East Herts District Council

Data Retention Policy

Document Control

Organisation	East Hertfordshire District Council
Title	Retention Policy
Author – name and title	Tyron Suddes, Information Governance and Data Protection Manager
Owner – name and title	Tyron Suddes, Information Governance and Data Protection Manager
Date	October 2022~~July 2021~~
Approvals	Executive
Version	1.0
Next Review Date	~~July 2022~~October 2023

Contents

1. Introduction

This Policy sets out the obligations of East Hertfordshire District Council ("the Council") regarding retention of personal data collected, held, and processed by the Council in accordance with Data Protection Legislation. "Data Protection Legislation" means all legislation and regulations in force from time to time regulating the use of personal data and the privacy of electronic communications including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR"), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation.

Data Protection Legislation defines "personal data" as any information relating to an identified or identifiable natural person (a "Data Subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Data Protection Legislation also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under Data Protection Legislation, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by Data Protection Legislation to protect that data).

In addition, Data Protection Legislation includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

1.1. Where the personal data is no longer required for the purpose for which it was originally collected or processed;

1.2. When the data subject withdraws their consent;

1.3. When the data subject objects to the processing of their personal data and the Council has no overriding legitimate interest;

1.4. When the personal data is processed unlawfully (i.e. in breach of Data Protection Legislation or any other legislation);

1.5. When the personal data has to be erased to comply with a legal obligation;

or

1.6. Where the personal data is processed for the provision of information society services to a child.

This Policy governs the Council's ~~separate~~ Data Retention Schedule which sets out the type(s) of personal data held by the Council's services for specific purposes, the period(s) for which that personal data is to be retained and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with Data Protection Legislation, please refer to the Council's ~~Policy for Handling Personal Data~~Data Protection Policy.

2. Aims and Objectives

2.1. The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Council complies fully with its obligations and the rights of data subjects under the Data Protection Legislation.

2.2. In addition to safeguarding the rights of data subjects under the Data Protection Legislation, by ensuring that excessive amounts of data are not retained by the Council, this Policy also aims to improve the speed and efficiency of managing data.

3. Scope

3.1 This Policy applies to all personal data held by all service areas within the Council and by third-party data processors processing personal data on the Council's behalf.

3.2 Personal data, as held by the above is stored in the following ways and in the following locations:

3.2.1 The Council's servers, located in Stevenage;

3.2.2 Third-party approved cloud hosting solutions ('The Cloud,)~~servers~~, operated by the Council's service providers;

3.2.3 Computers permanently located in the Council's premises at Wallfields, Pegs Lane, Hertford and Charringtons House, The Causeway, Bishops Stortford;

3.2.4 Laptop computers and other mobile devices provided by the Council to its employees;

3.2.5 Computers and mobile devices owned by employees, agents, and sub-contractors used in accordance with the Council's ICT user policies;

3.2.6 Physical records stored in the Council's premises;

3.2.7 and all off-site archives used by the Council

4. Data Subject Rights and Data Integrity

4.1. All personal data held by the Council is held in accordance with the requirements of Data Protection Legislation and data subjects' rights thereunder, as set out in the Council's ~~Policy for Handling Personal Data~~Data Protection Policy.

4.2. Data subjects are kept fully informed of their rights, of what personal data the Council holds about them, how that personal data is used, and how long the Council will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

4.3. Data subjects are given control over their personal data held by the Council including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by the Council's Data Retention Schedule), the right to restrict the Council's use of their personal data, the right to data portability, and further rights relating to automated decision-making and profiling.

5. Technical and Organisational Data Security Measures

5.1. The Council aims to ensure that all of the following technical measures are in place to protect the security of personal data:

5.1.1 All emails ~~containing~~ used to share personal data must be encrypted;

5.1.2 All emails ~~containing~~ used to share personal data must be marked "confidential";

5.1.3 Personal data may only be transmitted over secure networks;

5.1.4 Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;

5.1.5 Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient

5.1.6 All personal data transferred physically should be transferred in a suitable container marked "confidential";

5.1.7 No personal data may be shared informally and if access is required to any personal data, such access should be requested from the relevant data administrator

5.1.8 All hardcopies of personal data, along with any electronic copies

stored on physical media should be stored securely;

5.1.9 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Council or not, without authorisation;

5.1.10 Personal data must be handled with care at all times and should not be left unattended or on view;

5.1.11 Computers used to view personal data must always be locked before being left unattended;

5.1.12 No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Council where the party in question has agreed to comply fully with the Council's ~~Policy for Handling Personal Data~~Data Protection Policy and the Data Protection Legislation;

5.1.13 All personal data stored electronically should be backed up regularly with backups stored onsite **AND/OR** offsite. All backups should be encrypted;

5.1.14 All electronic copies of personal data should be stored securely using passwords and encryption;

5.1.15 All passwords used to protect personal data should be changed regularly and must be secure;

5.1.16 Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method;

5.1.17 All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;

5.1.18 No software may be installed on any Council-owned computer or device without approval; and

5.1.19 Where personal data held by the Council is used for marketing purposes, it shall be the responsibility of the relevant data administrator to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service.

5.2 The Council aims to ensure that the following organisational measures are in place to protect the security of personal data:

5.2.1 All employees and other parties working on behalf of the Council shall be made fully aware of both their individual responsibilities and the Council's responsibilities under the Data Protection Legislation

and under the Council's ~~Policy for Handling Personal Data;~~Data Protection Policy;

5.2.2 Only employees and other parties working on behalf of the Council that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Council;

5.2.3 All employees and other parties working on behalf of the Council handling personal data will be appropriately trained to do so;

5.2.4 All employees and other parties working on behalf of the Council handling personal data should exercise care and caution when discussing any work relating to personal data;

5.2.5 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

5.2.6 All employees and other parties working on behalf of the Council handling personal data will be bound by contract to comply with the Data Protection Legislation and the Council's ~~Policy for Handling Personal Data;~~Data Protection Policy;

5.2.7 All agents, contractors, or other parties working on behalf of the Council handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Council arising out of the Data Protection Legislation and the Council's ~~Policy for Handling Personal Data;~~Data Protection Policy;

5.2.8 Where any agent, contractor or other party working on behalf of the Council handling personal data fails in their obligations under the Data Protection Legislation and/or the Council's ~~Policy for Handling Personal Data,~~ Data Protection Policy, that party shall indemnify the Council against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

6. Data Disposal

6.1. Upon the expiry of the data retention periods set out in the Council's Data Retention Schedule, or when a data subject exercises their right to have their personal data erased and this is upheld by the Ccouncil, personal data shall be anonymised deleted, destroyed, or otherwise disposed of as follows:

6.1.1. Personal data stored electronically (including any and all backups thereof) shall be deleted securely by the user. This will be followed by a 30 day soft deletion delay until the personal data is permanently deleted ;

6.1.2. Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely by the user. This will be followed by a 30 day soft deletion delay until the personal

data is permanently deleted;

6.1.3. Personal data stored in hardcopy form shall be disposed of in the Council's confidential waste bins;

6.1.4. Special category personal data stored in hardcopy form shall be disposed of in the Council's confidential waste bins;

6.1.5. If appropriate, both personal and special category shall be made truly anonymous so that it is no longer in a form which permits identification of data subjects.

7. Data Retention

7.1. As stated above, and as required by law, the Council shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

7.2. Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out in the Council's Data Retention Schedule.

7.3. When establishing and/or reviewing retention periods, the following shall be taken into account:

7.3.1. The objectives and requirements of the Council;

7.3.2. The type of personal data in question;

7.3.3. The purpose(s) for which the data in question is collected, held, and processed;

7.3.4. The Council's legal basis for collecting, holding, and processing that data;

7.3.5. The category or categories of data subject to whom the data relates;

7.3.6. The technical and organisational security measures in place;

7.3.7. The Local Government Association's data retention schedule guidance.

7.3.8. If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

7.3.9. Notwithstanding defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Council to do so (whether in response to a request by a data subject or otherwise).

7.3.10. In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving

purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the UK GDPR.

8. Roles and Responsibilities

8.1. The Council's Data Protection Officer is the Information Governance and Data Protection Manager and can be contacted by emailing data.protection@eastherts.gov.uk

8.2. The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with it, the Council's other Data Protection-related policies and with Data Protection Legislation.

8.3. The relevant data administrator(s) shall be directly responsible for ensuring compliance with data retention periods within their service areas

8.4. Any questions regarding this Policy, the retention of personal data, or any other aspect of Data Protection Legislation compliance should be referred to the Data Protection Officer.