sustainable thriving achieving
East Dunbartonshire Council
www.eastdunbarton.gov.uk

Data Protection Policy 2018

Version 4
Freedom of Information/ Data Protection Officer
Date: May 2018

1 **Purpose**

1.1 In order to provide individuals with services the Council must obtain and use information that identifies them. This information is known as personal information.

1.3 The Council will always take care of the personal information it holds. The Council takes a 'privacy by design' approach to the care of personal information. The impact that the Council's activities may have on peoples' privacy will be considered at the very start of policy and process development.

1.2 As of 25th May 2018, the Council's handling of personal information is governed by the General Data Protection Regulations, also known as GDPR.

1.3 Further data protection law will be introduced by the new Data Protection Act which is currently being drafted at Westminster.

1.4 These legislation replace the existing Data Protection Act 1998.

1.5 The Council commits itself to the principles for the use of personal information set out under GDPR.

1. *Personal data shall be:*
   a. *processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*
   b. *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 ('purpose limitation');*
   c. *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*
   d. *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 ('accuracy');*
   e. *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 ('storage limitation');*
   f. *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 ('integrity and confidentiality').*

2. *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').*

In relation to the lawfulness of processing set out in the first principle above, the Council will only process personal information where a GDPR Article 6 condition is met. For the processing of special category personal data, the processing will only take place where a further GDPR Article 9 condition is met. Processing of personal data relating to criminal convictions and offences will comply with Article 10 of GDPR.

1.4 The Council will develop our commitment to data protection compliance by developing a range of policies, procedures and guidelines which will promote best information management practice. In addition to this policy, the key documents in terms of data protection are:

- Data Breach Reporting Procedure
- Subject Access Request Procedures
- Data Sharing Policy
- Data Protection Impact Assessment Policy
- Records Management Policy
- Corporate Retention Schedules
- Corporate ICT Security Policy
- Commissioner's Office Guidance

2 Scope

2.1 This policy sets out the corporate policy for the management all the personal information that the Council processes.

2.2 This Policy applies to all service areas, officers, and Elected Members of East Dunbartonshire Council. It also applies to third party service suppliers who are processing personal data on behalf of the Council.

3. Responsibilities

3.1 The Council has a corporate responsibility for data protection.

3.2 In their role as representatives of their constituents, Elected Members are each separately defined as “Data Controllers”.

3.3 The Council’s Chief Solicitor and Monitoring Officer is the Council’s Data Protection Officer (DPO) and has corporate responsibility for the Council’s processing of personal information.

3.4 Each Strategic Lead, as data controllers for their service remit, will retain responsibility for ensuring compliance with the provisions of GDPR within their service areas. Their main roles will be in monitoring compliance within their departments, monitoring compliance by external service providers who are processing personal data on behalf of the service areas, maintaining the accuracy of their departmental input into the Council’s notification, and processing Subject Access Requests which relate to records held by their departments.

3.5 All employees and Elected Members are individually responsible for ensuring that their collection, storage, processing and destruction of data are in accordance with GDPR. All employees and Elected Members have a duty to carry out regular accuracy checks of Personal Data in the normal course of business.

3.6 Disciplinary procedures may be enacted in the event of non-compliance with the Data Protection Policy. It is a criminal offense to knowingly or recklessly obtain or disclose Personal Data without the consent of the Data Subject unless this is necessary to detect or prevent crime, or is authorised by another statute or rule of law.

4. Training, guidance & advice

4.1 The Council’s Information Management Team will advise on all aspects of the Council’s dealings with personal data and will seek to instruct all users of personal data in best practice.

4.2 In addition to the Information Management Team, the Council’s Legal Services team will offer advice on Data Protection issues as they arise.

4.3 The Council’s Strategic Leads and service Managers will ensure appropriate Data Protection training is given to all employees within their service remit.

5. Notification

5.1 Data controllers must notify the Information Commissioner’s Office with a description of their processing of personal data.

5.2 The Commissioner maintains a public register which details:

5.3 The Council’s notification will be updated annually to reflect processing of personal data which is undertaken by the Council. Updates will take place when identified by individual services.

5.4 The Council will also arrange the annual notification for Elected Members, although they will be required to individually authorise notification and updates and as a consequence undertake to abide by the principles of GDPR.

5.5 The Council's DPO is responsible for establishing and maintaining the Council's notification. Strategic Leads will be responsible for reporting changes in their processing of personal information to the DPO.

6 Data Subject Rights

6.1 GDPR grants the subjects of personal information certain rights in relation to their information. These are:-

- Right to be Informed
- Right of Access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision making including profiling

6.2 It is the responsibility of all Council employees to recognise and facilitate requests to from individuals to exercise these rights.

7 Right of Subject Access

7.1 Every individual has the right to request a copy of all the information held about them by the Council. This is known as a Subject Access Request.

7.2 A Subject Access Request must be answered within a month. There may be situations where information about an individual is exempt from release. This could be because the individual's information is also the personal data of another person or it may be felt that the release of information may cause harm. The Information/ Data will provide advice on exemptions to the release of Information Management Team.

7.3 The Council has prepared detailed guidelines on dealing with subject access requests. Each service area has responsibility for providing the response to requests for access to personal information held by them, subject to any guidance from the Information Management Team.

8 Data Acquisition

8.1 Individuals must be made aware of what the Council will do with the personal information they entrust to the Council.

8.2 Each strategic lead will have in place an approved privacy notice for each of their different functions. The privacy notices must clearly explain exactly how and why an individuals' personal information will be used.

8.3 It is the responsibility of the relevant Strategic Lead to ensure that privacy notices are issued. When obtaining information directly from the individual this must be at the time

the information is obtained. If the personal information is obtained from a third party the individual must be informed quickly and within one month at the latest.

9 Data Retention

9.1 The Council has adopted the Scottish Council on Archives Record Retention Schedules (SCARRS). These cover all records in each department, and will define how long all types of information is to be retained.

9.2 All Officers and Elected Members have a responsibility to ensure that personal data is disposed of securely once the need to retain it has passed.

9.3 The Council's Information and Records Manager will provide guidance with retention scheduling and the most appropriate methods of destruction for different types of records.

9.4 Retention schedules will be available to employees through Council's Records Management Connections Group and on the Council HUB.

10. Security

10.1. The Council views the security of the personal information it holds as being of the highest importance.

10.2. The Council will take all organisational and technical measures to prevent against the unauthorised access to personal information and prevent accidental loss, destruction or damage to the personal data.

10.3. All officers and Elected Members must follow the Council's processes and procedures to ensure the security of personal data to which they have access.

10.4. The Information Commissioner has powers to impose fines of up to 20 million euros for data breaches.

10.5. All officers and Elected Members must adhere to the Council's Potential Data Breach process and report any suspected data breach to the Council's DPO.

10.6. All officers and Elected Members have a duty to report any suspected criminal offences under GDPR to the DPO.

10.7. Criminal offences under the GDPR include:-

- unlawfully obtaining, disclosing, or procuring the disclosure of personal data;
- selling, or offering to sell, personal data which has been unlawfully obtained;
- processing personal data without notifying the Information Commissioner (and other offences related to notification);
- failing to comply with an enforcement notice or an information notice, or knowingly or recklessly making a false statement in compliance with an information notice.

11. Audit

11.1. Data Protection arrangements and guidance will be reviewed annually. An audit of arrangements will be covered during systems audits conducted by Internal Audit.

12. Review

12.1. This policy will be reviewed annually with amendments being reported to the Policy & Resources Committee.

13. Legislative Context

13.1. This policy exists alongside a number of related information management policies and procedures governing the Council's management of information:-

- General Data Protection Regulations (GDPR)- replaces Data Protection Act 1998
- Data Protection Bill/Act, will replace the Data Protection Act 1998
- Freedom of Information (Scotland) Act 2002 – The Freedom of Information (Scotland) Act 2002 provides significant and important rights to access information.
- The Freedom of Information (Scotland) Act 2002 came into force on the 1st of January 2005 and gives everyone a legal right to request information held by a Scottish Public Authority.
- Environmental Information (Scotland) Regulations 2004 - The Environmental Information (Scotland) Regulations 2004 (also referred to as 'the EIRs') came into force on 1st January 2005. Every Scottish public authority has a duty to make environmental information available on request.
- Re-use of Public Sector Information Regulations 2015 – The Regulations implement an EU directive that encourages the re-use of public information for purposes other than its original purpose.
- BS 10008:2008 - Evidential Weight and Legal Admissibility of Electronic Information Specification British Standard that outlines best practice for the implementation and operation of electronic information management systems
- The INSPIRE (Scotland) Regulations 2009: The Regulations aim to make consistent spatial datasets about the environment available to the public and to create services for accessing these datasets.
- Public Records (Scotland) Act 2011 (the Act) - This legislation supports an ethos that better appreciates the value of records across the public sector came fully into in January 2013. The Act require that named public authorities across Scotland including the Scottish Government, Scottish Parliament, local authorities, the Scottish courts, the NHS and others will be required to produce and implement a records management plan (RMP) to be agreed with the Keeper of the Records of Scotland. The draft model plan suggests 14 elements that the Keeper would expect a Scottish public authority to consider when creating its RMP as follows:

    - Senior Management responsibility
    - Records Manager responsibility
    - Records management policy statement
    - Business classification
    - Retention schedules
    - Destruction arrangements
    - Archiving and transfer arrangements
    - Information security
    - Data protection
    - Business continuity and vital records

- Audit trail
- Competency framework for records management employees
- Assessment and review
- Shared information

13.2. Acknowledgement of Service Specific Legislation – This policy acknowledges that individual Council Services records may be subject to individual Acts of Parliament and Codes of Practice not mentioned above which should be followed unless superseded by more current legislation.

Document Control Table	
Prepared by	Stephen Armstrong – Freedom of Information/ Data Protection Officer
Peer Reviewed By	
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	April 2004	Freedom of Information/ Data Protection Officer	EDC Data Protection Policy 2004
V1.1	October 2009	Freedom of Information/ Data Protection Officer	EDC Data Protection Policy 2009
V1.2	December 2014	Freedom of Information/ Data Protection Officer	EDC Data Protection Policy 2015
V2	May 2018	Freedom of Information/ Data Protection Officer	EDC Data Protection Policy 2018