Renfrewshire Council

To: Finance & Resources Policy Board

On: 24 August 2016

Report by: Director of Finance and Resources

Heading: Data Protection Policy

1. **Summary**

1.1 The Data Protection Act 1998 ("DPA") regulates the processing of personal data and imposes obligations on the Council, as a data controller. It is, therefore, important that the Council makes proper provision for the way in which it handles personal data. The DPA came into force on 1st 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. As the most recent revisals to the Policy were approved by the Finance & Resources Policy Board on 27 August 2014, the two-yearly review is now due. The revisals are minor and simply reflect the current Information Governance arrangements within the Council.

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 this continued to be reviewed on a two yearly basis.

3. **Background**

3.1 Although the DPA is complex, the ethos is simple – it is legislation to protect people's personal information. There are eight data protection principles, which form the core of the DPA and regulate how and when personal data should be processed by data controllers, such as the Council.

3.2 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. 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.

3.3 Although the policy continues to devolve responsibility to Services for departmental compliance, it also provides that the Head of Corporate Governance will support the Director of Finance and Resources, in the role of SIRO, by assuming overall responsibility for information governance and reflects the arrangements to facilitate this.

Implications of the Report

1. **Financial** – none.

2. **HR & Organisational Development** – none.

3. **Community Planning –** N/A

4. **Legal** – this Policy ensures compliance with the provisions of the Data Protection Act 1998.

5. **Property/Assets** – none.

6. **Information Technology** – none.

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. 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 the Data Protection Act 1998.

11. **Privacy Impact** - none

List of Background Papers

N/A

Author: *Heather Syme, Senior Solicitor (Information Governance)*
0141 618 7022
heather.syme@renfrewshire.gcsx.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
Allison Black, Managing Solicitor (Information Governance)	Consulted	May 2016	Email
Joseph Bartoletti, Records Manager	Consulted	May 2016	Email
Francis Lannie, Information Governance Development Officer	Consulted	May 2016	Email
Data Protection Working Group	Consulted	May 2016	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	

Title	Data Protection Policy
Author	Heather Syme
Issue Date	August 2016
Subject	Data Protection
Description	Renfrewshire Council's policy on data protection and issues surrounding data protection to ensure compliance with the Data Protection Act 1998.
Version	4.0
Source	Version 2 of the Data Protection Policy by Allison Black in August 2012

Updating Frequency	Two Yearly.
Right	Not Protectively Marked.
Category	Data Protection

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 compliance with the Data Protection Act 1998 ("DPA") and has signed the Information Commissioner's 'Information Promise'.

1.2 Although the DPA is a complex piece of legislation, 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 It is impossible to understand the DPA without an awareness of some of the key definitions.

"**Processing**" covers anything which can be done with Personal Data, from simply collecting or storing, 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 from that data alone, or from that data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller. This means that even just an address can be Personal Data if it can be used with other information held to identify someone. The definition of "personal data" explicitly includes any expression of intention or opinion about the individual, who is known as the "data subject".

"**Sensitive Personal Data**" is an additional category of 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. There are some stricter rules in the DPA for lawful processing of sensitive personal data.

"**Data Controller**" is the organisation, such as the Council, who determines how Personal Data will be used.

"**Data Processor**" is anyone, other than an employee of the data controller, who processes Personal Data on the data controller's behalf.

1.4 The Council undertakes to comply with the eight data protection principles, which are at the core of the DPA, and regulate when and how Personal Data should be processed.

As such, the Council undertakes that Personal Data will:

1. Be processed fairly and lawfully.
2. Be obtained and processed only for one or more specified purpose(s).
3. Be adequate, relevant and not excessive.
4. Be accurate and kept up to date.
5. Be kept for no longer than is necessary.
6. Be processed in accordance with the rights of the data subject.
7. Be processed with due regard to security and adequate technical and organisational measures will be taken to prevent unauthorised or unlawful processing or accidental loss, destruction of, or damage to Personal Data.
8. Not be transferred to countries outwith the European Economic Area, unless special conditions are met.

1.5 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,
- 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 Sensitive Personal 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 "Data Controller" under the DPA.

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 Head of Corporate Governance and the Managing Solicitor (Information Governance). The Managing Solicitor (Information Governance) 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 will report to the CMT on at least a six monthly basis.

3.3 SMTs

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

3.3.2 All Services are required to nominate a departmental data protection officer or officers.

3.4. Employees

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

3.4.2 The Head of Corporate Governance will have 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 (Information Governance).

3.4.3 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 input into the Council's annual notification to the ICO, detailed in paragraph 4. The Records Manager will maintain an up to date list of Service data protection officers .

3.4.4 The Records Manager will have a co-ordinating role in relation to Subject Access Requests and will process any cross departmental subject access requests. 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.

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

3.4.6 The Senior Solicitor (Information Governance) has a key role in ensuring compliance with the seventh and eighth data protection principles relating to

data security by providing advice and guidance to Services on information security.

3.4.7. Responsibility for information management, which promotes efficiency when the Council processes information and extends beyond the processing of Personal Data, lies with ICT Services. The Enterprise Architecture Team within ICT Services will promote good information management by the provision of advice and guidance to Services.

3.5 Governance Groups and Working Groups

3.5.1 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, their departmental input into the Council's notification and the processing of subject access requests which relate to records from their departments.

3.5.2 The DPWG operates as a sub group of the Information Management Governance Group ("IMGG"), which is jointly chaired by the Technology Architect and Managing Solicitor (Information Governance). 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 (Information Governance), as co-chair, on behalf of the Head of Corporate Governance, 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.

3.5.3 The Information Security Group ("ISG"), which is chaired by the Chief Auditor and attended by the Managing Solicitor (Information Governance) 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, Legal Services and Internal Audit.

4. Notification

4.1 The DPA requires all Data Controllers who are processing Personal Data to notify the Information Commissioner of this. The Information Commissioner maintains 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 can consult the register to find out what Personal Data a particular Data Controller processes. Failure to notify is a criminal offence.

4.2 The Records Manager has the responsibility for maintaining the Council's notification. The Council's notification is renewed annually by the Records Manager.

4.3 Service data protection officers are responsible for reporting changes in processing to the Records Manager.

4.4 Elected Members require individual notifications. This is because they process Personal Data in three different capacities, which are as follows:-

- As a member of the Council, e.g. as a member of a Board
- As a representative of constituents, e.g. dealing with complaints.
- Representatives of a political party, e.g. campaigning.

When processing Personal Data as a member of the Council, Elected Members are covered by the Council's notification and when acting on behalf of their

political party, they are entitled to rely on the party's notification. However, when processing Personal Data on behalf of constituents, Members are Data Controllers in their own right, and so require a valid notification.

Members' Services will maintain notifications for all Elected Members.

5. Data Subject Rights

5.1 Data subjects have several significant rights under the DPA, which are as follows:-

- Subject access rights;
- The right to prevent processing that is likely to cause or is causing damage or distress;
- The right to prevent processing for direct marketing;
- The right to object to automated decision-taking;
- The right to have inaccurate data rectified, destroyed, blocked or erased; and
- The right to claim compensation for damages caused by a breach of the DPA.

5.2 The most significant of these rights is the right of subject access, i.e. the right of an individual to access his/her own Personal Data. The Council has 40 calendar days to comply with subject access requests. 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.

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

6. Training and Guidance

6.1 The Information Governance Team will continue to prepare and revise detailed guidelines on the practicalities of dealing with the DPA 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 data security and take account of guidance issued by the Information Commissioner, who polices the DPA.

7. Data Retention

7.1 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 the records which they hold, and to arrange for the secure destruction of data, in accordance with such schedules.

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

7.3 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.

8. Information Security

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

8.2 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.

8.3 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.

8.4 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.

8.5 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 Senior Solicitor (Information Governance), in line with the Information Security Incident Reporting Procedures.

8.6 Further information and advice on information security can be obtained from the Senior Solicitor (Information Governance) at any time.

9. 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 Data Controller, is obliged under the DPA to have a written agreement or contractual obligation that the data processor will comply with the seventh principle by keeping that information secure. In other words, there should be a written agreement that appropriate technical and organisational measures will be taken by the contractor to keep the Personal Data secure. Further information on Data Processor Agreements can be obtained from the Information Governance Team.

10. Information Sharing

Although processing of Personal Data must always be fair and lawful, the DPA 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?

11. Privacy Impact Assessments

11.1 Privacy Impact Assessment (PIA) 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.

11.2 The Cabinet Office and the Scottish Government recommend that PIAs be carried out for any new initiatives or changes of business practice involving Personal Data, as they believe that this will increase public confidence in the handling of Personal Data.

11.3 The Corporate Management Team (CMT) have instructed that where policies and decisions have implications for the use of Personal Data held by the Council then all Services must conduct a PIA.

The PIA must be 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.

11.4 Advice on and assistance with carrying out Privacy Impact Assessments can be obtained from the Information Governance Team.

12. Relationship with Other Legislation

12.1 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 compliance with the DPA 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.

12.2 Freedom of Information (Scotland) Act 2002

The interface between the DPA and the Freedom of Information (Scotland) Act 2002 ("FOISA") is complex. FOISA obliges the Council to be open and transparent, whereas the DPA 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 the DPA, 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.

13. Breach

13.1 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.

13.2 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.

14. Audit

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

15. Review

This policy will be reviewed on a two yearly basis. However, to ensure compliance with the DPA, any developments, significant cases, guidance from the ICO, or other lessons learned in this area, will be used to inform best practice.