

**East Dunbartonshire Council
Information Sharing Policy 2018**

Contents

- 1 Data Protection: East Dunbartonshire Council
- 2 Purpose and Scope
- 3 Data Sharing
- 4 Information Commissioner and Data Sharing
- 5 Fair and Lawful Sharing of Personal Information
- 6 East Dunbartonshire Council: Decision to Share Personal Information
- 7 Policy Review

1. Data Protection: East Dunbartonshire Council

To be able to meet our statutory functions and responsibilities East Dunbartonshire Council (“the Council”) must obtain and use information about individuals. This personal information, however it is acquired, held, used, released or destroyed, must be dealt with lawfully, fairly and transparently. The General Data Protection Regulations (“GDPR”) sets out the Council’s Legal responsibilities. The Council’s Policy for the handling of personal information can be found using the following link

<https://www.eastdunbarton.gov.uk/council/data-protection>

One of the ways in which the Council will use an individual’s personal data is to share it. The Council will always respect the rights of data subjects and will only share personal information where doing so is fair and lawful. This document sets out the Council’s policies on the sharing of information.

2. Purpose and Scope

This Policy sets out the Council’s decision making process and practices for the sharing of personal information. This data sharing is understood to include both the sharing of personal information with outside organisations and between different function of the Council.

This Policy applies to all Council employees and Elected Members when carrying out business on behalf of the Local Authority.

3. Data Sharing

It is often necessary for the Council to share personal information. This sharing is carried out in order to meet the needs of the individuals or to meet statutory responsibilities.

Broadly speaking personal data sharing falls broadly into two categories:-

- i. a one off sharing of the personal information.
- ii. a systematic or routine sharing of personal information.

The sharing of information may also fall into two other categories:-

- i. Sharing of personal information between the Council and other organisations.
- ii. Sharing of personal information between different functions of the Council

Data Sharing with Other Organisations

This could be

- a reciprocal exchange of personal data between organisations;

- one or more organisations providing data to a third party or parties;
- several organisations pooling information and making it available to each other;
- several organisations pooling information and making it available to a third party or parties; or
- exceptional, one-off disclosures of data in unexpected or emergency situations;

Other organisations are those separate from the Council. This could be other Local Authorities, the Police, the NHS, the East Dunbartonshire Health and Social Care Partnership, Scottish Government, Her Majesty's Revenues and Customs, other departments of Westminster Government or another regulatory body. It also includes MPs, MSPs and MEPs.

Data Sharing within the Council

- When different parts of the same organisation make personal information available to each other.

It would be reasonable to assume when considering the term data sharing that it refers to solely to the exchange of personal information between the Council and an external organisation. However, this is not always the case.

The Council processes personal information for clearly established purposes. These reasons for the Council using personal information should be clearly explained to the individual data subject.

It is vital to remember that because one part of the Council holds personal information it is **not** then freely available to the Council as a whole. Rather, the purpose for which it was obtained must be respected.

It is this use of personal information for a different purpose, which would be considered sharing within the Council.

It is a breach of GDPR to use personal information for another purpose unless strict criteria are met so the decision to share information within the Council must be considered with the same seriousness as a decision to share with an outside organisation.

4. Information Commissioner and Data Sharing

The Information Commissioner's Office (ICO) is the United Kingdom's data protection regulator. Having carried out a consultation exercise the Information Commissioner published a Code of Practice setting out their views on the sharing of personal information.

In the foreword to the Code of Practice the Commissioner states;

“... under the right circumstances and for the right reasons, data sharing across and between organisations can play a crucial role in providing a better, more efficient service to customers in a range of sectors – both public and private. But citizens’ and consumers’ rights under the Data Protection Act must be respected.

Organisations that don’t understand what can and cannot be done legally are as likely to disadvantage their clients through excessive caution as they are by carelessness. But when things go wrong this can cause serious harm. We want citizens and consumers to be able to benefit from the responsible sharing of information, confident that their personal data is being handled responsibly and securely.”

The benefits of robust data sharing arrangements are:-

- better protection for individuals when their data is shared;
- better public trust by ensuring that legally required safeguards are in place and complied with;
- minimised risk of breaking the law and consequent enforcement action by the ICO or other regulators;
- increased data sharing when this is necessary and beneficial;
- greater trust and a better relationship with the people whose information we want to share;
- reduced reputational risk caused by the inappropriate or insecure sharing of personal data;
- a better understanding of when, or whether, it is acceptable to share information without people’s knowledge or consent or in the face of objection; and
- reduced risk of questions, complaints and disputes about the way we share personal data.

5. Fair and Lawful Sharing of Personal Information

The decision to share personal information should not be taken lightly. The Council must be able to demonstrate that the sharing is proportionate and fair to the individuals whose personal data will be shared.

- The sharing of personal information must be carried out for a clearly understood and defined purpose.
- The sharing of information should be carried out to meet objectives that can only be achieved by sharing the personal information.
- Personal information can only be shared where the data subject has consented to the use of the information or there is another legal basis to share.

These grounds to share information are given through the conditions to process in Article 6 of the GDPR:-

- Consent
- The processing is necessary:
 - in relation to a contract which the individual has entered into; or
 - because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
- The processing is in accordance with the "legitimate interests" condition.
 - The 'legitimate interests' condition provides grounds to process personal data in a situation where an organisation needs to do so for the purpose of its own legitimate interests or the legitimate interests of the third party that the information is disclosed to.

Special Category Personal Data

GDPR identifies a 'special category' of personal information as being particularly sensitive. Special category personal data is information as to:-

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- processing of genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation

The criteria necessary to use special category personal data are given under Article 9 of GDPR. These are more difficult to meet. In addition to an Article 6 condition, one of the following conditions must apply.

Article 9 GDPR

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:
 - a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
 - 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 in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
 - 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 and that the personal data are not disclosed outside that body without the consent of the data subjects;
 - e. processing relates to personal data which are manifestly made public by the data subject;
 - f. processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
 - g. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
 - 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 on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

- 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, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
 - 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) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.
4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

6. Agreements with 3rd Parties

Where the recipient of the Council's personal information will process solely on the Council's instructions, that recipient will be a data processor. GDPR demands that every data sharing arrangement with a data processor has a contract in place. Sharing personal information with a processor without a contract is a breach of GDPR.

Where the recipient of the Council's personal information will also take decisions over the personal information that recipient will also be a data controller. The Council should have in place a formal data sharing arrangement to defend the Council.

7. The Council: Decision to Share Personal Information

The Council has put in place an approval process for the sharing of personal information.

Service Areas wanting to share any personal information held will seek approval to do so.

An application will be made to the Information Management Team, which will review and consult with the service area and the Council's Data Protection Officer (DPO) before a decision is taken on the sharing of the personal data.

The Council has prepared two forms to process this application. One form covers systematic and ongoing data sharing agreements. A separate application form covers one off requests to share personal data.

These forms require explicit justification for the sharing of information and serve as the record that the Council's actions are both fair and lawful.

One off requests to share personal data with the Police will not be dealt with through this approval process. Existing arrangements will remain. This type of request will be treated separately. In these circumstances, a request form will be provided to the Council by the Police and passed to the Information Management Team directly.

The Council's forms to share personal data are attached as appendices to this document and are available on the Council Hub and on the Council's 'Information Sharing' Connections Page.

Requests to share information will be supported by a Privacy Impact Assessment and, where appropriate, a Data Sharing Agreement will be agreed between the Council and the third party organisation.

8. Policy Review

This Policy will be reviewed annually to reflect operational improvements and changes to best practice.

Request to Share Personal Information

Please complete the following form and submit to the Data Protection Officer at the following email address: dpo@eastdunbartn.gov.uk

Please contact the Information Management Team should you wish to discuss the application.

Name of Officer/ Elected Member	
Date	
Information to be shared	

Is the sharing of personal information justified?		Yes	No
Questions to answer	Comments		
Is the proposed sharing of personal information a one off or routine?			
What is the purpose of sharing the personal information?			
What is the benefit to sharing the personal information?			
Would any individual be disadvantaged by the sharing of the personal information?			
Are conditions under Article 6 of GDPR and Article 9 if special category met? If so, which conditions?			

Does the Council have the power to share the personal information?		Yes	No
Questions to answer	Comments		

What condition under Article 6 of GDPR justifies the sharing of the personal information?	
Is the personal information special category personal information?	
If so, what condition under Article 9 of GDPR justifies the sharing of personal information?	
The nature of the information you wish to share (for example, was it given in confidence?).	
Will the recipient of the personal information take decisions over its use or will they process personal information solely on the instruction of the Council.	
If the recipient will only process personal information at the Council's instruction will there be a contract between the parties to cover the sharing of personal information?	
If the recipient of the personal information will take decisions over its use, is a sharing arrangement in place?	

Is the sharing of personal data proportionate and fair?	Yes	No
Questions to answer	Comments	
What information needs to be shared?		

Which other organisations will be involved?	
Can you tell people about the data sharing? If so how will you communicate this?	
What measures are to be taken to ensure adequate security is in place to protect the data?	
What arrangements need to be in place to provide individuals with access to their personal data if they request it?	
Is there an agreed common retention periods for the data.	
What actions are required to ensure secure deletion when required.	

Details of Decision: To be completed by DPO	
Decision	
Decision taken by	
Date of Decision	
Reason for Decision	
Any specific arrangements for retention/ destruction of the personal information	

Date of Disclosure	
Signed	
Dated	

Document Control Table	
Prepared by	Stephen Armstrong – Freedom of Information/ Data Protection Officer
Peer Reviewed By	Karen Watt- Information and Records Manager
Authorised by Senior Responsible Person	Signature:- _____ Date:- _____ Print Name _____
Source Location	
Published Location	
Other Documents Referenced	
Related Documents	Information and Records Management Strategy and Information Management Strategic Implementation Programme(IMSIP) EDC Classification Scheme and Retention Schedules Appraisal and Disposition Policy and Procedures Vital Records Policy Confidential Waste Policy Data Protection Policy Data Protection Breach Reporting Policy and Guidance Freedom of Information Policy and Guidance Toolkit Information Security Policy IM – File Housekeeping – Employees Guidance Note (1) 03.08.12 IM – Top Ten Tips for Better Records Management – Employee Guidance Note (2) 03.08. Saving an Email Guidance Naming Electronic Records
Acknowledgements	

Version Control Table			
Version number	Date issued	Author	Update information
V1	August 2017	Freedom of Information/ Data Protection Officer	Data Sharing Policy v1 Draft
V1.3	May 2018	Freedom of Information/ Data Protection Officer	Data Sharing Policy v1.3