



Tendring District Council

Corporate Data Protection Policy



Version Control

Name	TDC DPA Policy		
Version	3	Date	04/05/2011
Authors	Judy Barker	Roles	ICT Project Manager & DPA Officer
Approval	n/a	Roles	n/a

Amendment History / Change Record

Date	Version	Key Changes / Sections Amended	Amended By
04/05/2011	3	Version control implemented & definition added to Section g.	Judy Barker



Tendring District Council Corporate Data Protection Policy

1. The Data Protection Act 1998 and this Council Policy apply to all data relating to any identifiable living person, held by this Council, on computer or in manual filing systems.
2. The Council requires all of its members and employees to comply with this policy, the Council's Computer Security Policy and the Data Protection Act and to co-operate with all measures to ensure compliance.
3. Heads of Service are required to ensure compliance with this policy and nominate a Service Unit representative to be responsible for collation of information; informing the Corporate Data Protection Officer of all service processing requirements and acting as a contact point for receipt of all guidance/update information.
4. Personal information must be treated as confidential and must only processed and disclosed, for purposes that the Council has notified to the Information Commissioner's Office, to:
 - Council employees, where the information is necessary for their work; and
 - Others in accordance with the associated part of the Council's Data Protection notification.
5. All computerised and manual filing systems containing data relating to any identifiable living person must be:
 - Identified.
 - Secured.
 - Be accurate and kept up to date.
 - Notified to the Council's Data Protection Officer.
6. Such systems (computerised and manual) must be designed and operated so as to comply with the Data Protection Principles (see Section B).
7. Any person may ask the Council for the data that the Council holds about them. This is known in the legislation as **A Subject Access Request**. Any such request must be immediately passed to the Corporate Data Protection Officer for action throughout the Council. The legislation dictates that the required disclosure of information must be made within 40 calendar days. Any data that the person is entitled to must be presented in plain language in hard copy format along with information regarding why the data is held and what it is used for. An administration fee is allowed to be charged for a Subject Access Request; this is currently set at a maximum of £10.
8. Disciplinary action, including dismissal in a serious case, may be taken against any employee who commits a breach of this policy. The employee may also be open to criminal proceedings under the Data Protection Act 1998 which may result in an unlimited fine or a custodial sentence.



(A) GENERAL INFORMATION

Tendring District Council currently has 2 notifications in place with the Information Commissioner which are renewable annually. They are as follows: -

Council Main Notification	Registration No. Z577148X	Expiry Date: 18 October
Electoral Registration	Registration No. Z6205259	Expiry Date: 17 February

Notifications are renewable on an annual basis. However, the legislation states that any **new processing** must be notified to the Information Commissioner ***before*** this processing takes place. In addition, any redundant processing must be removed from the notification as soon as it has ceased. It is essential that the Council's notifications are maintained to provide an accurate statement of the required processing of personal data at all times. All changes should be provided in writing to the Corporate Data Protection Officer on a regular basis. An annual confirmation of the current situation will be sought by the Corporate Data Protection Officer each year prior to renewal.

Details of each of the Council's notifications can be viewed by accessing the link shown below and entering the appropriate Registration No. under the search option (see above)

http://www.ico.gov.uk/tools_and_resources/register_of_data_controllers.aspx

FURTHER ADVICE AND GUIDANCE CAN BE OBTAINED FROM: -

**ICT Project Manager/Corporate Data Protection Officer
Judy Barker
Town Hall
Clacton on Sea CO15 1SE**

Tel: 01255 686513
E-Mail: jbarker@tendringdc.gov.uk

Or

**Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF**

Additional Information:

By telephone: ICO Helpline:
08456 30 60 60
01625 54 57 45

E-Mail: notification@ico.gsi.gov.uk
Guidance:
http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx



(B) THE DATA PROTECTION PRINCIPLES (1998)

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-
 - (a) at least one of the conditions in Schedule 2 is met, and
 - (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. 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.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. 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.
8. 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.



(C) THE DATA PROTECTION ACT 1998 - SCHEDULE 2

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

1. The data subject has given his consent to the processing.
2. The processing is necessary-
 - (a) for the performance of a contract to which the data subject is a party, or
 - (b) for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary-
 - (a) for the administration of justice,
 - (b) for the exercise of any functions conferred on any person by or under any enactment,
 - (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
 - (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.
6.
 - (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
 - (2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.



(D) THE DATA PROTECTION ACT 1998 - SCHEDULE 3

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF SENSITIVE PERSONAL DATA

1. The data subject has given his explicit consent to the processing of the personal data.
2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation, which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order-
 - (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
 - (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
3. The processing is necessary-
 - (a) in order to protect the vital interests of the data subject or another person, in a case where-
 - (i) consent cannot be given by or on behalf of the data subject, or
 - (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or
 - (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
4. The processing-
 - (a) is carried out in the course of its legitimate activities by any body or association which-
 - (i) is not established or conducted for profit, and
 - (ii) exists for political, philosophical, religious or trade-union purposes,
 - (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
 - (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
 - (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.
5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
6. The processing-
 - (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
 - (b) is necessary for the purpose of obtaining legal advice, or
 - (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
7. (1) The processing is necessary-
 - (a) for the administration of justice,
 - (b) for the exercise of any functions conferred on any person by or under an enactment, or



- (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
- (2) The Secretary of State may by order-
 - (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
 - (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
- 8. (1) The processing is necessary for medical purposes and is undertaken by-
 - (a) a health professional, or
 - (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.
- 9. (1) The processing-
 - (a) is of sensitive personal data consisting of information as to racial or ethnic origin,
 - (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
 - (c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.
- 10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.



(E) LEGISLATIVE EXEMPTIONS FROM DISCLOSURE

There is provision within Sections 28 – 37 and Schedule 7 of the Data Protection Act 1998 (“the Act”) for certain types of data to be exempt from certain of the data protection principles (mainly the rights of access to data, the right to prevent processing, and the rights to require rectification, blocking, erasure or destruction of data). These principally comprise the following:-

- National Security (Section 28) - this does not directly affect the Council.
- Crime and Taxation (Section 29) – this is of great importance for the Council and includes personal data processed for
 - (a) the prevention or detection of crime
 - (b) the apprehension or prosecution of offenders
 - (c) the assessment or collection of any tax or duty or of any imposition of a similar nature
- Health, Education and Social Work (Section 30) – this has limited application for the Council, and includes information as the physical or mental health or condition of the data subject.
- Regulatory Activity (Section 31) – this exemption is of great importance for the Council and includes such matters as Ombudsman cases and other investigations/enquires of a diverse nature.
- Journalism, Literature and Art (Section 32) – this has little direct application for the Council.
- Research History and Statistics (Section 33) – again this has little direct relevance for the Council.
- Information available to the public by or under Enactment (Section 34) – as in the case of Freedom of Information, such information is exempt under the Act.
- Disclosures required by Law or made in connection with legal proceedings etc. (Section 35) – this is of great importance for the Council and includes the obtaining of legal advice in connection with actual or prospective legal proceedings or in establishing, exercising, or defending legal rights.
- Domestic purposes (Section 36) – this does not affect the Council.
- Miscellaneous – (Section 37 and Schedule 7) – matters that affect the Council include:-
 - (a) confidential references given by the Data Controller.
 - (b) management forecasts etc. – this includes personal data processed for the purposes of management forecasting or management planning to assist the Data Controller in the conduct of any business – information may be withheld in situations where the disclosure would prejudice the conduct of that business or other activity.
 - (c) negotiations – again information may be withheld in situations where disclosure would be likely to prejudice any negotiations.
 - (d) legal professional privilege – personal data is exempt from disclosure if the data consists of information in respect of which a claim to legal privilege could be maintained in legal proceedings.
 - (e) self-incrimination – a person need not comply with any request for personal data to the extent that compliance would expose him to proceedings for any offence (other than an offence under the Act).



(F) SUBJECT ACCESS DISCLOSURE GUIDANCE

F.1. THIRD PARTY INFORMATION

Information contained within personal data may often contain information relating to another person(s) (third party). There is a duty of care required regarding the balance between the data subject's right to access and the third party's right to privacy.

What should be done :-

(1) Consent

Where practicable, the consent of the third parties to release their data should be sought. Where consent is obtained then the information can be released. If consent is withheld, or cannot be obtained, further consideration must be given to the question of disclosure.

(2) Editing third-party data

Where there is no consent to supply the third party data, the information should be edited to remove any details that may lead to the identification of the third party. It is important to bear in mind that this editing must be applied to any information that might lead the data subject to *infer* the identity of the other party. Simple removal of names will not be sufficient if the third party can be identified from other details. Where the editing of all the information relating to a third party does not leave sufficient information for it to make sense to the data subject, the interest of all parties must be considered when determining whether or not that information should be disclosed.

(3) Balancing of interests

If the third party has already provided his or her information to the data subject, it may be considered reasonable to make a disclosure without consent or where consent cannot be sought. In other circumstances the information will usually be withheld, unless it is so significant and of such importance to the applicant that access should be allowed despite a lack of consent. This is usually viewed as a 'vital interest', which is protected by the Convention of Human Rights. The test case involved a young person in local authority care who applied for records relating to his time in care. Access was declined owing to the presence of third party information, which formed an integral part of the data requested. The case was taken to the European Courts and it was decided that due to his 'vital interest' in the information he could receive the information necessary to know and understand his childhood.

As the balancing test in relation to third party information can sometimes be very difficult to apply, especially where sensitive or confidential information is involved, it is recommended by the Information Commissioner's guidance that legal advice should be sought before making a decision to release information.



F.2. GENERAL

E-Mail

The disclosure of personal data held in e-mails is also required by the Act. Again, care must be taken not to infringe the rights of other individuals when supplying such correspondence.

Automated Decisions

Logic involved in automated decisions – the Act provides for individuals to request an explanation of the logic involved in any automated decisions taken in relation to them. However, these need only be provided where specifically requested by the individual.

CCTV

As with e-mail, CCTV must be provided in response to a subject access request where they are specifically capable of identifying the data subject. Again, care must be taken regarding third-party data. The Commissioner's office has issued a code of practice on the use of CCTV, which can be found on the Information Commissioner's website:

http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx

Intelligible Form

Providing information in an intelligible form – this means that the information must be intelligible to *them* not just the data controller. The use of jargon should be avoided or explained, and an explanation should be provided for abbreviations or codes contained within the information if their meaning would not otherwise be intelligible to the data subject.

Requests not originating from the data subject and requests from minors

Only data subjects can make access requests under section 7 of the Act. There is no provision for parents to make subject access requests on behalf of their children. Neither does the Act provide guidance on whether a minor can make a request on their own behalf. It should be noted that a minor ceases to be such at the age of 12 under the Data Protection Act. Careful consideration needs to be applied when handling requests from minors as to the harm that might arise against the possible benefits of supplying the information.

Individuals may of course authorise other individuals to make requests on their behalf. However if such a request is received, proof of the authorisation must be provided.



(G) Definition of Terms

Term	Definition
Data	Information which is : <ul style="list-style-type: none"> ➤ Being processed by means of equipment operating in response to instructions given for that purpose (i.e. Computer system) ➤ Recorded with the intention that it should be processed by means of such equipment ➤ Recorded as part of a filing system structured either by reference to individuals or be reference to criteria relating to individuals whereby specific information relating to an individual is readily accessible ➤ Forms part of an accessible record, e.g. manual card files, microfiche, etc.
Personal Data	Data that relates to a living individual who can be identified by name, number, code or default.
Processing	Obtaining, recording, organising, holding, disclosing, using and eliminating
Data Subject	The person identified, or who can be identified, from the personal data or when used with other data held.
Data Controller	The Council and its employees
Data Processor	A person or organisation who processed personal information on behalf of another Data Controller. TDC may also be a Data Processor if it processes information on behalf of a third party organisation or another Local Authority.
Data Subject Access Request	An individual has the right to be supplied with all the information the entire Council holds by submission of this request and payment of a fee, within 40 calendar days. Requests of this nature are coordinated by the Council's Corporate Data Protection Officer (Judy Barker)
Data Subject Notice	An individual can serve a data subject notice which requires the Council to cease or not to begin processing personal data of which he/she is the subject, where such processing is causing or is likely to cause damage or distress. Damage or distress must be of a real nature over and above annoyance level and without justification. The Council has 21 calendar days to respond to such a notice and must state that it either has complied, intends to comply or state reasons why it does not intend to comply.