

**PERTH AND KINROSS COUNCIL****Executive Sub-Committee  
of the Strategic Policy and Resources Committee****26 March 2014****Data Protection Policy****Head of Legal Services****PURPOSE OF REPORT**

This report presents a revision to the Council's Data Protection Policy which takes account of changes in the way the Council processes requests for personal information.

**1. BACKGROUND**

- 1.1 The current version of the Council's Data Protection Policy was approved in December 2010. The policy sets out the Council's approach to compliance with the Data Protection Act 1998.
- 1.2 The proposals in this report were considered by the Executive Officer Team on 18 February 2014.

**2. PROPOSALS**

- 2.1 The proposed policy is attached as Appendix 1 with the changes highlighted on pages 3 and 4 under the heading Subject Access.
- 2.2 Centralising the processing of subject access requests has been under consideration for several years and a commitment has been given to the Office of the Information Commissioner that the current process would be reviewed following some highlighted failings.
- 2.3 Currently, subject access requests may be received by any Service. The request should then be processed by the receiving Service, liaising with other Services for information as necessary. Some requests are received directly by the Information Compliance Section in Legal Services and are dealt with centrally; others are passed to Information Compliance because of the likely complexity or volume.
- 2.4 Those dealing with requests in Services frequently refer to Information Compliance for advice since Data Protection is a minor part of their responsibilities. It is recognised, as a consequence, that requests are dealt with to varying standards across the Council.

- 2.5 In discussion with those directly involved in processing requests, it was felt that the best route to improve this situation was to centralise the recording and processing of all subject access requests. This was with the proviso that, particularly in relation to requests for Social Work information, Services would be asked to advise on the disclosure and withholding of information.
- 2.6 When this was discussed, it was felt that the obvious place to deal with requests was the FOI team, but it was apparent at the time that the FOI team did not have the resources to undertake this additional work. A way of providing the team with an extra resource has since been identified and that is now in place.
- 2.7 In practical terms, this change will be implemented on a phased basis to the end of March 2014 to allow staff in the FOI team to become familiar with the complexities of the process.

### 3. CONCLUSION AND RECOMMENDATION

- 3.1 Access to a person's own personal information is a statutory right. The Councils processes for complying with this right have some identified weaknesses and the amendment to the policy should rectify them. Centralising the processing of requests for personal information will ensure greater consistency and provide a better service to requesters.
- 3.2 It is recommended that the Committee approve the revised policy.

#### Author

Name	Designation	Contact Details
Donald Henderson	Information Compliance Manager	T: 01738 477930 E: dhenderson@pkc.gov.uk

#### Approved

Name	Designation	Date
John Fyffe	Depute Chief Executive	13 March 2014

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 Donald Henderson



Council Text Phone Number 01738 442573

## 1. IMPLICATIONS, ASSESSMENTS, CONSULTATION AND COMMUNICATION

<b>Strategic Implications</b>	<b>Yes / No</b>
Community Plan / Single Outcome Agreement	No
Corporate Plan	No
<b>Resource Implications</b>	
Financial	No
Workforce	No
Asset Management (land, property, IST)	No
<b>Assessments</b>	
Equality Impact Assessment	Yes
Strategic Environmental Assessment	Yes
Sustainability (community, economic, environmental)	No
Legal and Governance	No
Risk	
<b>Consultation</b>	
Internal	Yes
External	No
<b>Communication</b>	
Communications Plan	

### 1. Strategic Implications

Community Plan / Single Outcome Agreement

1.1 None

Corporate Plan

1.2 None

### 2. Resource Implications

Financial

2.1 None

Workforce

2.2 None

Asset Management (land, property, IT)

2.3 None

### 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

- 3.3 The Environmental Assessment (Scotland) Act 2005 places a duty on the Council to identify and assess the environmental consequences of its proposals. No further action is required as the proposals do not qualify as a PPS as defined by the Act and is therefore exempt.

### Sustainability

- 3.3 None

### Legal and Governance

- 3.4 None

### Risk

- 3.5 None

## **4. Consultation**

### Internal

- 4.1 All Services were consulted about the strategy through their representation on the Policy and Governance Group.

### External

- 4.2 None

## **5. Communication**

- 5.1 Following approval, the revised policy will be published for both the public and employees. An Inside News bulletin will be published to draw attention to the changes and the timing of the changes for each Service.

## **2. BACKGROUND PAPERS**

None

## **3. APPENDICES**

Appendix 1 – proposed Data Protection Policy

## PERTH AND KINROSS COUNCIL

### Data Protection Policy

#### Scope

The data protection policy ('the 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 of reference 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.

Compliance with the policy and associated procedures are a condition of employment. Violations of the policy may result in disciplinary action against an employee.

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.

#### Roles and Responsibilities

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

Executive Directors are responsible for all aspects of compliance with the Act, and associated legislation, within their Service. They may, however, delegate their data protection responsibilities to individuals or service providers.

The Head of Legal 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.

Specific guidance will be produced for Elected Members who require access to personal information, and for employees who receive requests for access.

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.

Executive Directors 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 Freedom of Information Team are 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. Each individual employee is responsible for passing any subject access requests received to the Freedom of Information Team as soon as possible.

Services are responsible for passing information to the Freedom of Information Team in a timely manner. Employees must pass any information retrieved as part of a request to the Freedom of Information Team intact and unaltered.

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 co-operate with the FOI 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 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. [Services-The Freedom of Information 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 be made 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. ~~[Separate guidance on handling requests for personal information will be developed for use by staff.](#)~~

## **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 Legal 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 independently reviewed to ensure that practices laid down within the policy are



feasible, effective and are being adhered to. There will be a regular review of all areas of the Council to ensure compliance with the policy and procedures.

Executive Directors will ensure that all procedures within their area of responsibility are carried out correctly.

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**

Appropriate information sharing protocols 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.

The Council will not use Council Tax information for any other purpose out-with the processing and administration of Council Tax, unless specific statutory authority exists that allows secondary disclosure or purposes.

Individuals will be informed, at the point of data capture, of:

- The identity of the data controller (Perth and Kinross Council)
- The identity of 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
- Their right to access information the Council holds on them, on payment of a fee of £10

All forms which gather personal information will have a Fair Processing Notice at the bottom of each form.

## **Data Matching**

The Council will comply with the Information Commissioner's guidance on data matching and will produce a code of practice based on any advice received.

## **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	<p>Scope changed to remove references to partner organisations, contractors and agents following internal audit review (covered within contracts)</p> <p>Reference to third party confidentiality agreements removed following internal audit review (covered within contracts)</p> <p>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</p>	Head of Legal Services	7 December 2010
v7	<u>Responsibility for processing subject access requests updated to Freedom of Information Team following recent change in process. Subject access section updated to reflect change</u>		