# EAST RENFREWSHIRE COUNCIL

# DATA PROTECTION POLICY

| Version | Date | Reason |
|---|---|---|
| Version 2.0 | May 2018 | Legislative Changes |
| Version 2.1 | August 2020 | Minor Revision |
| Version 2.2 | August 2022 | Reflect new information governance group, amendments to DPIA Framework & document format changes |

**Version Awareness**

The audience of this document should be aware that a physical copy may not be the latest available version. The latest version, which supersedes all previous versions, is available only on our website. Those to whom this policy applies are responsible for familiarising themselves periodically with the latest version and for complying with policy requirements at all times.

# 1. Contents

# 1 Introduction

1.1 The Council needs to collect and use information about people (known as personal data) to discharge its functions as a local authority. This personal data must be handled fairly and lawfully.

The Council regards the fair and lawful treatment of personal data as central to our operations and essential to the maintenance of a relationship of trust between us and our staff and customers. The Council will encourage and promote in its staff a culture of awareness of the legislation governing the use of such data and its guiding principles.

1.2 Although data protection legislation is complex, its ethos is simple. As its title suggests it protects people's Personal Data by regulating the way in which organisations, such as the Council, handle it.

1.3 The data protection regime in the UK comprises the provisions of the UK General Data Protection Regulation ("UK GDPR"), and the Data Protection Act 2018 ("DPA18") and associated regulations. The previous domestic legislation, the Data Protection Act 1998 ("DPA98") is repealed.

1.4 The UK GDPR and the Data Protection Act 2018 introduces a number of key changes, which are reflected in this revised Policy.

1.5 Understanding data protection requires an awareness of some of the key definitions. Definitions can be found in the section Glossary of Definitions.

1.6 The Council, in recognition of its data protection obligations, first approved a Data Protection Policy in December 2003. Since then, a range of policies, procedures and guidelines promoting compliance and best practice, have been developed and incorporated into an Information Governance Framework, Appendix 1 which supports how we comply with the requirements of the data protection law and meet our obligations in terms of the Accountability Principle.

1.7 In recognition of our data protection obligations and in addition to this policy a range of policies, procedures and guidelines promoting compliance and best practice have been developed to support a robust data protection and the wider Information Governance Framework – Appendix 1. In addition to this Data Protection Policy, key Council documents include;

- Data Incident Breach Management Procedures
- DPIA Framework
- Information Classification Procedure
- Information Rights and Subject Access
- Information Security Policy
- Records Management Plan
- Records Management Policy

This list is not exhaustive and all relevant data protection and wider information governance guidance can be obtained from section on the Council's Information

Governance intranet pages and the Archives and Information Governance section of the Council's website.

## 2. Scope

This policy applies to all Services, employees and Elected Members of East Renfrewshire Council, its Cabinet, Committees and sub committees, and covers all Personal Data and Special Category Data which they process. It should be read alongside other Council policies and guidelines on the use of non-personal data and wider information governance issues.

## 3. Data Protection Principles

3.1 Under the UK GDPR, there are six principles that regulate when and how Personal Data should be processed. These principles cover rules for the collection, maintenance and security of personal data. The Council is fully committed to complying with the Data Protection Principles. As such, the Council undertakes that Personal Data will be:-

### Processed fairly and lawfully and transparently

We will only process personal data for one or more of the purposes specified in GDPR/DPA 18 and will tell the data subject what processing will take place through the use of appropriate privacy notices. We will ensure that the processing matches the description given to the data subject. We will highlight in the notice any special category or criminal conviction data that will be processed and advise of the basis for doing so.

### Collected and processed only for one or more specified, explicit and legitimate purpose(s)

We will specify what the personal data collected will be used for and limit the processing of that data to what is necessary to meet the specified purpose. We will ensure that the use of any special category data accords with the lawful bases for processing set out in Art 9 of GDPR.

### Adequate, relevant and limited to what is necessary

We will not store any personal data beyond what is strictly required for any given purpose. We will ensure that the use of special category or criminal conviction data is limited to that which is essential to the purpose of the processing

### Accurate and kept up to date and that inaccurate data will be erased or rectified without delay.

We will ensure that we have efficient processes in place to identify and address out of date, incorrect and redundant personal data. Special attention will be

given to ensuring the accuracy of special category and criminal conviction data held.

**Kept for no longer than is necessary.**

We will, where possible, store personal data in a way that limits or prevents identification of the data subject and will in any event ensure that personal data is disposed of in accordance with our Records Management Plan which ensures that we comply with not only data protection but the Public Records (Scotland) Act 2011.

**Processed with appropriate security and that it will use adequate technical and organisational measures to prevent unauthorised or unlawful processing or accidental loss, destruction of, or damage to Personal Data**.

We will use appropriate technical and organisational measures to ensure that the integrity and confidentiality of personal data is maintained at all times. We recognise the added sensitivity of special category and criminal conviction data and will take necessary steps to ensure that the level of security around such information reflects its importance to the data subject.

## 4. Special Categories of Personal Data and Criminal Convictions Data

### 4.1 Appropriate policy

In terms of the provisions of the UK GDPR & DPA2018 the Council will only be entitled to process special category and criminal conviction data in reliance of certain conditions if it has an appropriate policy document in place.

An appropriate policy document must explain our processes for ensuring compliance with the principles set out in Section 3 above and indicate the process of retention and erasure.

*4.1.1* The Council will only process **special categories** of data where the data subject explicitly consents to such processing or one of the following conditions apply:

- there is a substantial public interest which makes the processing necessary. In such cases the processing will be proportionate to the aim pursued and will be subject to further measures to safeguard the privacy rights of the data subject.

- the processing relates to personal data which has already been made public by the data subject

- the processing is necessary to carry out obligations and exercise rights in the field of employment and social security and social protection law

- the processing is necessary for the establishment, exercise or defence of legal claims

- the processing is specifically authorised or required by law

- the 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

- the processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent

- the processing is necessary for reasons of public interest in the area of public health In such cases the processing will be proportionate to the aim pursued and will be subject to further measures to safeguard the privacy rights of the data subject.

- the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In such cases the processing will be proportionate to the aim pursued and will be subject to further measures to safeguard the privacy rights of the data subject.

4.2 In any situation where special categories of data are to be processed the basis for processing will be recorded. The Council will adopt additional protective measures to ensure the security of special category and criminal conviction data and these will be reflected in the Information Handling Policy

## 5. Data Protection Governance Arrangements

### 5.1 Corporate Responsibility

The Council has a corporate responsibility for data protection and must take responsibility for ensuring it is compliant with its obligations. This is known as the Accountability Principle. To demonstrate our commitment to data protection and to improve the effectiveness of our compliance efforts, the Council has allocated particular responsibilities to certain officers. A governance chart is attached in Appendix 2 to this Policy.

### 5.2 SIRO and Corporate Management Team

The Chief Executive is currently the Senior Information Risk Owner ("SIRO") for the Council. The SIRO is supported in this role by the Head of ICT and Digital Enablement, the Strategic Insight and Communities Senior Manager, the Chief Officer – Legal and Procurement and the Information Governance Officer. These officers will report directly to the SIRO on information governance issues including data protection as necessary.

The SIRO is a member of the Council's Corporate Management Team which meets on a fortnightly basis.

## 5.3 Roles and Responsibilities

5.3.1 Under GDPR the Council must designate a statutory Data Protection Officer (DPO) on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices. The key tasks of the DPO are prescribed and are to:-

- Inform and advise the Council on GDPR compliance;
- Monitor Compliance;
- Advice on Data Protection Impact Assessments;
- Training;
- Conduct Information Audits
- Be the first point of contact for the regulators; and
- Have due regard to the risk associated with the Council's processing operations.

5.3.2 The Information Governance Officer is the Council's DPO. The Council will ensure that the DPO has sufficient independence to properly undertake the above tasks and reports directly to the SIRO and Corporate Management Team in matters relating to Data Protection.

5.3.3 Each Service and its senior management team will be responsible for ensuring compliance with the provisions of UK GDPR / DPA18 within their own department and service areas. The Service Director will bear ultimate responsibility for compliance with the Information Governance Framework across their directorate and services.

## 5.4 Employees and Elected Members

5.4.1 All employees and Elected Members are individually responsible for ensuring that their handling of Personal Data is in accordance with GDPR/DPA18. They should familiarise themselves and comply with all relevant Council data protection guidance. Advice can be obtained at any time from the DPO.

5.4.2 The SIRO has overall responsibility for information governance. However, the day to day responsibility for driving the Council's information governance agenda is delegated to the Strategic Insight and Communities Senior Manager and the Information Governance Officer.

5.4.3 The Records Manager will record and co-ordinate the handling of all Subject Access Requests received by the Council. They will process and respond to any cross departmental subject access requests and provide advice and guidance as necessary. Requests relating to a single Service are the responsibility of that Service.

5.4.4 The Information Governance Officer will conduct requests for reviews and offer advice on data protection issues upon request.

5.4.5 The Information Security and Digital Risk Officer has a key role in ensuring compliance with the sixth principle relating to data security by providing advice and guidance to Services on information security.

### 5.5 Governance and Working Groups

Each Service will have a representative on the I**nformation Governance Delivery Group** which provides cross-department leadership, ownership and enthusiasm on behalf of the Corporate Management Team to drive the information governance agenda, coordinate action across departments, and ensure the Council is meeting its ambitions and statutory responsibilities.

This group will promote and facilitate best practice in;

- information governance and assurance;
- risk management; and
- a *privacy by design - data protection by default* way of working.

Provide support to SIROs to understand how strategic goals may be impacted by information governance risks and of how such risks may be effectively managed to ensure accountability with legislative compliance.

## 6. Notification of Processing Activities

6.1 The Council must advise the Information Commissioner's Office that it holds personal information about living people. It must also pay a fee in accordance with the Data Protection (Charges and Information) Regulations 2018.

6.2 The DPO shall ensure that prompt payment of any relevant fee is made on behalf of the Council as and when required.

6.3 **Controllers** are obliged to document their processing activities under UK GDPR. The Council's notification and the updated Information Asset Register (IAR) will form the basis of the Council's documentation of processing activities.

6.2 The **Information Asset Owners** (IAOs) role is to understand what information is held by their service, what is added and what is removed, how information is moved, and who has access and why. They must ensure that written procedures are in place and followed relating to these activities, risks are assessed, mitigated and the risk assessment processes are audited. They are also responsible for ensuring their service Information Asset Register entries are accurate and up to date.

## 7. Data Subject Rights

7.1 The GDPR provides **data subjects** with the following rights regarding their personal information:

- The right to be informed about how their information will be used.
- The right of access to their personal information (**subject access request**)
- The right to rectification, which is the right to require the Council to correct any inaccuracies.
- The right to request the erasure of any personal information held by the Council where the Council no longer has a basis to hold the information.

- The right to request that the processing of their information is restricted.
- The right to data portability.
- The right to object to the Council processing their personal information.
- Rights in relation to automated decision making and profiling.

7.2 The Council will publish detailed information for the public that will set out what these rights are and how these can be exercised within its Privacy Policy and Service Privacy Notices which are published on our website.

7.3 The Council will respond to any requests to exercise these rights without undue delay and, in any event, no later than 30 days from receipt and confirmation of the applicant's entitlement. No fee will be charged unless the DPO considers the request to be manifestly unfounded or excessive in which case he/she shall determine the appropriate level of charge.

7.4 Further information on compliance with all data subject rights, can be obtained from the Council's Subject Access Request guidelines.

## 8. Privacy Notices

8.1 Data subjects have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UKGDPR. The Council must provide data subjects with information including:

- purposes for processing their personal data
- retention periods for that personal data, and
- with whom it will be shared within a 'Privacy Notice'.

8.2 Privacy Notices must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language. To meet this requirement the Council will adopt a combination of different techniques including layering, dashboards, and just-in-time notices to inform our residents on how we use their personal data.

8.3 Privacy Notices must be regularly reviewed, and where necessary, updated.

## 9. Training and Guidance

9.1 All Council staff will be required to undertake annual on-line data protection refresher training as a minimum. The requirements of this policy will be advised to new employees of the Council at their induction training.

9.2 Services to ensure that staff training is commensurate with their employment role and reflects the nature of the personal information and data sets that they interact and that refresher training is undertaken annually.

## 10. Data Retention

10.1 The fifth data principle states that Personal Data should "not be held for longer than is necessary". What is necessary can vary, depending on the nature of the information and why it is held.

10.2 Each Service has a responsibility to ensure that appropriate retention schedules are in place for records which they hold, and to arrange for the secure destruction of data in accordance with such schedules. The Records Manager, as outlined in the Council's Records Management Policy, shall provide advice on request in relation to records management and retention issues.

10.3 In accordance with its obligations under the Public Records (Scotland) Act 2011, the Council has adopted a Records Management Plan containing appropriate retention and disposal schedules. Services will adhere to this plan to ensure compliance with the fifth data protection principle.

## 11. Information Security

11.1 *The sixth data protection principle provides that appropriate technical and organisational measures should be taken to ensure that all Personal Data is secure*.

11.2 All employees and Elected Members have responsibility for keeping the Personal Data which they handle in the course of their work, safe and secure.

11.3 By adopting recognised information security practices, the Council can demonstrate to customers, partners and stakeholders that it can be trusted to protect the confidentiality, integrity and accessibility of the information it holds.

11.4 Information Security is not purely a technical issue. Information security principles apply to all information held by the Council, whether this is held in electronic or non-electronic format.

11.5 Further information and advice on information security can be obtained from the Information Security and Digital Risk Officer at any time and from the Council's Information Handling Policy.

## 12. Data Processors

12.1 When a third party processes Personal Data on the Council's behalf the Council, as **Controller**, is obliged to have a written agreement with them. That person is known as a Processor. The main purpose of this requirement is to ensure that the data processor will keep the information as secure as the Council would, will be aware of and will comply with the instructions of the council, and will not use the information in any other fashion. Under UK GDPR, there are some additional requirements and the Council's contract documentation has been updated to reflect those.

12.2 All Directors will ensure that any new contracts entered into by their Service involving the handling of personal data are subject to written contracts containing the information required under UK GDPR. Further information on Data Processing

contract terms and conditions can be obtained from the Chief Officer – Legal and Procurement.

## 13. Information Sharing

13.1 Although processing of Personal Data must always be fair and lawful, data protection should not be perceived as a barrier to effective inter-agency and inter-departmental information sharing. There are many situations where information can, and indeed, must be shared, for example, to protect individuals.

13.2 Advice on the appropriateness of sharing can be obtained, at any time, from the Data Protection Officer. Services shall always, however, consider the following issues before such sharing occurs:

- What information needs to be shared?
- With whom?
- Why?
- How?
- What are the risks of not sharing the information?
- Could the same aim be achieved without sharing the data or by anonymising it?
- Is it necessary to undertake a Data Protection Impact Assessment

## 14. Data Protection Impact Assessments (DPIA)

14.1 DPIA is a process which enables the council to address the potential privacy risk and impact from collecting, using and disclosing of personal information as part of proposed new initiatives. DPIA will ensure data protection compliance and privacy concerns are appropriately addressed and enables **data protection by design** into projects and initiatives.

14.2 Conducting a DPIA is mandatory where data processing *"is likely to result in a high risk to the rights and freedoms of natural persons"*. This is particularly relevant when;

- new data processing technology is being introduced;
- large scale data sharing or processing activities;
- automated decision making

14.3 Services must engage and follow the requirements of the DPIA framework and complete the screening questions which will determine if an assessment is requried.

14.4 If a new project, process, module or the development or acquisition for the processing of personal data is planned or underway and a DPIA is not necessary there must still be compliance with the data protection principles and Assessment of Data Protection Compliance template completed.

## 15. Management of Data Incidents and Breaches

15.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

15.2 There is a duty on all organisations to report certain personal data breaches to the Information Commissioner. Commissioner) within 72 hours of becoming aware of the breach. 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.

15.3 Employees and Elected Members who become aware of a potential incident, must immediately report this to the DPO, in line with the Data Incident and Breach Management Procedures.

## 16. Relationship with Other Legislation

### 16.1 Human Rights Act 1998

16.1.1 Public authorities, such as the Council, must comply with the Human Rights Act 1998 ("HRA") in the performance of their functions. Section 6 HRA obliges public authorities to act in a manner which is compatible with the rights contained in the European Convention of Human Rights ("ECHR"). Article 8 ECHR affords everyone the right to respect for private and family life, including home and correspondence. Although this right is not absolute, any interference must be justified on the basis that it is lawful, necessary to pursue a legitimate aim and proportionate. This means that the interference should not be greater than is necessary to achieve the legitimate aim.

16.1.2 HRA is therefore a consideration when considering whether there is a justification for sharing information. Whilst data protection compliance may render an interference lawful, the Council must also consider whether information sharing exercises are necessary in the public interest or whether the same ends can be achieved by a less intrusive means. If there is a less intrusive alternative, the interference will be disproportionate.

16.1.3 The Council will ensure that an assessment of the necessity and proportionality of any proposed sharing arrangements is undertaken before such sharing takes place.

### 16.2 Freedom of Information (Scotland) Act 2002

The interface between data protection and the Freedom of Information (Scotland) Act 2002 ("FOISA") is complex. FOISA obliges the Council to be open and transparent, whereas data protection and HRA protect people's information and personal privacy.

Although FOISA provides the public with a right of access to all information held (unless covered by one of a number of fairly narrow exemptions), there is an absolute exemption from disclosure of information which would breach the data protection principles. Further information on how to deal with freedom of information requests without breaching data protection can be obtained from the Records Manager or the Chief Officer- Legal and Procurement.

## 17. Policy Breach

17.1 Breach of this policy may be regarded as a serious act of misconduct and may lead to disciplinary action. Employees must therefore make every effort to ensure that they understand their responsibilities under this policy.

17.2 It is a criminal offence under the DPA to knowingly or recklessly obtain, disclose or procure Personal Data without the consent of the Data Controller. The Council reserves the right to report any such offence to the Police, as well as the Information Commissioner.

## 18. Audit

Data protection procedures will be subject to routine internal audit by the DPO and by Internal Audit to ensure that an adequate level of compliance with this policy is being achieved.

## 19. Review

This policy will be reviewed on a two yearly basis, unless earlier review is deemed necessary by the DPO for any reason including legislative changes, revised guidance from the ICO, developing case law or a change in Council policy.

## 20. Further Information

Data Protection procedures and guidance are available on the Intranet. For further advice contact Data Protection Officer on 0141 577 3344 or DPO@eastrenfrewshire.gov.uk

## 21. Glossary of Definitions

| Definition | Meaning |
|---|---|
| **Controller** | Any person (or an organisation) who makes decisions (either jointly or in common with other organisations/persons) with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed |
| **Data Processing Agreement** | Ensures the "rules" of sharing have been clearly communicated and understood by all parties who are processing data on behalf of a Controller. Aims to ensure that methods of sharing, storing, use, in transit, backups, destruction, etc. are agreed before sharing is undertaken |
| **Data Subject** | Data subject means 'an individual who is the subject of personal data'. A data subject must be a living individual. |
| **Information Asset Register** | An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and used efficiently to help the Council provide a service. Information assets have recognisable and manageable value, risk, content and lifecycles. Maintaining an Information Asset Register (IAR) is a requirement of the UK GDPR. The IAR is a simple way to help Council Officers understand and manage the Council's information assets and the risks around those assets. |
| **Information Sharing Protocol** | Is a commitment and agreement between controllers to put in place the arrangements required to ensure secure and appropriate sharing of information and data between organisation, whilst maintaining the controls that give assurances and accountability and respects the right to privacy. |
| **Processing** | The definition of processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| **Personal Data** | 'Personal data' means any information relating to an identified or identifiable living person ('data subject' see below). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living person. |
| **Personal Data Breach** | a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed. |
| **Processor** | is anyone, other than an employee of the controller, who processes Personal Data on the data controller's behalf. |
| **Special Category Data** | is an additional category of personal data, replacing "Sensitive Personal Data" and includes information on racial or ethnic origin, religion, political opinions, religious beliefs, details of physical or mental health or condition, sexual life or details of any offence. This type of data is subject to much stricter conditions of processing. Personal data relating to criminal convictions and offences are not included within special category data per se but similar extra safeguards apply to its processing |
| **Third Party** | Any individual/organisation other than the data subject, the controller or its agents. |

## Appendix 1 - Information Governance Framework


| | Data Protection | Open Data/Freedom of Information | Information Security | Records Management | Data Quality |
|---|---|---|---|---|---|
| **Roles and Responsibilities** | Everyone will understand the importance of handling information correctly, sharing it appropriately and protecting it from improper use. The Data and Digital Governance Group is responsible for implementing the Information Governance framework | | | | |
| **Policies and Procedures** | For each top-level framework, there is a policy setting out the council's rules, requirements and responsibilities. All those handling information will adhere to these policies at all times. There will be documented procedures to support agreed policies. These will specify any operational instructions required to ensure compliance with legislation and standards | | | | |
| **Training and Awareness** | There will be a planned approach to training and awareness for each policy. This will be role-based, regularly assessed and will equip each person to fulfil their responsibilities | | | | |
| **Information Risk** | Information risk will be continuously managed. There will be robust processes in place to report information losses, security breaches and incident management and escalation | | | | |
| **Lifecycle management** | Proportionate and effective processes, systems and guidance will be implemented to manage the lifecycle of data and information | | | | |
| **Monitoring and Assurance** | There will be timely and effective monitoring, reporting and assurance | | | | |

## Appendix 2 – Data Governance Structure