DUNDEE CITY COUNCIL

DATA PROTECTION POLICY

2015

DATA PROTECTION ACT 1998 POLICY

CONTENTS

1. INTRODUCTION 2
2. PROVISIONS OF THE ACT 2
3. SCOPE 3
4. ROLES AND RESPONSIBILITIES..... 3
5. ADVICE AND TRAINING ……..... 4
6. NOTIFICATION ……..... 4
7. SUBJECT ACCESS 4
8. COMPLIANCE 4
9. DATA SHARING ……..... 5
10. RETENTION AND DISPOSAL OF DATA ……..... 5
11. INFORMATION SECURITY …….. 5
12. ISSUE AND REVIEW ……..... 5

DATA PROTECTION ACT 1998 POLICY

1. INTRODUCTION

In order to carry out is functions as a Local Authority, Dundee City Council needs to collect and use information about people, including members of the public, current, past and prospective employees, clients and customers, and suppliers.

The Council is committed to protecting the privacy and rights of all people it holds information about. It regards the fair and lawful treatment of personal information as essential to its operations and to maintaining confidence and trust between the Council and its customers. The Council will encourage and promote a culture of awareness of the Data Protection Act 1998 and its guiding principles.

The personal information that the Council holds must be handled and dealt with appropriately, however it is collected, recorded and used. Whether the information is on paper, in computer records or recorded by any other means there are safeguards within the Act to ensure this.

The Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the Council and those with whom it carries out business. The Council will ensure that it treats personal information lawfully and correctly.

To this end the Council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998 (the Act).

2. PROVISIONS OF THE ACT

The Data Protection Act 1998 regulates the processing of information relating to living persons in the UK. It requires that data controllers be registered with the UK Information Commissioner.

The Council is required to process all personal data held by it in accordance with the eight data protection principles contained within the Act. The data protection principles state that:-

a. personal data shall be processes fairly and lawfully, i.e. only for the purposes for which it was obtained and with the consent of the data subject (unless an exemption applies)

b. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

c. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

d. Personal data shall be accurate and, where necessary, kept up to date.

e. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

f. Personal data shall be processed in accordance with the rights of data subjects under this Act.

g. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

h. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3. Scope

The data protection policy ('the policy') will apply to all employees and Elected Members of Dundee City Council ('the Council').

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.

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'.

4. Roles and Responsibilities

The Legal Manager is the Council's Data Protection Officer and has overall responsibility for the administration and implementation of the data protection policy.

Each department and their senior management team will retain a departmental responsibility for ensuring compliance with the Act, and associated legislation, within their department. All departments will be required to nominate a departmental representative for data protection.

Employees are individually responsible for ensuring that the collection, storage, processing and destruction of data are in accordance with the Data Protection Act 1998 and must be familiar with its requirements.

Employees will only have access to personal information where that access is essential to their duties. 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.

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.

5. Training

The Council will provide advice and training for employees to comply with this policy. Additional guidance will be provided to staff who routinely handle personal, sensitive and confidential information.

Heads of Service are responsible for ensuring that employees within their Department are trained appropriately.

The Data Protection Officer will assist Departments in evaluating training need. Training materials will be developed in accordance with requirements.

6. Notification

The Council will ensure that it maintains its Notification entry with the Information Commissioner on an annual basis.

7. Subject Access

The Legal Manager is responsible for processing subject access requests on behalf of the Council, with the exception of those received by the Social Work section which is responsible for processing those requests received by their own section.

Each individual employee is responsible for passing any subject access requests received to the Legal Manager as soon as possible. The Council will endeavour to process all subject access requests within the statutory forty day deadline.

A fee of £10 is payable for subject access requests made by members of the public. However this is waived where the information to which access is sought is held by Social Work or Education. The Council will not charge a fee for employees wishing access to information which relates to their employment with the Council.

8. Compliance

Departments will undertake regular reviews to ensure compliance with this policy and other procedures relating to Data Protection.

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.

9. Data Sharing

The Council will ensure that personal information is not shared except in accordance with the Council's Code of Practice on Data Sharing.

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

10. Retention and Disposal of Data

All personal information must be processed in compliance with the Council's Records Management policy and associated procedures to ensure that data is not retained for longer than it is required.

Personal data must be disposed of in a way that protects the rights and privacy of those the information is about, such as shredding, disposal as confidential waste and secure electronic deletion.

All systems should be reviewed on a regular basis to identify records which are no loner required and these will be destroyed in line with the Council's Retention schedule.

11. Information Security

All staff and elected members are responsible for ensuring that personal information which they hold is kept safe and secure.

12. Issue and Review

Heads of Service shall ensure that a copy of this policy will brought to the attention of the employees within their Department.

This policy will be reviewed every two years and amended as appropriate