PERTH AND KINROSS COUNCIL

Strategic Policy & Resources Committee

8 February 2017

DATA PROTECTION POLICY

Head of Legal & Governance Services

PURPOSE OF REPORT

To amend the Council's Data Protection Policy to implement external and internal audit recommendations and reflect current law and good practice in respect of use and management of personal data.

1. BACKGROUND / MAIN ISSUES

1.1 The current version of the Council's Data Protection Policy was approved in March 2014 and sets out our approach to compliance with the Data Protection Act 1998.

1.2 An internal audit in respect of information sharing and the subsequent report [Internal Audit Report 16-05] was considered by the Audit Committee on 28 September 2016. This report made a number of recommendations in respect of the current policy and processes, namely that the policy should be amended to include :-

- a definition of what is meant by "data sharing"
- clarification as to which officers may authorise data sharing
- a requirement to consult with and implement any advice from the Data Protection Officer with regard to Data Sharing Agreements

1.3 Furthermore, Internal Audit recommended that a corporate register of all data sharing protocols in place across the organisation should be kept by the Information Compliance Officer.

1.4 Audit Scotland carried out a review of data management within the Council in 2013 and recommended more consistent use of Privacy Impact Assessments. Whilst this is now being implemented in practice, the Data Protection Policy was not formally amended to reflect the operational changes. These amendments are now incorporated as part of the proposed policy changes.

2. PROPOSALS

2.1 The current Data Protection Policy has been amended to implement the recommendations made by Internal Audit Report 16-05, to provide clarity and consistency in respect of the use of Privacy Impact Assessments as recommended by Audit Scotland and to reflect current good practice. The proposed policy is attached at Appendix 1.

2.2 Other amendments to the Policy include: -

- Approval of non-material changes by the Head of Legal & Governance Services
- Clarification in respect of the delegation of a Director's responsibilities
- Minor textual updates.

3. CONCLUSION AND RECOMMENDATION(S)

3.1 It is important that the Council's policy reflects best practice and provides assurance to the public about the way personal information is handled.

3.2 The proposed Data Protection Policy implements audit recommendations and reflects best practice in line with guidance from the Information Commissioner.

3.3 It is recommended that the Committee approve the revised policy attached at Appendix 1.

Author(s)

Name	Designation	Contact Details
Donald Henderson	Information Compliance Manager	Ext: 77933

Approved

Name	Designation	Date
Jim Valentine	**Depute Chief Executive**	**11/01/2017**

If you or someone you know would like a copy of this document in another language or format, (on occasion, only a summary of the document will be provided in translation), this can be arranged by contacting the Customer Service Centre on 01738 475000.

You can also send us a text message on 07824 498145.

All Council Services can offer a telephone translation facility.

1. IMPLICATIONS, ASSESSMENTS, CONSULTATION AND COMMUNICATION

Strategic Implications	**Yes / None**
Community Plan / Single Outcome Agreement	**None**
Corporate Plan	**None**
Resource Implications	
Financial	**None**
Workforce	**None**
Asset Management (land, property, IST)	**None**
Assessments	
Equality Impact Assessment	**Yes**
Strategic Environmental Assessment	**Yes**
Sustainability (community, economic, environmental)	**Yes**
Legal and Governance	**Yes**
Risk	**None**
Consultation	
Internal	**Yes**
External	**None**
Communication	
Communications Plan	**Yes**

1. Strategic Implications

Community Plan / Single Outcome Agreement

1.1 n/a

Corporate Plan

1.2 n/a

2. Resource Implications

Financial

2.1 n/a

Workforce

2.2 n/a

Asset Management (land, property, IT)

2.3 n/a

3. Assessments

Equality Impact Assessment

3.1 The proposals have been considered under the Corporate Equalities Impact Assessment process (EqIA) and assessed as not relevant for the purposes of EqIA.

Strategic Environmental Assessment

3.2 The Environmental Assessment (Scotland) Act 2005 places a duty on the Council to identify and assess the environmental consequences of its proposals.

The proposals have been considered under the Act and no further action is required as it does not qualify as a PPS as defined by the Act and is therefore exempt.

Sustainability

3.3 n/a

Legal and Governance

3.5 The Head of Democratic Services has been consulted about the changes to the policy and, specifically, about the inclusion of Privacy Impact Assessments in the Committee report template and is in agreement with the proposals.

Risk

3.6 n/a

4. Consultation

Internal

4.1 The Policy & Governance Group, which comprises representatives of all the Services and key specialists, have reviewed and approved the proposed changes.

External

4.2 n/a

5. Communication

5.1 A detailed communications plan has been prepared for the introduction of Privacy Impact Assessments including briefings for Elected Members and key staff, information on the Council intranet, and awareness-raising material for staff in general.

The other changes to the policy will be highlighted separately to staff.

2. BACKGROUND PAPERS

n/a

3. APPENDICES

Appendix 1: Proposed Data Protection Policy

PERTH AND KINROSS COUNCIL

Data Protection Policy

Scope

The Data Protection Policy ('the DP policy') will apply to all employees and Elected Members of Perth & Kinross Council ('the Council'). The policy forms an integral part of the Council's Information Security Management System (ISMS).

Terms within this policy (e.g. 'personal information', 'subject access request') are used with the same intent as the definitions applied within the Data Protection Act 1998.

Violations of the policy may result in disciplinary action for an employee, referral to the Standards Commission for an Elected Member, and may constitute a criminal offence.

The policy is applicable to all personal data/information processed by the Council.

It is the Council's policy to fully comply with the Data Protection Act 1998 and all other related statutory, criminal and civil obligations to which the Council is required to adhere. This applies to the retrieval, storage, processing, retention, destruction and disposal of 'personal information'.

The policy will be reviewed every three years and, if appropriate, amended to retain its relevance. If at any time there is a need to bring forward changes to reflect statutory requirements or other developments that would be considered beneficial to the Council or the operation of the Policy, this will be done within the review period. Non-material changes will be approved by the Head of Legal & Governance Services.

Roles and Responsibilities

The Head of Legal & Governance Services is responsible for developing, publishing, maintaining and administering the data protection policy.

Service Senior Management Teams are responsible for all aspects of compliance with the Act, and associated legislation, within their Service.

The Head of Legal & Governance Services will designate a Data Protection Officer who will develop appropriate procedures, strategies, codes of conduct and guidance and will oversee a management framework with the purpose of controlling adherence to the Data Protection Act 1998 within the Council.

Role of Employees

Employees will only have access to personal information where that access is essential to their duties. Employees should discuss with their line manager any instance where access rights require clarification. Access rights are not to be regarded as permanent and are subject to change at any time depending upon the nature of the duties being fulfilled by an employee.

Employees with access to personal information must be familiar with the requirements of the Data Protection Act 1998.

Employees should only record information about an individual which is relevant, and should be aware that they may be required to justify what has been written and be prepared for that information to be released as part of a subject access request.

Any employee who is found to have inappropriately divulged personal information will be subject to investigation under the Council's disciplinary procedure, which may result in dismissal and possible legal action.

All employees must follow good practice as indicated by the Data Protection Act and any such codes of practice issued by the Office of the Information Commissioner, or the Council, when processing personal data.

Elected Members

Elected Members have no automatic rights to access personal information, except, for example, when acting as a member of a committee or acting on behalf of an individual or under their instruction. The requirement for access must be clearly demonstrated at all times.

Elected members are bound by the terms of the Act for the duration of their tenure of office. Elected members must, when their term of office expires or for some other reason they cease to be an elected member, arrange for the transfer or secure disposal of all personal information held by them or their support staff on their behalf. Where information is being transferred, the Head of Democratic Services, or their representative, in consultation with the Council's Data Protection Officer, will make the necessary arrangements for the transfer and future management of the information transferred.

Elected members are required to notify the Information Commissioner that they are data controllers. The Council will assist in this process and pay the associated fees.

Training

Data protection training is mandatory for all Elected Members and employees of the Council.

Service Senior Management Teams are responsible for ensuring that employees within their Service are trained appropriately.

The Data Protection Officer will assist Services in evaluating training needs and ensuring adequate resources are provided. Training materials will be developed in accordance with requirements.

Notification

The Council will ensure that it maintains its Notification entry with the Information Commissioner on an annual basis. Services will be responsible for providing an annual return on the use and processing of personal information within their Service, and for informing the Data Protection Officer of any amendments to the register entry as and when they occur.

The Data Protection Officer will be responsible for assisting Services in understanding the Notification process. A mechanism will be put in place to ensure the notification entry is reviewed regularly and kept up to date.

Subject Access

The Information Compliance Team is responsible for processing subject access requests on behalf of the Data Protection Officer.

All employees have a duty to assist a person in making a subject access request. Where a Subject Access request has been made by an individual, the employee who received the request should pass this to the Information Compliance Team immediately to ensure that the request can be processed within the statutory timescales.

Where information is requested by the Information Compliance Team as part of a Subject Access request, Services should provide this information intact and unaltered as soon as possible. The Data Protection Officer shall determine what, if any, information requires to be redacted in accordance with Data Protection legislation prior to release of the information.

Some subject access requests are complex and require an understanding of the individual or case to decide whether the information requested can be disclosed. In these instances, employees must cooperate with the Information Compliance Team in aiding the decision-making process by providing professional opinions and guidance.

The Council will endeavour to process all subject access requests within the statutory forty calendar day deadline. Where the Council is unable to process the request within the timeframe, the data subject should be notified as soon as possible of any potential delay, the reasons for such a delay, and the date when their information will be made available.

A fee of £10 will be applicable for subject access requests made by members of the public. The Information Compliance Team have the right to waive the fee where appropriate. This decision should be taken on a case by case basis, bearing in mind that the Council has adopted a policy on charging. The Council will not charge a fee for employees wishing access to information relating to them in the course of their employment. Employees wishing access to any other type of personal information, e.g. Council tax records, must do so as a private individual through the formal subject access procedure.

The Data Protection Officer will develop appropriate guidance and literature explaining the subject access procedure clearly and coherently.

Processing of Personal Information

The Data Protection Act applies to personal information processed by any forms of medium, including CCTV images, photographs, and digital images. Any processing of such data must be in accordance with the principles of the Data Protection Act and this policy.

Direct Marketing

The Council will not participate in direct marketing practices where individuals do not consent to the use of their personal information for this purpose.

All individuals must be given the opportunity to opt-in to receive material at the point of data collection, or opt-out of receiving material at the point of distribution.

The appropriate opt-in and opt-out mechanisms must be put in place where third party marketing or advertising materials are distributed to named individuals. In situations where this cannot be feasibly done, the materials must not be distributed.

Third Parties

Contracts for processing of information by a third party on behalf of the Council will require the insertion of confidentiality clauses and specific advice must be sought from the Head of Legal & Governance Services. The Council must be satisfied that the Information Security measures adopted by the third party are adequate before access to information is granted.

Compliance

The Data Protection Officer will ensure that the data protection policy is reviewed to ensure that it remains adequate, effective and compliant with current legislation. The Data Protection Officer will also review the application and operation of the policy and procedure across the Council on a regular basis.

Service Senior Management Teams will ensure that all data protection procedures are properly implemented within their area of responsibility.

All Council employees have a responsibility to report suspected breaches of the Data Protection policy to their own management or to the Data Protection Officer.

Data Sharing

The Council will comply with the Information Commissioner's statutory Data Sharing Code of Practice.

Data sharing occurs when personal data is passed to another organisation for its own purposes. It does not apply when the other organisation is processing the data on behalf of the Council e.g. under contract.

An appropriate written agreement for the sharing of data (known as a data sharing agreement or information sharing protocol) must be in place before personal information will be shared with other agencies. These protocols will be reviewed, amended and updated on a regular basis. Services must consult the Data Protection Officer prior to agreeing any information sharing protocol. An information sharing protocol must be approved by the Data Protection Officer and then signed by the relevant information asset owner (normally a Chief Officer).

The Data Protection Officer will maintain a register of all the Council's information sharing protocols.

Fair Processing

Individuals will be informed at the point their personal data is requested or recorded, of:

- The identity of the data controller (Perth and Kinross Council)
- Any organisation other than the Council with whom the information may be shared
- The purpose or purposes for which the data are or are intended to be processed

They will also be informed that additional information will be available via the Council's website or by contact with the Data Protection Officer.

Data Matching

The Council will comply with the Information Commissioner's guidance on data matching.

Privacy Impact Assessments

A Privacy Impact Assessment (PIA) will be undertaken to identify and minimise the privacy risks of new project or policy that will involve processing personal information. The Data Protection Officer will assist Services to identify the need for a PIA, guide employees through the assessment process when one is required, and help make recommendations to ensure the Council's duties under the Data Protection Act are adhered to. Information about completed PIAs will be published on the Council's website.

Records Management

All personal information must be processed in compliance with the Council's Records Management policy and associated procedures.

Complaints

Any complaints received regarding the Data Protection policy or its associated procedures, including subject access requests, should be handled through the Corporate Complaints system in the first instance.

Document History

Version	Summary of Changes	Approved	
v4	General review	SP&R	16 June 2004
v5	Responsibility changed from Depute Director of Corporate Services to Head of Legal Services following Corporate Core review	Policy & Governance OCIP Group	19 June 2008
v6	Scope changed to remove references to partner organisations, contractors and agents following internal audit review (covered within contracts) Reference to third party confidentiality agreements removed following internal audit review (covered within contracts) Reference to Article 10 Notices in Data Sharing section changed to "Fair Processing" in line with the terminology used in the Information Commissioner's new guidance	Head of Legal Services	7 December 2010
v7	Responsibility for processing subject access requests updated to Freedom of Information Team following recent change in process. Subject access section updated to reflect change.	EOT SP&R (Exec Sub)	4 February 2014 26 March 2014
V8	Minor textual changes to clarify definition of 'personal data', timescale for subject access request, and organisations involved in data sharing	Head of Legal Services	29 May 2015
V9	Clarification of data sharing and process for approving information sharing protocols (Internal Audit 16-05) Register of information sharing		

	protocols (Audit Scotland recommendation) Privacy Impact Assessments (Audit Scotland recommendation) Sentence about delegation of responsibilities removed. Fair processing notices to be “layered”. Non-material changes to be agreed by Head of Legal & Governance Services		