EAST RENFREWSHIRE COUNCIL

DATA PROTECTION POLICY

VERSION 2.0 May 2018

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 From 25 May 2018, the data protection regime in the UK comprises the provisions of the EU General Data Protection Regulation ("GDPR"), a new domestic act- the Data Protection Act 2018 ("DPA18") and associated regulations. The previous domestic legislation, the Data Protection Act 1998 ("DPA98") is repealed.

1.4 GDPR 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. Some definitions in GDPR are slightly different to those in the Data Protection Act 1998. These are as follows:-

"Controller", previously known as "Data Controller" means the organisation who determines the purposes and means of processing
"Processor", previously known as "Data Processor" is anyone, other than an employee of the controller, who processes Personal Data on the data controller's behalf.
"Processing" still covers anything which can be done with Personal Data, from collecting, storing, recording or altering it to disclosing and destroying it.
"Personal Data" is information relating to a living individual who can be identified directly or indirectly from it.
"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. Like sensitive personal data and the DPA98, there are some stricter rules in the GDPR for lawful processing of Special Category Data.
"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 transmitted, stored or processed.

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.

In addition to the Data Protection Policy, key Council documents include:

Information Handling Protocol
Records Management Plan,
Freedom of Information Policy,
Data Protection Guidelines,
Subject Access Request Guidelines,
Information Security Policy; and
ICT Acceptable Use Policy.
Data Incident and Breach Management procedures

This list is not exhaustive and all relevant data protection and wider information governance guidance can be obtained from the GDPR section on the Council's intranet 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 The Data Protection Principles

3.1 Under 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.

3.2 The Council is fully committed to complying with the Data Protection Principles. As such, the Council undertakes that Personal Data will:-

3.2.1. **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.

3.2.2. **Be 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.

3.2.3. **Be 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

3.2.4. **Be 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.

3.2.5. **Be 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 stated retention period.

3.2.6. **Be 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.

3.3 In addition, under GDPR, the Council now needs to be able to demonstrate compliance with these principles. This is referred to as "accountability".

4. Data Protection Governance Arrangements

4.1 Corporate Responsibility

The Council has a corporate responsibility for data protection, and is defined as a "Controller" under GDPR. 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 1 to this Policy.

4.2 SIRO and Corporate Management Team

4.2.1 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 Data and Information Manager and the Chief Officer – Legal and Procurement. These officers will report directly to the SIRO on information governance issues including data protection on a monthly basis, and more regularly, as necessary.

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

4.3 Statutory DPO

4.3.1 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;

- Advise on Data Protection Impact Assessments;

- Train staff

- Conduct internal audits

- Be the first point of contact for the regulator; and

- Have due regard to the risk associated with the Council's processing operations.

4.3.2 The Data and Information Manager is the Council's DPO. The Information Security and Digital Risk Officer will deputise for the Data and Information Manager in the event that he/she is unable to fulfil those duties for any temporary period. Although both posts currently lie within Corporate and Community Services and report on a day to day basis to the Head of ICT and Digital Enablement, the Council will ensure that the DPO has sufficient independence to properly undertake the above tasks and reports directly to the Corporate Management Team in matters relating to Data Protection.

4.3.3 The DPO will be supported in carrying out their role by the Service data protection officers.

4.4 Senior Management Teams and Service Data Protection Officers

4.4.1 Each Service and its senior management team will be responsible for ensuring compliance with the provisions of GDPR / DPA18 within their own department. The Service Director will bear ultimate responsibility for compliance within their service area.

4.4.2 All Services are required to nominate a Service data protection officer (or officers) of appropriate seniority and a deputy.

4.4.3 The main role of the Service data protection officer will be to ensure compliance within his/her Service, by supervising the handling of Service specific subject access requests, passing on advice and training and maintaining the accuracy of the Service's entries into the Council's Information Asset Register, detailed in paragraph 6.1. The DPO will maintain an up to date list of Service data protection officers. Service data protection officers will also attend meetings of the Data Protection Working Group which will generally meet on a quarterly basis.

4.5. Employees and Elected Members

4.5.1 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 and Chief Officer- Legal and Procurement.

4.5.2 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 DPO, the Head of ICT and Digital Enablement and the Chief Officer – Legal and Procurement.

4.5.3 The Records Manager will 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. Requests relating to a single Service are the responsibility of that Service.

4.5.4 The Chief Officer - Legal and Procurement and his staff will offer ad hoc advice on data protection issues upon request and will proactively bring developments in the law to the attention of Council staff. Information will be cascaded via the Data Protection Working group and by publishing guidance documentation on the Council's intranet.

4.5.5 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, maintaining the Council's Information Security log and leading on information security incident management.

4.6 Governance and Working Groups

Each Service data protection officer is a member of the Data Protection Working Group ("DPWG"), which meets quarterly and is chaired by the Chief Officer – Legal and Procurement. The members of the DPWG each have the responsibility of disseminating training and good data protection practice throughout their service. The remit of the DPWG is to discuss compliance across the various Council services, to pass on advice and training, and to contribute to the ongoing development of corporate policy, procedure and guidance.

5. Notification

5.1 *The DPA98 required all Data Controllers who were processing Personal Data to notify the Information Commissioner. The Information Commissioner maintained a public register of Data Controllers who had notified. Each register entry included the name and address of the Data Controller and a general description of how they processed Personal Data and for what purposes. Individuals could consult the register to find out what Personal Data a particular Data Controller processed. Failure to notify was a criminal offence. GDPR changes this and removes the requirement to notify.*

5.2 Under regulations (the Data Protection (Charges and Information) Regulations 2018) Controllers still need to pay the ICO a fee, dependent on the size of the organisation. The ICO has produced guidance on the new fee structure. The DPO shall ensure that prompt payment of any relevant fee is made on behalf of the Council as and when required.

6. Documentation of Processing Activities

6.1 *Although there is no longer a notification requirement, Controllers are obliged to document their processing activities under GDPR. There are some similarities between this new obligation and the information previously provided to the ICO for notification*. 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 Head of ICT and Digital Enablement shall maintain the Council's IAR. This contains details of the Council's information assets, how those were obtained, how they are being used and who they are shared with. It is the responsibility of Service data protection officers to update the IAR and ensure that the entry for their Service is accurate at all times. The IAR is hosted on the Council's intranet.

7. Data Subject Rights

7.1 *Data subjects have several significant rights under GDPR, which are as follows:-*

- *Right to be informed;*
- *Right of access;*
- *Right to rectification of inaccurate data;*
- *Right to erasure in certain circumstances;*
- *Right to object to certain processing, including the right to prevent processing for direct marketing;*
- *Right to prevent automated decision-making;*
- *Right to data portability; and*
- *Right to claim compensation for damages caused by a breach*

7.2 Staff can obtain further information on these rights by reading the Council's Data Protection Guidelines on the intranet. Advice can also be obtained at any time from the DPO and/or Chief Officer – Legal and Procurement. The Council will

respond to any requests to exercise these rights without undue delay and, in any event, no later than one calendar month 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.

7.3 Further information on compliance with all data subject rights, particularly subject access rights, can be obtained from the Council's Subject Access Request guidelines, available on the Council's intranet, or from the Chief Officer – Legal and Procurement.

8. Training and Guidance

8.1 The Data Protection Working Group will prepare and revise detailed guidelines on the practicalities of dealing with GDPR and oversee the development and implementation of a Data Protection Learning and Development Strategy. The purpose of this strategy is to ensure that the learning and development needs of individual groups in relation to data protection and wider information governance are adequately addressed. The strategy shall identify the training needs of Elected Members, Directors and Heads of Service, other managers, employees who have specific requirements and those who require only a general awareness.

8.2 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. Data Retention

9.1 *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*.

9.2 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.

9.3 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.

10. Information Security

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

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

10.3 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.

10.4 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.

10.5 Employees and Elected Members who become aware of a potential breach of information security, such as a loss of data, must immediately report this to the DPO, in line with the Data Incident and Breach Management procedures.

10.6 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.

11. Data Processors

11.1 When a 3rd 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 GDPR, there are some additional requirements and the Council's contract documentation has been updated to reflect those.

11.2 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 GDPR. Further information on Data Processing Agreements can be obtained from the Chief Officer – Legal and Procurement.

12. Information Sharing

12.1 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.

12.2 Advice on the appropriateness of sharing can be obtained, at any time, from Legal Services. 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?

13. Data Protection Impact Assessments

13.1 *The Council has conducted some Privacy Impact Assessments (PIAs) under the DPA98 as a matter of good practice. PIAs are carried out for any new initiatives or changes of business practice involving Personal Data where the processing entails some possible risk to the individual's privacy.*

13.2. The purpose of the PIA was to identify any potential and likely effect on privacy; and to minimise and manage the identified impact and privacy risks.

13.3 GDPR replaces PIAs with Data Protection Impact Assessments (DPIAs) and makes them mandatory, rather than just good practice. Like PIAs, this is a process which enables the Council to address the potential privacy risk and impact from the collection, use and disclosure of Personal Data as a result of new initiatives and to ensure means are in place to make sure data protection compliance and privacy concerns are addressed appropriately. *Advice on and assistance with carrying out DPIAs can be obtained from the DPO*.

13.4 All DPIAs shall be conducted using the standard Council template. Service data protection officers will oversee the completion of DPIAs within their service area and shall ensure that the results of the assessment are reflected in the IAR if the processing goes ahead.

14. Special Categories of Personal Data and Criminal Convictions etc Data

14.1 **Appropriate policy**

In terms of the provisions of the new Data Protection Act, 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 Section3 above and indicate the process of retention and erasure.

14.2 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.

14.3 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

15. Relationship with Other Legislation

15.1 Human Rights Act 1998

15.1.1 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.

15.1.2 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.

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

15.2 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.

16. Breach

16.1 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.

16.2 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.

17. 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. Recommendations by Internal Auditors shall be considered by the relevant service and the DPO who shall liaise in determining the response to any recommendations made.

18. 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 or developing case law.

Appendix 1 – Data Governance Structure