East Devon District Council

Issue details	
Title	Data Protection and Document Retention Policy
Version	Version 1.0
Officer responsible	Data Protection Officer
Authorisation	Cabinet
Authorisation date	April 2018
Review date	April 2019

History of Policy Changes

Date	Page	Change	Origin of change (eg change in legislation)

1 Previous Policies/Strategies

This Policy supersedes the following two policies;

- Data Protection Policy (April 2016)
- Retention and Disposal of Documents Policy (undated)

2 Why has the council introduced this policy?

The processing of personal data is essential to many of the services and functions we carry out. In so doing we recognise the importance of the need to comply with the requirements of the data protection legislation and other relevant legislation which seeks to protect an individual's fundamental rights and freedoms. This policy seeks to help ensure compliance with the relevant legislation when we process an individual's personal data in relation to those services and functions and also when an individual seeks to exercise their rights in respect of their personal data. An important part of compliance relates to the retention of documentation, and therein an individual's personal data, and so this policy also covers our approach to document retention and disposal.

3 Scope

This policy applies to the collection and processing of all personal data by all services within the Council, the sharing of information between services and other parties and how we will act when using third parties who may process personal data on our behalf. It covers all formats (including paper, electronic, audio and video) and covers both manual and automated filing systems. The policy applies to all employees (including temporary staff), Councillors and all people or organisations acting on our behalf.

4 Policy Statement

4.1 *Data Protection Principles*

4.1.1 We will, by putting in place appropriate policies and procedures, be responsible for ensuring that an individual's personal data is;

- Processed lawfully, fairly and in a transparent manner,
- Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes,
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed,
- Accurate and kept up to date (where necessary) and every reasonable step taken to ensure that inaccurate personal data (having regard to purposes for which it is processed) is erased or rectified without delay,
- Kept in a form which permits identification for no longer than is necessary for the purpose for which it is being processed,
- Processed with appropriate security which will include protection against unauthorised or unlawful processing and against accidental loss, destruction / damage using appropriate technical or organisational measures.

4.1.2 In addition we will, through this policy and other measures, ensure that we are accountable in that we can demonstrate compliance with the responsibilities detailed above.

4.2 *Individual's rights*

4.2.1 We recognise that an individual has rights in relation to the way we obtain and process their personal data. Accordingly, and as part of our responsibilities detailed above, we will ensure that an individual is able to exercise them where permitted.

4.2.2 Individuals have the right to be provided with information about how we process their personal data. The information to be provided varies depending on whether we obtain the personal data from the individual or from a third party. We will generally satisfy this requirement through the use of privacy notices. We will ensure that the information provided is concise, transparent, intelligible and easily accessible and written in clear and plain language.

4.2.3 In addition we will ensure that individuals are able to exercise the following rights (where permitted);

- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object
- Rights in relation to automated decision-making (including profiling)

4.2.4 Detail in relation to each of the above rights and the processes / procedures for exercising them will be clearly detailed on our website and we will treat any request to exercise the rights in accordance with the legal requirements and the specific detail below.

5. Specific policy areas

5.1 *Purpose and Processing*

5.1.1 We will only collect information that is necessary for what we do by ensuring that there is a specific, explicit and legitimate purpose to be doing so. We will endeavour to ensure that information about individuals is accurately recorded when we collect it and up to date when we use it and that only the minimum necessary personal information is used to assist in the performance of its functions.

5.1.2 We will ensure that there is at least one lawul basis for processing an individual's personal data. Given what we do, on the whole this will be because the processing is necessary to comply with a legal obligation or because we are performing a task in the public interest / in the exercise of official authority. However, other lawful basis may apply depending on the circumstances.

5.1.3 We will make sure that the purpose for processing and the lawful basis are properly recorded and provided to individuals, generally through our website and in other formats on request.

5.1.4 We may carry out further processing provided it is not incompatible with the original purpose for which we collected the personal data. This would include processing for archiving purposes in the public interest, scientific or historical research or statistical purposes.

5.1.5 Where staff may have access to systems for more than one purpose, they will be given very clear advice about using data only in connection with the specific and authorised purpose. Just because they may have access to other information about a customer, does not imply that they can use it for more than one purpose.

5.2 *Special categories of information*

5.2.1 Certain personal data is particularly sensitive (this covers information relating to race, religious belief, political opinion, heatlh information, sexual orientation, trade union membership and (where processed to uniquely identify an individual) genetic and biometric data). We are not permitted to process this type of informarion unless one of the special conditions are met. By way of examples, the special conditions include situations where an individual gives their consent to the processing or an individual cannot give consent but processing is necessary to protect their vital interests.

5.2.2 We will ensure that we do not process special categories of information without one of the special conditions being met.

5.3 *Data Security*

5.3.1 In order to ensure the security of personal data, we will ensure we have appropriate physical, technical and organisational security measures in place. We will process personal data in accordance with our Information Security Policy – S01 (January 2018) and other related policies and procedures. Our employees are required to comply with the Information Security Policy – S01 (January 2018).

5.3.2 These measures will keep an individual's information secure and will protect it against unauthorised use, damage, loss and theft.

5.4 *Data sharing*

5.4.1 We are permitted in appropriate circumstances to share data within the organisation and also with external bodies. This is most likely to occur when we are required to disclose personal data by a court order, to comply with other legal requirements including prevention or detection of crime, preventing fraud[1] / gathering of taxation and carrying out our other

[1] The Cabinet Office's National Fraud Initiative is one such example.

regulatory functions. For instance, it would be acceptable to share data between services if we had good reasons to believe that fraudulent activity was taking place or if we had reason to believe that a crime had been (or was going to be) committed.

5.4.2 We will only share personal data internally or externally where we are permitted to do so and individuals will be made aware the circumstances in which this will occur through privacy notices. Any new system access requests from staff or services within the Council will be considered by the DPO.

5.4.3 We will use any relevant codes of practice on data sharing issued by the Information Commissioner to help with implementing these aims. Data matching techniques will only be used for specific lawful purposes and will also comply with any relevant codes of practice.

5.4.4 Where we obtain personal data from a third party rather than directly from an individual, we will, wherever possible, make sure they know that we have done this.

5.5 *Third Party processing*

5.5.1 We do on occasion ask external agencies or companies to carry out processing of personal data on our behalf. While such bodies are now also subject to detailed requirements regarding those processing activities, we are also under an obligation to ensure that those third parties are able to provide sufficient guarantees that their processing complies with legal requirements and protects the rights of an individual.

5.5.2 We will therefore ensure that there is a contract in place with any third party processors which complies with the legal requirements governing how a third party carries out the processing on our behalf.

5.5.3 We will endeavour to use only those third party processors who have signed up to and adhere to any relevant code of practice or certification scheme relevant to the processing activities they will be carrying out.

5.5.4 All contracts with third parties for the processing of personal data will be reviewed by the Data Protection Officer (or by the legal department on his behalf) to ensure it meets the relevant requirements.

5.6 *Privacy by design and data protection impact assessments*

5.6.1 We will ensure that an individual's rights in relation to privacy and data protection are a key consideration in the formulation and early stages of production of any project, process or policy as well as seeking to integrate them into existing project management and risk management methodologies and policies. Privacy and data protection will remain relevant throughout the lifecycle of any project, process or policy.

5.6.2 Having regard to certain factors, including the nature, scope, context and purposes of processing and related costs, we will implement appropriate technical and organisational measures to ensure we have integrated privacy and data protection into our processing activities.

5.6.3 Carrying out data protection impact assessments can help identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy. Again having regard to the nature, scope, context and purposes of processing, where we are considering introducing a new technology or to carry out processing in either case which is likely to result in a high risk[2] to the rights and freedoms of individuals then we will carry out an impact assessment.

5.7 *Transparency*

5.7.1 We are under obligations to provide individuals with certain information regarding how we will use their personal data and their rights. The information to be provided varies depending on whether we have obtained the information directly from an individual or from a third party. The

---

[2] This includes systemic evaluation based on automated decision making which results in decisions that produce legal effects or significantly affect an individual, large scale processing of special categories of information or systemic monitoring of a publicly accessible area on a large scale (CCTV).

information provided should be concise, transparent and intelligible. We will comply with our obligations primarily through the use of Privacy Notices (which are on our website) or by directly contacting the individual concerned, in either case using clear and plain language.

5.7.2 In addition, we are also under an obligation to keep records of our processing activities and information relating to it so that we are able to demonstrate to the Information Commissioner that we are complying with out obligations overall. We will ensure that we maintain the records as required.

5.8 *Document retention*

5.8.1 We will hold information about individuals for as long as is necessary and, subject to any statutory retention periods, we will ensure that the information is disposed of in a secure and proper manner when it is no longer needed.

5.8.2 It is important that we understand what documents to keep and for how long and that we don't keep unnecessary documentation nor keep documentation for longer than is necessary. This is not only from the data protection point of view but also good administration (in the sense of resources for keeping documentation, whether electronic or manual files).

5.8.3 Any decision taken in respect of the retention / disposal of documents will be taken in accordance with the Council's Document Retention Schedule (available on our website) and the key retention / disposal considerations set out in Appendix 1.

5.8.4 We will ensure that when disposing of papers which may contain personal or confidential data, we will use the confidential waste bins provided or place the documents in the confidential sacks. It is permissible to shred papers on-site (with a cross cutting device). Employees shall not dispose of personal or confidential papers in normal refuse or recycling bins.

5.8.5 Where the Council uses an external shredding contractor for the destruction of records or information, there shall be a contract which specifies clearly what is required, including transmission of records off-site and what constitutes destruction. Where possible, the Council shall inspect the premises of external contractors, both before the contract is awarded and periodically thereafter, to ensure security is adequate and that records are destroyed soon after they are received. This is particularly important if the records are confidential in any way. The contractor shall be required to supply a certificate of destruction and, for confidential records, a certificate of confidential destruction. Destruction certificates shall be kept by the Council for a period of one year.

5.8.6 Disposal of computer equipment / electronic media are outside the scope of this policy and will be covered in a separate policy.

5.9 *Data subject's rights*

5.9.1 We recognise the importance of individuals being able to exercise the fundamental rights available to them in respect of their personal data. These rights are identified in section 4.2 above. We will ensure that all requests from individuals to exercise their rights are dealt with as quickly as possible and in any event within one month of receipt unless we consider it necessary, due to the complexity or number of requests, to extend the time period by two months. Any extension of time will be notified to the individual within one month of the receipt of the request.

5.9.2 The exercise of an individuals rights will be provided free of charge unless, in our view, requests are manifestly unfounded or excessive (including where this is due to repeat requests) in which case we may choose to either charge a fee for providing the information / taking the action requested or to refuse to act on the request. Additional copies of information already provided may be subject to a reasonable charge at our discretion.

5.9.3 Where there is an exemption which would permit us not to progress any request or which may limit the application of any right, we will normally apply the exemption unless it is appropriate or reasonable not to do so and, in any event, will always do so in circumstances where it is deemed necessary to the effective operation of our tasks, for the prevention and detection of crime, to protect an individual or is required by law.

5.9.4 Where we are not confident of the identity of an individual making a request we may ask for information (or additional information) in order to confirm the identity before progressing their request to exercise their rights.

5.9.5 The Council will inform individuals of its decisions in respect of any requests and any further rights there may be in terms of lodging a complaint with the Information Commissioner and / or seeking remedy through the Courts.

5.10 *Breach reporting*

5.10.1 A personal data breach occurs when (whether deliberate or accidental) there is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. In broad terms this means a security incident that has affected the confidentiality, integrity or availability of personal data.

5.1.0.2 We will implement a process to ensure all staff handling personal data know when and how to report any actual or suspected data breach(es) and we will also provide a process for breach reporting by an individual and any third party processors that we may use.

5.10.3 Appropriately trained staff will deal with the reports of any breaches and where appropriate we will take steps to deal with the breach including measures to mitigate any adverse impacts.

5.10.4 Where a breach results in a risk to an individual's rights and freedoms we will ensure the breach is appropriately reported to the Information Commissioner and / or the individual(s) concerned in accordance with the legal requirements and prescribed timeframes.

5.10.5 Individuals also have the right to progress a complaint under the Council's complaints procedure.

5.11 *Training*

5.11.1 Data protection training is crucial so that all staff understand their responsibilities relating to data protection and the use of personal data. Failure to comply with the data protection principles and our legal obligations could lead to serious problems and result in the rights and freedoms of an individual being adversely affected. This could lead to significant fines or criminal prosecution.

5.11.2 It is therefore our policy that all individuals handling personal data will be trained to an appropriate level in the use and control of personal data. This may include employees that do not have internet or email access and line managers will be responsible for ensuring that these staff members complete an appropriate training course. Training will be given to all staff on a periodic basis to refresh existing staff and educate new staff. In addition to the corporate training, some post-holders are required to undertake further data protection training where appropriate for a particular role or within a specific service area.

5.11.3 Councillors will be furnished with a copy of this Policy and all future elected Members will receive a copy as part of their information pack on beginning their duties along with appropriate training.

6 Who is responsible for delivery?

6.1 The Data Protection Officer will be accountable for ensuring compliance with our legal requirements. In so doing he will ensure that this policy is followed across the Council and that there is an appropriate training programme for staff and identification of those members of staff who require enhanced training.

6.2 All staff are also responsible for ensuring compliance - the commitment of all Council Members and staff is essential to make this policy work. Employees should check with their line manager or the Data Protection Officer if they are unsure about their responsibilities or the handling of an individual's personal data, particular if it relates to disclosing such information.

6.3 All staff are expected to comply with our other policies relating to the management and security of information, including personal data, and to follow any good practice guidance that we issue.

7 Disciplinary action and criminal offences

7.1 Where an employee breaches this Policy and where caused by deliberate, negligent or reckless behaviour then the normal consequence will be an appropriate disciplinary sanction (which could include dismissal) and may even give rise to criminal offences.

7.2 The person concerned may also become liable for any financial consequences resulting from a breach of the Policy.

8 Policy Consultation and review

8.1 This policy has been consulted upon with relevant officers and the Strategic Management Team.

8.2 The Data Protection Officer will review this policy in 2019 or in the light of any legislative changes or relevant guidance issued, particularly by the Information Commissioner.

9 Equality impact considerations

The equality impact considerations relating to this policy have been considered. It is not considered that this is a high impact policy in relation to adverse impacts relating to the protected characteristics outlined in the Equality Act 2010.

11 Related Legislation, Policies and Strategies

- General Data Protection Regulations 2016 / Data Protection [Act 2018]
- Freedom of Information Act 2000
- Human Rights Act 1998
- Environmental Information Regulations 2004
- Local Government (Access to Information) Act 1985
- Equality Act 2010
- Data sharing code of practice (Information Commissioner's Office)
- Cabinet Offices' National Fraud Initiative
- East Devon District Council's Data Protection & Information Handling Good Practice Guide
- The Council's Complaints Procedure
- Information Security Policy – S01 (January 2018)

Appendix One

Disposal / Retention Considerations

There are some documents that do not need to be kept at all and staff may routinely destroy such information in the normal course of their duties. However, staff are advised to refer to the Council's Document Retention Schedule to ensure that they are not destroying any documents prior to their normal destruction date. Unimportant documents or information include:

- 'with compliments' slips
- catalogues and trade journals
- telephone message slips
- trivial email or notes that are not related to the business activities of the Council
- requests for stock information such as maps, plans or advertising material
- out-of-date distribution lists
- working papers which lead to a final report
- duplicated or superseded material

In addition the following will be considered prior to destruction;

1. Has the document been appraised?

Once a document has been initially highlighted for disposal it should be appraised to ensure it is suitable for disposal. In most cases this should only take a few minutes or even less, but it is a skilled task depending on the documents involved. It should therefore only be undertaken by officers who have sufficient operational knowledge to be able to identify the document and its requirements for continued need within the service.

2. Is retention required for evidence?

Any document which may be required for legal proceedings should be kept until the threat of proceedings has passed. While this should be covered in the timeframes set out in the Council's Document Retention Schedule, in the event it isn't then it is important to have regard to the fact that the Limitation Act 1980 specifies time limits for commencing litigation and therefore the starting point should be whether that period has now expired. The main time limits that are directly relevant to local government are as follows:

- Claims founded on simple contract or tort (other than personal injury claims) cannot be brought after the expiration of **6 years** from the date on which the cause of action occurred. This areas includes such matters as debt recovery actions, and compensation claims in respect of sub-standard work, negligent advice, and damage to property.
- Compensation claims for personal injury are barred on expiry of **3 years** from the date on which the cause of action occurred (this will usually be the date when the incident causing the injury occurred; **or**
- the date when the injured person first had knowledge of the injury
- Claims that are based on provisions contained in documents that are 'under seal' are barred after the expiration of **12 years** from the date on which the cause of the action occurred

3. Is retention required to meet the operational needs of the service?

In some cases retention may be desirable (whether permanent or otherwise) even though no minimum retention period applies, or has expired. Documents might be useful for future reference purposes (e.g. training), as precedents, or for performance management (performance indicators, benchmarking and comparison exercises). A professional judgment needs to be made as to the usefulness of a particular document. This decision should be made by the relevant Manager or his/her designated officer. In this case it will not be appropriate for any attributable personal data to be retained.

4. Is the document of historic interest or intrinsic value?

In most cases this consideration will not be applicable. However, some documents currently in Council storage may be of historic interest and/or even have some monetary value. Even if the document is of historical or monetary value disposal, rather than retention by the Council, it may well be the appropriate option to transfer to the County Archivist or even sale to an external body. There should be no processing of personal data in relation to any document in this category.