www.erewash.gov.uk EREWASH BOROUGH COUNCIL

Data Protection Policy

2016-2019

Version: Final
Review Date: April 2019
Owner: Performance and Community Manager

Erewash Borough Council is committed to protecting the rights and privacy of all people with regards to the processing of personal data. During the course of our activities we will collect, store and process personal information about our staff, customers, suppliers and other third parties. We recognise the need to treat it in an appropriate and lawful manner and all processing will be conducted in accordance with the Data Protection Act 1998 and any subsequent amendments and everyone's rights with regard to how their personal information is handled.

This document sets out Erewash Borough Council's policy regarding data protection. The Data Protection Acts 1984 and 1998 and the EU Data Protection Directive form the background to the document. The policy is developed using the terms of the Data Protection Act 1998. The Freedom of Information Act 2000 will affect the council's use of non-personal information and the operation of this policy. The Human Rights Act 1998 will further enhance the protection and individual rights given under the Data Protection legislation.

1. Introduction

1.1 The purpose of the data protection legislation is to regulate the way in which personal information about individuals, whether held on a network, computer or in a manual filing system, is obtained, stored, used and disclosed. The legislation grants rights to individuals, to see the data stored about them, the purpose for which we process it, who we have shared it with and to require modification of the data if it is wrong and in certain cases, to compensation. The provisions amount to a right of privacy for the individual.

1.2 The Data Protection Act 1998 presents a number of significant challenges for local authorities. There is the extension of the scope of data protection from purely automated records to certain types of paper and other manual records. There are new rules that require data controllers establish a legitimate basis for the processing of personal data; and there will be significant changes to the system of registration that exists under the 1984 Act.

1.3 The 1998 Act requires all processing of personal data to be notified to the Information Commissioners Office and to be kept and used in accordance with the provisions of the Act.

2. Definitions

2.1 To aid the understanding of this document and the provisions of the Data Protection Act the following definitions are provided for assistance:-

2.2 **Data** is information that is:

- being processed by means of equipment operating automatically in response to instructions given for that purpose (e.g. payroll system).
- recorded with the intention that it should be processed by means of such equipment.
- recorded as part of a manual filing system or with the intention that it should form part of a relevant filing system (see definition below).
- one of a number of records to which public access is allowed.

2.3 **Data Controller** is any person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. In our case the "Council" as a whole is the data controller.

2.4 **Data Processor** means any person, other than an employee of the Council, who processes data on behalf of the data controller (e.g. someone contracted to the Council to print documents containing personal data). An employee of the Data Controller (the Council) is regarded by the DPA 1998 as constituting part of the Data Controller

2.5 **Data Subject** is the individual about whom personal data is held.

2.6 **Personal Data** means data about a living individual who can be identified from that information (or from that and other information in the possession of the data controller). This includes an expression of opinion about the individual, and any indication of the intentions of the data controller or any other in respect of that individual.

2.7 **Sensitive Personal Data** means personal data consisting of information as to:

- racial or ethnic origin of the data subject.
- his/her political opinion.
- his or her religious beliefs or other beliefs of a similar nature.
- whether he or she is a member of a trade union.
- his or her physical or mental health or condition.
- his or her sexual life.
- the commission or alleged commission by him or her of an offence.
- any proceedings for any offence committed by him or her, the disposal of such proceedings or the sentence of any court in such proceedings.
- The council also considers bank account details, national insurance numbers, passports and driving licences as sensitive.

2.8 **Processing** is very widely drawn and means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including:

- organisation, adaptation or alteration
- retrieval, consultation or use
- disclosure
- destruction of the information or data.

2.9 **Third Party** is any individual/organisation other than the data subject, the data controller (Council) or its agents.

2.10 **Relevant Filing System** means any data that is recorded as part of a manual filing system or with the intention that it should form part of a relevant filing system (e.g. "any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible").

3. Principles

3.1 The Data Protection Act 1998 contains **Eight Data Protection Principles** relating to the collection, use, processing and disclosure of data, and the rights of data subjects to have access to personal data concerning them. The aim of this policy is to ensure that the Council complies with the eight enforceable principles of good practice when processing personal data. These provide that personal data must be:

- Processed fairly and lawfully;
- Processed for limited purposes and in an appropriate way;
- Adequate, relevant and not excessive for the purpose;
- Accurate;
- Not kept longer than necessary for the purpose;
- Processed in line with data subjects' rights;
- Secure; and
- Not transferred to people or organisations situated in countries without adequate protection.

3.2 **Fair and Lawful processing** – the Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

3.3 For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party

to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

3.4 Data about staff may be processed for legal, personnel, administrative and management purposes and to enable the data controller to meet its legal obligations as an employer, for example to pay staff, monitor their performance and to confer benefits in connection with their employment.

4. Policy

4.1 The Council fully supports the objectives of the Data Protection Act 1998. This policy is intended to maintain the confidentiality of personal data held or processed either on computer or in manual files and to increase the access given to individuals to information relating to them.

4.2 The Policy links to the other council policies:-

- Information Security User Policy
- Data Retention Policy
- Freedom of Information Policy

4.3 It also links to the council's information sharing agreements register. Data may also be shared with certain other public authorities in accordance with statutory and other requirements (see Disclosures).

4.4 **External and Internal Registration/Notification**
The Council has an external registration/notification with the Information Commissioner. The Register can be searched at https://ico.org.uk/esdwebpages/search
The Erewash Borough Council registration references are:

- Z5708006 Erewash Borough Council
- Z5707929 Electoral Registrar of Erewash Borough Council

The Register Entry gives general descriptions of the type of data processing activities carried out by Local Government. The Register Entry is therefore supplemented by an internal register of data repositories, maintained by the Performance and Information Security Officer.

4.5 **Amount of data to be held**
The Council will hold the minimum personal data necessary to enable it to perform its functions. The data will be erased once the need to hold it has passed. Every effort will be made to ensure that data is accurate and up-to-date, and that inaccuracies are corrected quickly.

4.6 **Accuracy of Information**

Personal data will be accurate and kept up to date, steps will therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards, inaccurate or out-of-date data will be destroyed.

4.7 **Data Retention**

Personal data will not be kept longer than is necessary for the purpose, this means that the data will be destroyed or erased from our systems when it is no longer required.

4.8 **Subject Access**

A formal request from a data subject for information that the council holds about them must be made in writing. A £10.00 fee is payable by the data subject for the provision of this information. Any member of staff who receives a written request should forward this to the Performance and Information Security Officer immediately, the Council must respond within 40 calendar days.

The Council will only disclose personal data to those recipients listed in the Notification Register, or where it is otherwise permitted by law to do so. The council will always endeavour to seek the permission of the data subject, where it is required by law to do so.

4.9 **Data Security**

The Council will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage, to personal data.

The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:-

- **Confidentiality;** means that only the people who are authorised to use the data can access it.
- **Integrity;** means that the personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability;** means that authorised users should be able to access the data if they need it for authorised purposes.

4.10 **Disclosures**

Disclosures of information must be in accordance with the provisions of the Act and the council's registration/notification. Where the council has a duty to disclose certain data to public authorities (for example: the Inland Revenue, Customs and Excise, and the Benefits agency), this will be done in accordance with statutory and other requirements.

Legal and internal rules limit disclosure within the authority either to council officers or elected members. When a request for information is made, the minimum of personal data will be made available on a need to know basis as defined by the "Eight Data Protection Principles". The Data Protection Officer should be consulted if clarification is required.

4.11 **Public Registers**

The Council maintains a number of public registers that contain personal data or data that could be used to identify individuals. Strict compliance with the legislation giving rights of access will be used in all cases.

4.12 **System Design**

The Council intends that personal data must be treated as confidential. Computer and manual systems will be designed to comply with the Principles of the Data Protection Act so that access to personal data should be restricted to identifiable system users. Personal data will be kept in an appropriately controlled and secure environment.

4.13 **Training**

It is the aim of the Council that all staff will be informed of their obligations under the Data Protection Act and aware of their personal liabilities, and where appropriate further training will be given.

4.14 **Disciplinary Action**

The Council expects all of its staff and members to comply fully with this Policy and the Principles of the Data Protection Legislation. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures following from this policy.

5. Responsibilities

5.1 Overall responsibility for the efficient administration of the Data Protection legislation lies with the Council, and is managed by the councils Corporate Management Team. Day to day delivery is exercised by the Communities Directorate and administered by the Performance and Community Manager and the Performance and Information Security Officer who is the Councils designated **Data Protection Officer**.

The Data Protection Officer has the following responsibilities:-

- Lead corporate implementation and monitoring of compliance with the data protection policy;
- Development of and compliance with data protection training programmes for council staff;
- Provide advice and guidance on the provisions and requirements of the act in this data protection policy;
- To ensure that the Council's notification as a data controller is accurately maintained at all times;
- To manage requests for access to personal data and the exercise of other rights under the Act, including subject access and data sharing requests;
- To provide advice and guidance in respect of unusual or controversial disclosures of personal data, and contracts with data processors;
- To investigate incidents and complaints in relation to the security or disclosure of personal data held by the council;
- To report to the Information Governance Group on relevant data protection matters.

5.2 Day to day responsibility for administration and compliance with the Act is delegated to **Directors and Heads of Service**, for compliance with the Act's provisions within their respective areas of authority.

5.3 **All Officers and Members (Councillors)** have a duty to observe the Principles of the Act and the procedures referred to in this document. Please note: Councillors could be regarded as data controllers if they process personal data either manually or by computer, whether on their own equipment or on equipment provided to them by the local authority. Just as any other individual holding and processing personal information about others, Councillors need to comply with the Data Protection Act, and need to notify the Information Commissioner of all purposes for which they hold and process personal data.

5.4 However, where holding and processing personal data about individuals in the course of undertaking council business, the elected member will be covered by the authority's notification, and have the same responsibilities in respect of data protection as an employee of the authority.

5.5 Individuals who do not handle data as part of their normal work have a responsibility to ensure that any personal data they see or hear goes no further. This includes personal data and information extracted from such data, thus, for example, unauthorised disclosure of data might occur by passing information over the telephone, communicating information contained on a computer print-out or even inadvertently by reading a computer screen.

6. Data Subject Access Requests

6.1 A citizen has the right to ask to see the information the council keeps about them. This is known as a Data Subject Access Request.

6.2 To make such a request, a Data Subject Access Request Form must be completed. The Form is available on the council's website or by contacting the Performance and Information Security Officer.

6.3 The council will:-

- Ask for proof of identity before providing the information,
- Provide the information within 40 calendar days of receiving the request, or give a reason why it cannot do so,
- Charge a fee of £10 for providing the information.

6.4 **Processing in line with the data subjects' rights**

Data will be processed in line with data subjects' rights. Data subjects have a right to:

- Request access to any data held about them by a data controller;
- Prevent the processing of their data for direct-marketing purposes;
- Ask to have inaccurate data amended;
- Prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else; and
- Object to any decision that significantly affects them being taken solely by a computer or other automated process.

7. Review of Policy

7.1 The Data Protection Policy will be reviewed every three years and approved by the Council Executive. Minor amendments may be made from time to time, and updates and re-issues will be circulated as necessary.

7.2 The policy will however be reviewed sooner in the event of any one or more of the following:-

- Weakness in the policy is highlighted;
- Weaknesses in hardware and software controls are identified;
- New threat(s) emerge or risks change;
- Changes in legislative requirements;
- Changes in local and/or national Government occur which are relevant to a review; and
- New directives are received.

8. Contact Details

8.1 The council's Performance and Information Security Officer handles requests for information covered by the Data Protection Act 1998. For further details contact:-

The Performance and Information Security Officer
Erewash Borough Council
Town Hall
Wharncliffe Road
Ilkeston
Derbyshire DE7 5RP
Email: dataprotection@erewash.gov.uk

Date Issued	Version	Status	Reason for change
29 October 2004	0.1	Draft	
9 May 2005	0.2	Draft	Revised Policy in line with established good practice.
20 July 2005	1.0	Approved Policy	Approved by Council Executive (subject to confirmation by Council)
24 December 2009	To be updated 311210	Approved Policy	Policy update
15 December 2014	2.0	In draft updated	Policy expired and revised in line with good practice
January 2016	3.0	Draft	Light touch refresh