understand, for example, '02' means monthly payment, '03' means 'overdue'. **No** Go to **10**.

Yes, You must make sure that terms are explained so the information can be understood. Go to **10**.

10 Prepare the response

A copy of the information should be supplied in a permanent form except where the individual agrees or where it is impossible or would involve undue effort. This could include very significant cost or time taken to provide the information in hard copy form. An alternative would be to allow the individual to view the information on screen. You have 40 calendar days to comply with the request. Individuals can complain to the ICO or apply to a court if you do not respond within this time limit

Appendix D

Information Sharing Protocol

This document is being developed as a separate procedural document.

Appendix E

Information Governance Policy Framework

Information Gov

Policies:

Freedom of Information Policy

Environmental Information Regulations Policy

Procedures:

Relevant ICT Procedures:
- **Email**
- **Internet usage**

Data breach Procedures

Guidelines:

Disclosing personal information

still under development.

d Procedures in '**bold**

Appendix F

GLOSSARY

Processing – obtaining, recording or holding information or data, or carrying out any operation or set of operations on that information or data.

Data Subject – any living individual who is the subject of personal data.

Personal Data – data that relates to a living individual who can be identified either from those data and/or other information that is in the possession of, or is likely to come into the possession of, the data controller. This includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

Data Controller – person who (either jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed.

Note: The Data Controller is usually a company or organisation and is not an individual within that company or organisation.

Durham County Council is the data controller of all of the systems in use within this organisation and is registered with the Information as such.

Sensitive personal data
This is personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

Appendix G

Conditions for Processing (Schedule 9 and 10 of the DPA)

Conditions necessary for processing personal information (Schedule 2 and Schedule 3 of the Data Protection Act)

Processing is not allowed unless one or more of the following conditions is satisfied

1. with the consent of the data subject
2. to establish or perform a contract with the data subject
3. to comply with a legal obligation
4. to protect the vital interests of the data subject
5. for the exercise of certain functions of a public interest nature
6. for the legitimate interests of the data controller unless outweighed by the interests of the data subject.

There are additional conditions for processing sensitive data (Schedule 10 of the Act):

Sensitive personal data may be processed if one of the conditions in the first list is met **and** one of the following.

1. with the explicit consent of the data subject
2. to perform any right or obligation under employment law
3. to protect the vital interests of the data subject or another person
4. for the legitimate activities of certain not-for-profit bodies
5. when the data have been made public by the data subject
6. in connection with legal proceedings
7. for the exercise of certain functions of a public interest nature
8. for medical purposes
9. for equal opportunities monitoring

Individual Rights under the DPA

There are seven rights under the Data Protection Act.

Appendix H

1. The right to subject access

This allows people to find out what information is held about them on computer and within some manual records.

2. The right to prevent/restrict processing

Anyone can ask a data controller not to process information relating to him or her that causes substantial unwarranted damage or distress to them or anyone else.

3. The right to prevent processing for direct marketing

Anyone can ask a data controller not to process information relating to him or her for direct marketing purposes.

4. Rights in relation to automated decision-taking

Individuals have a right to object to decisions made only by automatic means e.g. there is no human involvement.

5. The right to compensation

An individual can claim compensation from a data controller for damage and distress caused by any breach of the act. Compensation for distress alone can only be claimed in limited circumstances.

6. The right to rectification, blocking, erasure and destruction

Individuals can apply to the court to order a data controller to rectify, block or destroy personal details if they are inaccurate or contain expressions of opinion based on inaccurate information.

7. The right to ask the Commissioner to assess whether the Act has been contravened

If someone believes their personal information has not been processed in accordance with the DPA, they can ask the Commissioner to make an assessment. If the Act is found to have been breached and the matter cannot be settled informally, then an enforcement notice may be served on the data controller in question.

Appendix I

Data Breach Procedures

These are available as a separate procedural document from the Information Management Team and on the Council's website Data Protection page https://www.durham.gov.uk/dataprivacy