Information Management Team

Data Protection Policy 2018

Altogether better

Durham County Council

Details:

Review Frequency: Every 3 years	Date of last review: 29 June 2021 Date of next review: 29 June 2023
Service number ID (if appropriate)	Manual: Information Management Team

Version Version ref	Date	Revision History	Reviser	Approved by	Review Date
21 May 2018	V1	Final	Lawrence Serewicz	GDPR/IGG	21 May 2021
15 April 2019	V2	Revised (contact details)	Paula Sheen		
29 January 2020	Web Version	Contact details and links modified	Lawrence Serewicz		
29 June 2021	V3.	Updates on privacy by design, DPO contact,	Lawrence Serewicz		

CONTENTS

Introduction

1. 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 General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

2. The GDPR sets out a number of standards and rules and places obligations on those who process personal information while giving rights to those who are the subject of the data. 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.

3. 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 Regulations and the six data protection principles. For more detailed advice and guidance, the Information Management Team (IMT) is available.

Statement of policy

4. 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.

5. The 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

6. At the heart of the Regulations is the need to protect personal information otherwise known as personal data and special category personal data. Special categories of personal data include data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union memberships; health; sex life or sexual orientation; genetic or biometric data uniquely identifying a natural person.

7. What this means is when the Council collects and uses personal information, it must then handle it and deal with it according to the six principles of data protection.

The Six Principles of Data Protection

8. If the Council or the individual follows these six principles, they will be acting in accordance with the Regulations. 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 GDPR.

9. The following six principles form the basis of the GDPR:

a) Lawfulness, fairness and transparency
Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

b) Purpose limitation
Personal data shall be 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.

c) Data minimisation
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d) Accuracy
Personal data shall be 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.

e) Storage limitation
Personal data shall be 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

f) Integrity and confidentiality
Personal data shall be 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.

10. The principles come with an additional responsibility as the council must be able to demonstrate compliance with these principles. The council must demonstrate how it is Accountable. It will do this through the policies and procedures it has to meet the Act's principles and requirements. The council is required by the Act to demonstrate that it complies with these principles. Generally, this is understood as the responsibility to demonstrate Accountability.

Scope

11. The policy covers all data that falls within the definition of personal data under the GDPR.

12. **Personal data** means data which relate to a living individual who can be identified:
    a) from those data, or
    b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and 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.

13. 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 Members in their role as a Member of the Council.

14. The policy covers all personal information that the Council holds in either electronic or paper format or file system and 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.

Roles and Responsibilities

Members

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

16. 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 to the ICO. As such, they have to handle personal information in line with the requirements of the six principles of data protection.

Staff

17. In line with the Council's code of conduct, all employees have a responsibility to protect confidential information. **The policy applies to all staff**.

Corporate Management Team (CMT)

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

19. 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

20. The Information Governance Group:

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

Heads of Service (HOS)

21. Heads of Service have responsibility for seeing that their service complies with the principles of data protection when processing personal data. They must ensure that staff are aware of their responsibilities under the GDPR and are trained to discharge those responsibilities. Heads of Service 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;
- ensuring 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;
- ensuring appropriate resources are in place to enable compliance with the data protection policy.

The Information Management Team

22. The Information Management Team is 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

23. 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

24. The Council has a standard clause in Council contracts, which requires the other party to comply with the requirements of the GDPR. 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.

Senior Information Risk Owner

25. The Senior Information Risk Owner (SIRO) is an Executive Director or Senior Management Board Member who will take overall ownership of the Organisation's Information Risk Policy, act as champion for information risk on the Board and provide written advice to Chief Executive on internal control in regard to information risk.

    The Senior Information Risk Owner in Durham County Council is:

    John Hewitt

Corporate Director Resources
Tel. 03000 261943

Caldicott Guardian

26. A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information for Health and Social Care 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. Their remit covers all social care records for children and adults.

    The Caldicott Guardian in Durham County Council is:

    Keith Forster
    Strategic Manager Performance and Information Management
    Children and Young Peoples Service
    Tel 03000 267396
    E mail: CaldicottGuardian@durham.gov.uk

Data Protection Officer (DPO)

27. A DPO is a statutory role as the legislation requires qualifying public authorities to have one. The DPO is an expert in data protection who monitors internal compliance, informs and advises the council on its data protection obligations, provides advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

    The DPO in Durham County Council is:

    Kevin Edworthy
    Strategic Manager Executive Support
    03000 268045
    E mail: DPO@durham.gov.uk

Development of Service and Corporate Procedures

28. From this policy, additional procedures and guidance notes will be developed. Each service must consider what specific guidance it may need to have in place to meet the data protection principles. The following areas cover the day-to-day work when dealing with personal information under the GDPR:

    - How we use personal information
    - Privacy notices
    - Information Rights
    - Data Protection Impact Assessments (DPIA)

- How we store it
- How we keep it confidential
- How we keep it secure
- How we respond to subject access requests
- How we keep it up to date
- How we share it

29. Please be aware that there will technical areas within the GDPR that are not relevant to the day to day work. If an issue, not covered in the relevant policy or procedure arises please contact the Information Management Team for advice and assistance.

How to process or use personal data

30. The GDPR has a very broad definition of processing data. Almost everything the council does with information, such as when it: obtains, holds, files, organises, transmits, retrieves, disseminates, discloses or destroys data, is processing information. Before we begin to use personal information, we have to provide a privacy notice that explains amongst other things what we are going to do with the information and the legal powers to use the information. In addition, we have to explain the legal rights available to the person.

31. As mentioned earlier, officers and Members have to comply with the data protection principles when they use personal information. Even though all the principles are equally important, you need to keep in mind that when you use personal information it is done fairly, lawfully, and transparently. (Principle 1).

32. This means for personal information it must have at least one condition for processing. For special category data you need at least one condition for processing and must have one from the second schedule. See Appendix 1.

33. Before we can use someone's personal information we have to give them a privacy notice. Whether we collect the personal information directly or we get it indirectly, another organisation gives it to us, we have to provide the person a privacy notice.

Privacy Notices

34. Being transparent and providing accessible information to individuals about how you will use their personal data is a key element of the Data Protection Act 2017 (DPA) and the EU General Data Protection Regulation (GDPR). The most

common way to provide this information is in a privacy notice. This document explains what we collect, why we collect it, how we will use it, what are the legal basis for using it, how we will store it, and the contact details for the Data Protection Officer.

35. In many situations where we obtain personal data as part of a simple transaction it should be straightforward to be transparent about what we are going to do with the personal information. Usually, this is done with the privacy notice.

36. However, in other situations it will not be effective to use a single document to tell the person what we do with personal data. There are other ways that we give the person privacy information such as face to face meetings, when we explain how a service works, or what the service does.

37. For more information on privacy notices see the guidance available on the intranet.

Information Rights

38. When we use a person's personal information, we have to let them know about their relevant information rights. When they want to exercise those rights, we must have a procedure in place to deal with them. In some cases, the rights are limited by the council's responsibilities so they require us to exercise judgments when dealing with them or refusing them.

39. The information rights are:

- **The right to be informed**
  In this right, the organisation has to inform the person about what is being collected and how it will be used. This is mainly met through the privacy notice.

- **The right of access**
  When asked, the council has to provide a person with access to their personal information. This is commonly called the subject access request (SAR) process.

- **The right to rectification**
  Here the person can ask for their personal information to be corrected or changed such as if we have the wrong address. In some cases, this can

be quite complex and controversial as there are limits on what can be changed.

- **The right to erasure**
  This right is also known as the right to be forgotten where a person can ask for some of their personal information to be deleted. However, there are limits to what can be erased as it is limited by the council's legal responsibilities.

- **The right to restrict processing**
  With this right, the person can ask that we stop or restrict processing of their personal information. The council has to demonstrate why it needs to continue to process the personal information and the consequences from stopping or restricting the use of the personal information.

- **The right to data portability**
  In certain circumstances, where we process a person's information under consent or a contract, and we use an automated process where no person is involved, we have to make the information available so they can transfer to another organisation.

- **The right to object**
  The person has the right to object to any processing we do. It is for the council to show why the processing is necessary. Where this is mainly available is when we use personal information based on consent such as marketing or doing a task in the public interest. In the latter situation, we have to justify why we need use the information.

- **Rights in relation to automated decision making and profiling**
  Like the right to data portability, this is based on automated systems where no person is involved. As such, this right is going to be applied rarely as the council does not use automated systems.

40. For further information on information rights, please see our information rights guidance documents on the intranet.

Data Protection by design and default

41. Data protection by design is about considering data protection and privacy issues upfront in everything we do. It helps us comply with the UK GDPR's fundamental principles and requirements, and forms part of our focus on accountability.

42. In pursuing Data Protection by design and default, we will follow the ICO's guidance on the matter.

43. We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

44. We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

45. All new systems used for data processing will have data protection built in from the beginning of the system change. This will be considered as part of the Data Protection Impact Assessment procedure

46. We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

47. In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

48. Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

Data Protection Impact Assessments

49. In certain circumstance, especially if we are using a new technology, we have to conduct a data protection impact assessment (DPIA). This is a process to identify and minimise the data protection risks of a project.

50. The DPIAs are mandatory for process that involves a high risk to individuals' interests such as;

    - a systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects

concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences;
- systematic monitoring of a publicly accessible area on a large scale.

51. At a minimum, a DPIA must

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

52. When a DPIA is needed, the Data Protection Officer (DPO) has to be consulted and should sign it off because of the high risk both in terms of the likelihood and severity of any impact on individuals.

53. For more information on Data Protection Impact Assessments see the guidance on the intranet which will explain when a short DPIA or a full DPIA is required. At a minimum all council processes that use personal data will need to have either a short DPIA or a full DPIA to signify that they have been reviewed.

How to hold personal information (records management)

54. The GDPR 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.

55. 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 Regulations.

56. For more information on records management see the Corporate Records Management Policy on the intranet

Archiving

57. 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 Records Office, you can contact them at the following:

Durham County Record Office
County Hall
Durham
DH1 5UL
03000 267619 record.office@durham.gov.uk
http://www.durhamrecordoffice.org.uk/

The duty of confidence

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

- the information itself must have the necessary quality of confidence;
- the information must have been imparted in circumstances that oblige confidence;
- disclosure must harm the party communicating it.

59. 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);
- about other organisations, since Data Protection only applies to information about individuals;
- which is not recorded, either on paper or electronically

60. For more information on the duty of confidence see the Duty of Confidence guidance on the intranet.

How to keep personal information secure

61. 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.

62. The Council is required to take all reasonable measures to ensure the personal information is held securely. 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.

63. 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.

64. 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.

PISP and ICT security policy

65. For more information on the PISP and ICT Security procedures see the relevant Personal Information Security Policy and the Information Security Policy on the intranet.

66. If records are to be moved, please refer to the Secure Handling and Transit of Papers policy on the intranet.

What to do about a data breach?

67. 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 Policy as qualifying breaches have to be reported to the ICO within 72 hours. A qualifying breach is one where there is a high risk to a person or persons about the consequences from the breach. If we can demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, Then we don’t need to report it.

68. To put it briefly, the council has to show the reasons for not reporting a data breach.

69. If the breach is likely to result in a high risk of adversely affecting individuals’ rights and freedoms, we must also inform those individuals without undue delay.

70. When we have to notify the ICO of a breach, we have to tell them the following:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects

concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

71. The Policy will state the procedure to be followed in order to:

- find out what data has been lost;
- mitigate the loss;
- contact the people whose data was lost;
- if serious, notify the Information Commissioner's Office.

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

73. For more information on potential data breaches, please see the Potential Data Breach guidance on the intranet.

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

74. 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 30 calendar days. Although there are some exceptions to this right, it is rare that these exceptions are used.

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

76. If you are in doubt, please contact the Information Management Team who can advise you on the appropriate response.

77. The Council's Subject Access Request procedure can be found on the Find out what information we hold about you page on the Council's website.

Data Quality

78. What we do to keep personal information 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. As a council we recognise the importance of having good quality data and the same applies for personal data.

79. A Data Quality Policy has been developed and approved. The policy defines data quality in terms of accuracy, validity, reliability, timeliness, relevance and completeness. When we collect and use personal data we should strive for the same principles.

- Accuracy means that performance data is presented in an accurate, clear, consistent and unbiased manner.

- Validity ensures data is recorded and used in compliance with relevant requirements i.e. the protection of information from unauthorised access or revision to ensure that the information is not compromised through corruption or falsification.

- Reliability means the data must be in an agreed format which conforms to recognised national standards.

- Timeliness ensures that data is available when it is needed as the collection of up to date information is essential to the effective and efficient operation of our processes.

- Relevance means that every effort should be made to ensure that recorded data is appropriate for the purposes for which it is used.

- Completeness ensures that data requirements meet the needs of the organisation and that the data collection processes match these requirements.

- For more information on data quality see the Data Quality Policy on the intranet.

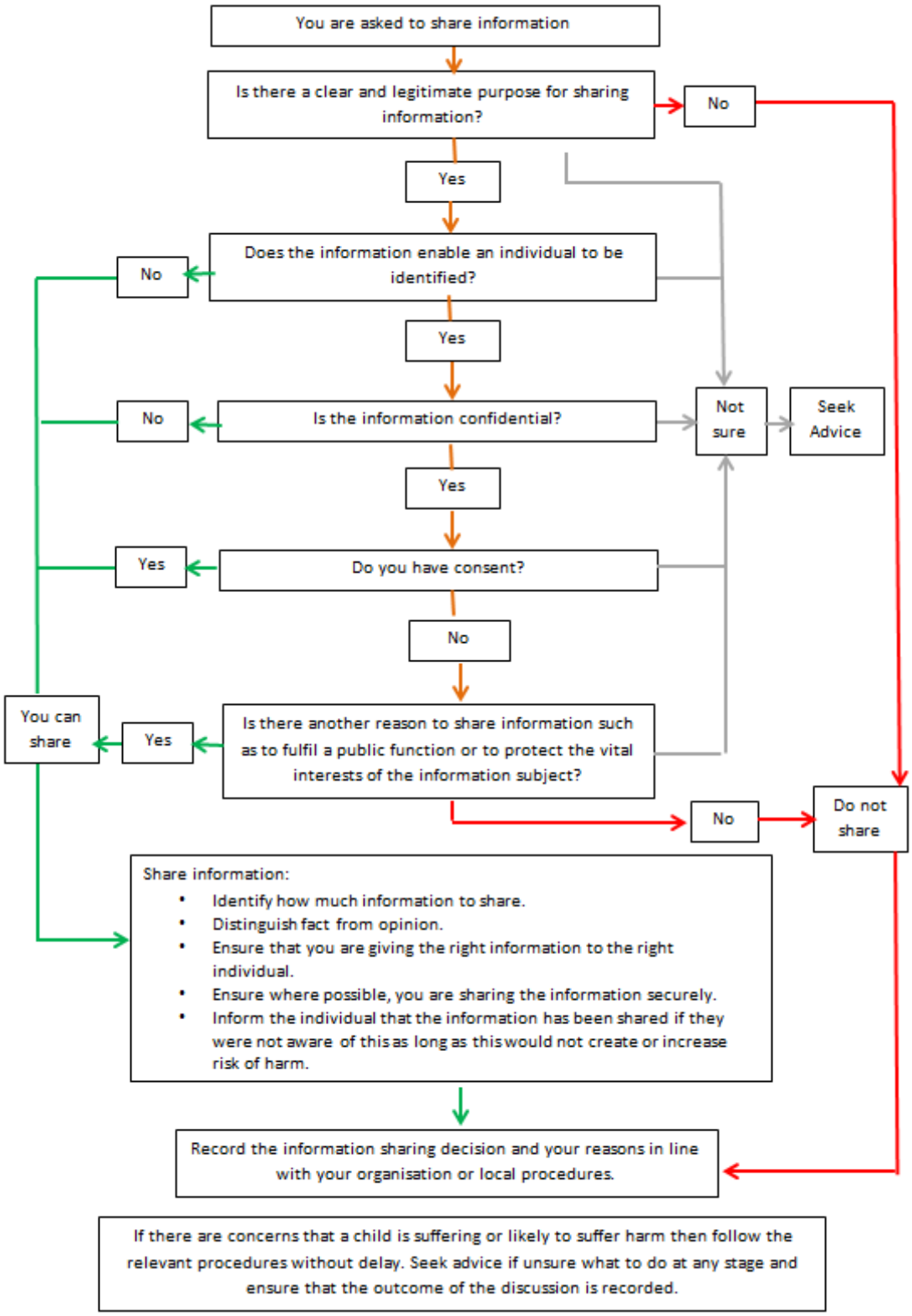
Sharing personal information

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

80. Information sharing is key to the Council's ability to deliver effective and 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, promoting welfare and for wider public protection. This sharing can be with a service level agreement or statutory sharing with other public authorities and agencies.

81. 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 preserving the privacy of the individual and sharing information when appropriate.

82. The flow chart below provides additional information on how to share data:


You are asked to share information
Is there a clear and legitimate purpose for sharing information?
No
Yes
Does the information enable an individual to be identified?
No
Yes
Is the information confidential?
No
Not sure
Seek Advice
Yes
Do you have consent?
Yes
No
Is there another reason to share information such as to fulfil a public function or to protect the vital interests of the information subject?
Yes
You can share
No
Do not share
Share information:
Identify how much information to share.
Distinguish fact from opinion.
Ensure that you are giving the right information to the right individual.
Ensure where possible, you are sharing the information securely.
Inform the individual that the information has been shared if they were not aware of this as long as this would not create or increase risk of harm.
Record the information sharing decision and your reasons in line with your organisation or local procedures.
If there are concerns that a child is suffering or likely to suffer harm then follow the relevant procedures without delay. Seek advice if unsure what to do at any stage and ensure that the outcome of the discussion is recorded.

S212 and S215 of the Data Protection Act

83. Schedule 2 Part 1 Paragraph 2 (212) and Schedule 2 Part 1 Paragraph 5 (215) of the Data Protection Act enable other organisations, e.g. Police, DWP, HMRC to request information relevant to crime prevention and detection of mental legal proceedings. These requests are processed by the Information Management Team working with relevant DCC services on the responses.

84. See the guidance note regarding these types of disclosure on the intranet

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

Training and Awareness

85. 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 an awareness guide is available. 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.

E-Learning

86. An online Data Protection course is available to all staff, with regular refresher training. All staff are required to complete this training, and the completion rate is monitored by regular reports to Service Grouping Management Teams and the Information Governance Group.

Enforcement

87. 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.

88. The GDPR removes the corporate protection of individual employees or agents from prosecution should they breach the conditions imposed by the Regulations. This means that staff are individually responsible for compliance with the provisions of the Regulations. The unauthorised accessing or processing of personal data is a criminal offence.

Performance Management

89. 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 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 30 days	Reported quarterly

Number of adverse judgements from the Information Commissioner's Office linked to data protection issues.

Notification to the Information Commissioner

90. The Information Commissioner maintains a public register of data controllers. Durham County Council is registered as such. The General Data Protection Regulations require every data controller to notify and renew their notification on an annual basis. Failure to do so is a criminal offence.

Equality and Diversity

91. Durham County Council is committed to promoting equality of opportunity, valuing diversity and ensuring discrimination, harassment or victimisation is not tolerated. Our policy is to treat people fairly, with respect and dignity. We also comply with legal requirements in relation to age, disability, gender, pregnancy and maternity, marriage and civil partnership, gender reassignment, race, religion or belief and sexual orientation.

Contacts

92. Further guidance is available on the Intranet at Think Privacy page.

You can contact the Information Management Team: E mail: dataprotection@durham.gov.uk and Telephone: 03000 267 803

Appendix 1 Lawful basis for processing personal data

Lawful Basis (Article 6)

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Special Category Data

When we use special category data we must have at least one of the conditions set out below from Article 9 of the GDPR. If we don't have one, we cannot use the special category data. We must stop using the data and delete it. Special category data is any personal information that is one or more of these categories.

• personal data revealing **racial or ethnic origin**;
• personal data revealing **political opinions**;
• personal data revealing **religious or philosophical beliefs**;
• personal data revealing **trade union membership**;
• **genetic data**;
• **biometric data** (where used for identification purposes);
• data concerning **health**;
• data concerning a person's **sex life**; and
• data concerning a person's **sexual orientation**.

Conditions from Article 9

a) the data subject has given explicit consent;
b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes;
e) processing relates to personal data which are manifestly made public by the data subject;
f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
g) processing is necessary for reasons of substantial public interest,
h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services ;
i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices,;
j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR which sets out the safeguards and derogations relating to processing data for archiving purposes.

Alternative formats