Renfrewshire Council

To: Finance & Resources & Customer Services Policy Board

On: 28 March 2018

Report by: Director of Finance and Resources

Heading: Data Protection Policy

1. **Summary**

1.1 The Data Protection Act 1998 ("DPA") has regulated the processing of personal data and imposed obligations on the Council, as a data controller, since 1 March 2000. In response to this, the Council first introduced a Data Protection Policy in June 2001, outlining roles and responsibilities for data protection compliance. The policy is subject to two –yearly review. Although the most recent revisals were approved by the Finance & Resources Policy Board on 24 August 2016, a review is required in advance of 25 May 2018 when the EU General Data Protection Regulation ("GDPR") comes into force. The revisals reflect the changes to data protection law made by GDPR.

2. **Recommendations**

2.1 It is recommended that the Council approve the revised Data Protection Policy, which forms Appendix 1 to this report, and agree that the revisals come into force on 25 May 2018 and continues to be reviewed on a two yearly basis.

3. **Background**

3.1 The Council is committed to data protection compliance and first approved a Data Protection Policy in June 2001. The purpose of a Data Protection Policy is to outline roles and responsibilities for Data Protection compliance. The Director of Finance and Resources is the Senior Information Risk Owner (SIRO) for the Council. GDPR requires the Council to have a statutory officer, known as the Data Protection Officer. This role is discharged by the Managing Solicitor (DPO). Finance and Resources therefore take the overall lead in Data Protection and wider Information Governance matters. However, each Service and its senior management are obliged to retain a responsibility for data protection compliance. Given this devolved responsibility, each Service has a nominated data protection officer or officers. Service data protection officers are members of the Council's Data Protection Working Group, which meets quarterly. The role of the Service data protection officer is to ensure data protection compliance within their Service, albeit advice can be obtained from the Information Governance team, at any time.

3.2 Although the policy continues to devolve responsibility to Services for departmental compliance, it also reflects the statutory role of the Managing Solicitor (DPO) and provides that the post-holder will support the Director of Finance and Resources, in the role of SIRO, by assuming everyday responsibility for information governance.

3.3 Data protection is not new. Although it is a complex area of law, its ethos is simple – it protects people's personal information. Compliance with the DPA is a good foundation for GDPR compliance. There were eight data protection principles, which formed the core of the DPA and regulate how and when personal data should be processed by data controllers, such as the Council. These principles cover the collection, maintenance and security of personal data. GDPR contains six principles, which are similar.

3.4 GDPR does, however, introduce a number of important changes. It introduces some new rights for individuals and enhances some existing rights, which are reflected in the revised policy. For example, the £10 fee for subject access requests is abolished and the Council must comply with any such request within one calendar month, rather than 40 calendar days. Notifying serious information security breaches to the Information Commissioner becomes mandatory, rather than voluntary. Notably, the maximum penalty for getting data protection wrong increases from £500,000 to 20 million Euros.

Implications of the Report

1. **Financial** – none.

2. **HR & Organisational Development** – HR & OD are assisting with training in and awareness of GDPR, by facilitating the launch of a GDPR specific iLearn module.

3. **Community Planning –** N/A

4. **Legal** – this Policy ensures compliance with the provisions of the EU GDPR, which is the most significant change to data protection legislation in twenty years..

5. **Property/Assets** – none.

6. **Information Technology** – ICT are essential to the successful implementation of GDPR, given their information management function and their lead role in relation to the Council's Information Asset Register.

7. **Equality & Human Rights** - The Recommendations contained within this report have been assessed in relation to their impact on equalities and human rights. No negative impacts on equality groups or potential for infringement of individuals' human rights have been identified arising from the recommendations contained in the report. This policy seeks to ensure compliance with individuals' information rights. If required following implementation, the actual impact of the recommendations and the mitigating actions will be reviewed and monitored, and the results of the assessment will be published on the Council's website.

8. **Health & Safety** – none.

9. **Procurement** – none.

10. **Risk** – this Policy supports the management of information risk, such as a potential breach of GDPR. Compliance is addressed on the Council's corporate risk register to ensure that key milestones are met and the Council is fully compliant.

11. **Privacy Impact** – the Council has conducted Privacy Impact Assessments (PIAs) for some time, as good practice in relation to projects or initiatives which involve processing personal information in new ways and have a potential privacy impact. GDPR makes PIAs,

which will be known as Data Protection Impact Assessments (DPIAs) mandatory.

12. **Cosla Policy Position**

List of Background Papers

N/A

Author: *Allison Black, Managing Solicitor (DPO)*
0141 618 7175
Alison.Black@renfrewshire.gov.uk

Renfrewshire Council

Data Protection Policy

Document History

Version	Date	Author	Reason for Issue/Change
1	June 2001	Craig Geddes, Archivist	
2	June 2012	Allison Black, Assistant Managing Solicitor	New governance arrangements
3	August 2014	Heather Semple Solicitor (Information Governance)	2-yearly update
4	August 2016	Heather Syme, Senior Solicitor (Information Governance)	2-yearly update

Document Review and Approval

Name	Action	Date	Communication
Andrew Connor, Records Manager	Consulted	March 2018	Email
Data Protection Working Group	Consulted	March 2018	Email

Related Documents

Ref	Document Name/ Version	Document Location
1	Guidance on Responsible Use of Personal Data and Confidential Information	

2	Records Management Policy	
3	Freedom of Information Policy	
4	Data Protection Guidelines	
5	Subject Access Request Guidelines	
6	Information Security Policy	
7	ICT Acceptable Use Policy	
8	Information Handling Policy	

Title	Data Protection Policy
Author	Allison Black
Issue Date	May 2018
Subject	Data Protection
Description	Renfrewshire Council's policy on data protection and issues surrounding data protection to ensure compliance with GDPR
Version	5.0
Source	Version 2 of the Data Protection Policy by Allison Black in August 2012
Updating Frequency	Two Yearly unless required earlier due to legislative change
Right	Not Protectively Marked.
Category	Data Protection

1. Introduction

1.1 The Council needs to collect and use information about people to discharge its functions. This Personal Data must be handled properly and lawfully and the Council is committed to data protection compliance and has signed the Information Commissioner's 'Information Promise'.

1.2 Although data protection legislation is complex, its ethos is simple. It does what its title suggests and protects people's Personal Data by regulating the way in which organisations, such as the Council, handle this. In other words, it is legislation to regulate the processing of Personal Data.

1.3 The Data Protection Act 1998 ("DPA") has imposed obligations on the Council, as a data controller, since 1 March 2000. However, as of 25 May 2018, the EU General Data Protection Regulation ("GDPR") is in force and is the biggest change to data protection law in twenty years.

1.4 GDPR introduces a number of key changes, which are reflected in this Policy.

1.5 It is impossible to understand data protection without an awareness of some of the key definitions. Some definitions in GDPR are slightly different to those in the DPA. 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 simply collecting or storing, recording, altering, to actively disclosing this and includes verbal, as well as written exchanges, information left on desks or in confidential waste bags.

"**Personal Data**" is information relating to a living individual who can be identified directly or indirectly from this. This means that even just an address can be Personal Data if it can indirectly identify someone.

"**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 DPA, 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 Data Protection Principles

There were eight data protection principles, which were at the core of the DPA, and regulated when and how Personal Data should be processed. Under GDPR, there are six such principles, which are similar and like the DPA principles, cover rules for the maintenance, collection and security of personal data. The Council is committed to complying with the Data Protection Principles.

As such, the Council undertakes that Personal Data will:

1. Be processed fairly and lawfully and transparently.
2. Be collected and processed only for one or more specified, explicit and legitimate purpose(s).
3. Be adequate, relevant and limited to what is necessary.
4. Be accurate and kept up to date and that inaccurate data will be erased or rectified without delay.
5. Be kept for no longer than is necessary.

6. Be processed with appropriate security and use adequate technical and organisational measures to prevent unauthorised or unlawful processing or accidental loss, destruction of, or damage to Personal Data.

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

1.7 The Council, in recognition of its data protection obligations, first approved a Data Protection Policy in June, 2001. 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:

- Guidance on Responsible Use of Personal Data and Confidential Information,
- Information Handling Policy
- Records Management Policy,
- Freedom of Information Policy,
- Data Protection Guidelines,
- Subject Access Request Guidelines,
- Information Security Policy; and
- ICT Acceptable Use Policy.

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

2. Scope

This policy applies to all Services, employees and Elected Members of Renfrewshire Council and its Joint Committees and covers all Personal Data and Special Category Data which they process. It may, however, be read

alongside other Council policies and guidelines on use of non-personal data and wider information governance issues.

3. Data Protection Governance Arrangements

3.1 Corporate Responsibility

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

3.2 Corporate Management Team and SIRO

The Director of Finance and Resources is the Senior Information Risk Owner ("SIRO") for the Council. The SIRO is supported in this role by the Managing Solicitor (DPO). The Managing Solicitor (DPO) reports to the Director of Finance and Resources, as SIRO, on information governance issues, including data protection, on at least a monthly basis, and more regularly, as necessary. The SIRO reports to the CMT on at least a six monthly basis.

3.3 Statutory DPO

The GDPR obliges the Council to 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 and
- 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.

3.4 SMTs

3.4.1 Each Service and its senior management will retain a departmental responsibility for ensuring compliance with the provisions of the DPA.

3.4.2 All Services are required to nominate a departmental data protection officer or officers of appropriate seniority and a depute.

3.5. Employees

3.5.1 All employees and Elected Members are individually responsible for ensuring that the processing of Personal Data is in accordance with GDPR and should familiarise themselves and comply with Council data protection guidance. Advice can be obtained at any time from Information Governance Team.

3.5.2 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 Managing Solicitor (DPO).

3.5.3 The main role of the Service data protection officer will be to ensure compliance within his/her Service, by dealing with 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 5.1. The Records Manager will maintain an up to date list of Service data protection officers.

3.5.4 The Records Manager will have a co-ordinating role in relation to Subject Access Requests and will process any cross departmental subject access requests and any Finance and Resources requests. Although requests relating to only one Service are the responsibility of that Service, subject to any guidance from the Records Manager and the Information Governance Solicitors, the Records Manager will have oversight of all subject access requests.

3.5.5 The Information Governance Team will offer ad hoc advice on data protection issues.

3.5.6 The Senior Solicitor (Information Governance) 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..

3.5.7. Cyber security and technical information security issues, including compliance with industry standards, are dealt with by the Council's Cyber Security Architect and Cyber Security officer, within the Enterprise Architecture Team in ICT Services. Responsibility for information management, which promotes efficiency when the Council processes information and extends beyond the processing of Personal Data, also lies with the Enterprise Architecture Team within ICT Services will promote good information management by the provision of advice and guidance to Services.

3.6 Governance Groups and Working Groups

3.6.1 Each Service data protection officer is a member of the Data Protection Working Group ("DPWG"), which meets quarterly and is chaired by the Records Manager. The members of the DPWG each have the responsibility for dealing with data protection issues within their department and disseminating training and good data protection practice throughout their department. The remit of the DPWG is for each of these officers to discuss compliance within their department, pass on advice and training, and the processing of subject access requests which relate to records from their departments.

3.6..2 The DPWG operates as a sub group of the Information Management Governance Group ("IMGG"), which is jointly chaired by the Enterprise Architect and Managing Solicitor (DPO). The Records Manager and Senior Solicitor (Information Governance) are also members of the IMGG. The IMGG consists of key officers with information management and information governance expertise. Although the remit of IMGG extends to wider information management and information governance issues, the Managing

Solicitor (DPO), as co-chair, on behalf of the SIRO, will have the opportunity to manage and direct the agenda of IMGG to promote and progress the Council's information governance agenda. The Records Manager shall provide regular updates to the IMGG on the work of the DPWG.

3.6.3 The Information Security Group ("ISG"), which is chaired by the Chief Auditor and attended by the Managing Solicitor (DPO) and Senior Solicitor (Information Governance), also operates as a sub-group of the IMGG. The remit of the ISG is to support IMGG to ensure that information security is appropriate, proportionate, measured and embedded into business as usual. Membership of the ISG includes appropriate representation from ICT and Internal Audit.

4. Notification

4.1 The DPA required all Data Controllers who are processing Personal Data to notify the Information Commissioner of this. The Information Commissioner maintained a public register of Data Controllers who have notified. Each register entry includes the name and address of the Data Controller and a general description of how they process Personal Data and for what purposes. Individuals could consult the register to find out what Personal Data a particular Data Controller processes. Failure to notify was a criminal offence.

4.2 GDPR changes this and removes the requirement to notify. However, a provision in the Digital Economy Act means that 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, which was laid before Parliament at the end of February 2018..

5. Documentation of Processing Activities

5.1 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 will form the basis of the Council's documentation of processing activities.

5.2 The Enterprise Architecture Team within ICT Services maintain the Council's Information Asset Register (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 his/her Service is accurate at all times.

6. Data Subject Rights

6.1 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

6.2 Further information on those rights is available in the Council's Data Protection Guidelines and intranet and advice can be obtained at any time from the Information Governance Team. The right most frequently used by Council service users is likely to be the right of access, i.e. the right of an individual to access his/her own Personal Data. Under GDPR, the Council has one a

maximum of one calendar month instead of 40 calendar days to comply with subject access requests. The maximum £10 fee which was chargeable under the DPA has been abolished by GDPR and so, this is now free of charge. 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 Records Manager.

6.3 The Information Governance Team has responsibility for maintaining the Council's subject access request guidelines.

7. Training and Guidance

7.1 The Information Governance Team will continue to prepare and revise detailed guidelines on the practicalities of dealing with GDPR and oversee the implementation of the Council's Information Governance/ 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 identifies the training needs of Elected Members, Directors and Heads of Service, 3rd and 4th tier managers, employees who have specific requirements and those who require only a general awareness.

The existing guidelines, available from the Information Governance Team, or on the information governance section of the Council's intranet, familiarise officers with data protection compliance and the importance of information security and take account of guidance issued by the Information Commissioner, who enforces data protection.

8. Data Retention

8.1 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. 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.

8.2 The Records Manager, as outlined in the Council's Records Management Policy, provides advice on records management and retention issues.

8.3 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. This will ensure compliance with the fifth data protection principle.

9. Information Security

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

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

9.3 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.

9.4 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, even extending to conversations between individuals.

9.5 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 Information Governance Team, in line with the Information Security Incident Reporting Procedures.

9.6 Further information and advice on information security can be obtained from the Information Governance Team at any time and from the Council's Information Handling Policy and regular 'Think Twice' bulletins.

10. Data Processors

If someone, other than an employee of the Council, is processing Personal Data on the Council's behalf, for example, a contractor, the Council, as Controller, is obliged to have a written agreement with the Processor. Under the DPA, the main purpose of this was to ensure that the data processor would comply with the seventh principle by keeping that information as secure as the Council would. In other words, there should be a written agreement that appropriate technical and organisational measures would be taken by the contractor to keep the Personal Data adequately secure. Under GDPR, there are some additional requirements and the Council's contract documentation has been updated to reflect those. Further information on Data Processor Agreements can be obtained from the Information Governance Team.

11. Information Sharing

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. Detailed guidance on information sharing is available in the Council's Data Sharing Code and advice can be obtained, at any time, from the Information Governance Solicitors. Consideration should, however, be given to the following:

- 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?

12. Data Protection Impact Assessments

12.1 The Council have conducted Privacy Impact Assessments (PIAs) under the DPA for some time, as a matter of good practice. PIAs are carried out for any new initiatives or changes of business practice involving Personal Data.

12.2 The Corporate Management Team (CMT) have instructed, for some time, that where policies and decisions have implications for the use of Personal Data held by the Council then all Services must conduct a PIA as an integral part of any project planning process rather than an add-on. Its purpose is to:

- Identify any potential and likely impact on privacy; and
- Minimise and manage the identified impact and privacy risks.

12.3 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.

12.2 Advice on and assistance with carrying out DPIAs can be obtained from the Information Governance Team.

13. Relationship with Other Legislation

13.1 Human Rights Act 1998

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.

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 before an interference with Article 8 privacy rights can be justified. If there is a less intrusive alternative, the interference will be disproportionate.

13.2 Freedom of Information (Scotland) Act 2002

The interface between the 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 this is covered by one of a number of fairly narrow exemptions, there is an absolute exemption from disclosure for information, disclosure of which would breach the data protection principles. Further information on the Personal Data exemption under FOISA and how to deal with freedom of information requests without breaching data protection, can be obtained from the Freedom of Information Guidance Manual, available from the Council's intranet, or the Records Manager and legal advice can be obtained at any time from the Information Governance Solicitors.

14. Breach

14.1 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.

14.2 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.

15. Audit

Data protection procedures are subject to routine internal and external audit and recommendations implemented accordingly.

16. Review

This policy will be reviewed on a two yearly basis, unless earlier review is required due to legislative changes. However, to ensure ongoing data protection compliance, any developments, significant cases, guidance from the ICO, or other lessons learned in this area, will be used to inform best practice.