Town Hall, Penrith, Cumbria CA11 7QF
Tel: 01768 817817
Email: info.governance@eden.gov.uk

Data Protection Policy

Deputy Chief Executive
(01768) 212205
6 June 2017

1. Introduction

1.1 Eden District Council ("the Council") is fully committed to complying with the requirements of the Data Protection Act 1998 (the Act), which came into force on 1 March 2000.

1.2 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 and for whom it carries out business. The Council will follow procedures that aim to ensure that all employees, elected Members, contractors, agents, consultants, partners or other servants of the Council who have access to any personal data held by or on behalf of the Council, are fully aware of and abide by their duties and responsibilities under the Act.

2. Background

2.1 In order to operate efficiently, the Council has to collect and use information about people with whom it works and for whom it provides services. These people may include members of the public, current, past and prospective employees, residents, visitors to the area, contractors and suppliers. In addition, the Council may be required by law to collect and use information.

2.2 All personal information must be handled and dealt with properly and in accordance with the law, regardless of how it is collected, recorded and used. This includes data collected and stored in all formats including; paper files, computer records, sound recordings, video recordings and photographs.

2.3 The Act requires the Council to comply with the rules of good information handling practice, known as the data protection principles. In summary, these principles require that personal data is processed fairly and lawfully, is accurate and relevant and is subject to appropriate security.

3. Definitions

3.1 To aid the understanding of this policy and the provisions of the Data Protection Act, the following terms need to be understood:

Term	Definition
Data	Refers to any living individual about who data is collected or received by the Council.
Data Controller	In our case, this means the Council.
Processing	Means any use which is made of the data, from collecting the data, using it, storing it, and destroying it.

Term	Definition
Personal Data	Is data about a living individual who can be identified from that information or from that and other information in the possession of the Council.
Sensitive Personal Data	Means information relating to the racial or ethnic origin of an individual, his or her political opinions, religious beliefs, trade union membership, sexual life, physical or mental health or condition, or criminal offences or record.

4. The Principles of the Act

4.1 The Data Protection Act 1998 contains eight principles relating to the collection, use, processing and disclosure of data and the rights of data subjects to have access to personal data concerning themselves.

These principles are that all data:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;

2. 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;

3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;

4. Shall be accurate and where necessary, kept up to date;

5. Shall not be kept for longer than is necessary for that purpose or those purposes;

6. Shall be processed in accordance with the rights of data subjects under the Act;

7. Shall be kept secure ie protected by an appropriate degree of security; and

8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

These eight principles are the minimum standards the Council strives to meet with respect to personal data.

5. Associated Policies

5.1 This Policy should be read in conjunction with other Council policies as may be appropriate and in particular:

The Information Security Policy;

The Access to Information Policy;

Employment policies;

The Members' and Officers' Code of Conduct.

6. Subject Access Requests

6.1 The Act provides any individual the right to obtain a copy of all information held by the Council, about him / her. This is known as a Subject Access Request.

6.2 The Council can charge a fee of up to £10 for this service and must respond or complete all requests within 40 calendar days.

6.3 Occasionally the Council may have legitimate reason to withhold some information from a Subject Access Request. For example, information may be withheld:

- where information requested details relating to another person, the Council may have to seek permission to share that information in order for it to be supplied; or

- for the purpose of the prevention or detection of crime.

7. Fair and Lawful Processing

7.1 The Council will follow all procedures to ensure that collection, retention, processing and disposal of data fully complies with the Data Protection Act. The Council also has obligations to share data with key organisations for crime prevention and detection purposes.

National Fraud Initiative

7.2 The Council is required by law to protect the public funds that it administers. This requires the Council to share some personal information that customers provide with other bodies in order to prevent and detect fraud. This includes the Cabinet Office's National Fraud Initiative ("the NFI").

7.3 The NFI is responsible for carrying out data-matching exercises. The NFI matches data from 1,300 public sector and 77 private sector organisations, including audit bodies in Scotland, Wales and Northern Ireland, government departments and other agencies. This can flag up inconsistencies in the information that indicate a fraud, an

error or an overpayment may have taken place, signalling the need for review and potential investigation. No assumption is made as to whether there is fraud, error or another explanation until an investigation is carried out.

7.4 This data sharing does not require the consent of the individuals concerned. The data sharing powers were bestowed on the Minister for the Cabinet Office by Part 6 of the Local Audit and Accountability Act 2014 , effective from 1 April 2015.

8. Data Sharing

8.1 The ICO's Data Sharing Code of Practice of 2011 states that:

"People want their personal data to work for them. They expect organisations to share their personal data where it's necessary to provide them with the services they want. They expect society to use its information resources to stop crime and fraud and to keep citizens safe and secure."

8.2 This acknowledges and reflects the need for organisations to legitimately share data in order to provide effective services or for the purposes of crime prevention or detection. The Council is also required by law to collect and use information in order to comply with the requirements of central government.

8.3 The Council will ensure that only the minimum and relevant information is shared both within the Council and with external bodies. This is in compliance with the principles of the Act.

8.4 Any disclosure of information or sharing of information will be made in accordance with the provisions of the Act. Disclosures of data to other public authorities (such as the Inland Revenue, Customs and Excise, the Benefits Agency, the Department of Works and Pensions) will be made in accordance with statutory and any other requirements.

9. Data Transfer Overseas

9.1 The Act states that "Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) 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". The EEA includes all EU Member states together with Iceland, Liechtenstein and Norway.

9.2 Whilst the Council has no direct dealings in personal information with any country outside of the EEA, the internet and the Council's increased use of web based channels and technologies and social media, may result in personal information being communicated outside of the EEA. Any individual whose personal details (name, picture, etc) appear on the Council's web sites or social media channels will be informed of the implications of doing so, prior to publication and have given their "informed consent" for their personal details to be processed in this way.

10. Responsibilities

10.1 The overall responsibility for the efficient administration of the Data Protection legislation lies with the Council and is exercised through the Resources Portfolio Holder and Deputy Chief Executive. Day to day responsibility for administration and compliance with the Act is undertaken by the Directors and their staff.

10.2 Council Members will be covered by the authority's notification and have the same responsibilities in respect of data protection as an employee of the Council, when holding and processing personal data about individuals in the course of undertaking Council business and acting as a Councillor.

10.3 All individuals in the Council have a responsibility to ensure that personal data is treated confidentially and in compliance with the Act and this policy. Training on the Act and an individual's responsibilities is provided to all employees and Members of the Council.

Disciplinary Action

10.4 The Council expects all of its members and staff to comply fully with this policy and the principles of the data protection legislation.

10.5 Disciplinary action may be taken against any employee who breaches any of the instructions or procedures in this policy. A disclosure of information by a Member in breach of the Data Protection provisions may be a breach of the Members' Code of Conduct.

Senior Council Officers

10.6The officer with overall responsibility for the implementation of the Act is the Deputy Chief Executive who is the Council's Data Protection Officer. The Deputy Chief Executive and the Assistant Director (Legal Services) are able to provide advice on the interpretation and application of this policy and the Act.

10.7 The Council is registered as a data controller with the ICO as follows;

- Data Controller: Eden District Council
- Registration: Z6208207

11. The Information Commissioners Office

1.1The Information Commissioner's office maintains a public register of data controllers and provides advice and guidance to organisations and individuals on data protection issues.

The ICO can be contacted via;

www.ico.org.uk

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113

12. Review

12.1 This policy will be reviewed annually by the Deputy Chief Executive . It will be revised in May 2018, in line with the requirements of the General Data Protection Regulation (GDPR), which comes into effect (and replaces the Data Protection Act 1998) on 25 May 2018. The policy is available to all staff and is published on the website.

Accessibility Information

A summary of the information contained in this document is available in different languages or formats upon request. Contact Eden District Council's Communication Officer, telephone: 01768 817817 or email: communication@eden.gov.uk

Polish

Streszczenie informacji zawartych w niniejszym dokumencie można uzyskać na życzenie w innym języku lub formacie. Prosimy o kontakt telefoniczny z Referentem Rady ds. Komunikacji Okręgu Eden pod numerem telefonu 01768 817817 lub pocztą e-mail na adres communication@eden.gov.uk

Traditional Chinese

若閣下要求，本文件的摘要資訊可以其他版式和語言版本向您提供。請聯絡伊甸區地方政府傳訊主任 (Eden District Council's Communication Officer)，其電話為：01768 817817，或發電郵至：communication@eden.gov.uk

Urdu

اس دستاویز میں شامل معلومات کا خلاصہ درخواست کیے جانے پر مختلف زبانوں اور فارمیٹوں (شکلوں) میں دستیاب ہے۔ ایڈن ڈسٹرکٹ کاونسل کے افسر برائے مواصلات سےفون نمبر 01768817817 پر رابطہ کریں یا communication@eden.gov.uk پر ای میل کریں۔