Epping Forest District Council

Data Protection

Protocol for the handling of Subject Access Requests pursuant to Section 7(1) of the Data Protection Act 1998

1. INTRODUCTION

1.1 Epping Forest District Council is a data controller pursuant to the Data Protection Act 1998 ('the Act'). The Council regards the fair and lawful treatment of personal data as important to the efficient performance of its operations and the delivery of services, and to maintaining confidence between the authority and those with whom it works.

1.2 The Council fully endorses and adheres to the principles of data protection set out in the Act, including the right of subject access. This protocol sets out how the Council handles requests for personal data, known as Subject Access Requests, in accordance with best practice guidance issued by the Information Commissioner's Office (ICO) and the provisions of the Act.

2. THE RIGHT OF ACCESS TO PERSONAL DATA

2.1 In order to carry out its functions, the Council has to collect and use personal information about people with whom it works, including members of the public, current, past and prospective employees, clients, customers and suppliers. Personal data is any information which relates to a living individual.

2.2 The subject access provisions of the Act promote the principles of transparency and accountability, enabling individuals to understand how their personal data is being used by the Council, to check the accuracy of information that the authority holds, and to exercise rights over the 'processing' of such information. The act of processing personal information concerns operations such as the organising, retrieving, consulting, using, adapting, altering or deleting of data, and covers virtually any lawful use that the Council may make of the personal data that it holds.

2.3 Subject access provides a right for any individual who is the subject of the processing of personal data (a 'data subject'), to request access to the personal data that the Council holds about them. Access to personal data can only be denied in limited circumstances, where an exemption specified by the Act applies. The right of subject access provides that a data subject is entitled to be told whether a data controller is processing their personal data, and to a description of:

(a) the personal data;
(b) the purposes for which the data is being processed; and
(c) those to whom the data are or may be disclosed.

2.4 In addition, an individual is also entitled to a copy of the personal data that the Council holds relating to them, unless an exemption applies, and details about the rationale behind any decisions taken about them solely by automatic means.

3. SUBJECT ACCESS REQUESTS

3.1 Requests for personal data are made in the form of a 'Subject Access Request'. The subject access provisions of the Act only apply to the personal data of living individuals and do not give any right of access to the data of the deceased, although the Council may still owe a common law duty of confidentiality to the estate of a deceased person

3.2 A data subject does not have to explain why they wish to make a Subject Access Request, or why they require access to their personal data, but the request must: only be for the individual's own personal data.

3.3 The subject access requirements of the Act are for a data subject to receive personal data, rather than necessarily the documents that contain the data. Whilst the data subject is not therefore strictly entitled to receive the original documents that include the personal

information, the provision of copies of documents that contain personal data is considered to be the simplest and most effective way of dealing with a Subject Access Request. The personal data provided in response to a Subject Access Request will always be provided in an intelligible form.

3.4 Whilst an individual may request an opportunity to view their 'file', the Act does not provide this right and only entitles a data subject to receive copies of their personal data as part of a Subject Access Request. However, the Act provides that a data controller can meet the subject access provisions by allowing a data subject to view their records (rather than being provided with a copy of relevant information), providing that they agree to this approach.

4. SUBJECT ACCESS REQUESTS - RESPONSIBILITY AND PROCESS

4.1 The Council's designated Data Protection Officer is responsible for considering and responding to all Subject Access Requests, including the processing of requests and the disclosure (or otherwise) of appropriate personal data. Subject Access Requests should be made directly to the Data Protection Officer wherever possible, to limit the possibility of delay in the provision of a response.

4.2 A template Subject Access Request Form can be used to submit a request for personal information. However, the Council does not insist that this form be used for Subject Access Requests, which can be made in any 'permanent' form (i.e. in writing, or by email/fax etc.). A Subject Access Request does not have to be marked as such or to quote the Data Protection Act, but cannot be made verbally or over the telephone.

4.3 The Council must be satisfied as to the identity of an individual making a Subject Access Request, in order to ensure that personal data is only supplied to the correct person, and appropriate identity checks will therefore be undertaken by the Data Protection Officer. Guidance that forms part of the template Subject Access Request Form specifies the types of information that a data subject will need to provide to confirm their identity.

4.4 A data subject may authorise another person to make a Subject Access Request on their behalf. In such cases, written authority from the data subject will be required to be submitted before the Council will comply with a Subject Access Request. An agent appointed by the Court of Protection or with a valid Power of Attorney, may also make a Subject Access Request on behalf of an individual.

4.5 A child is entitled to a make a subject access request because, as a general rule, children aged twelve or over are presumed to be of sufficient age and maturity to be able to make a request for their own data. Where a child is less than twelve years of age, a parent or guardian is able to exercise access rights on their behalf. In dealing with these cases, the Council will need to be satisfied that the person with parental responsibility is acting in the best interests of the child, before disclosing relevant personal data.

4.6 If a Subject Access Request is made by an agent acting on behalf of a data subject, the Data Protection Officer will also ensure that the agent has the necessary authority to act in this respect. The Council will take particular care in circumstances where spouses, partners or other relatives of a data subject claim to be authorised to access personal data, as unauthorised disclosures of personal information to family members are a breach of the Act and a frequent cause of complaint to the ICO. The validity of any Power of Attorney or Court of Protection Order will be substantiated by the Data Protection Officer, and a Power of Attorney must specify the purposes for which it is granted and be a certified copy.

4.7 An administration fee of £10.00 will be required to be paid for each Subject Access Request. This is the maximum allowable fee prescribed by the Act and, although the charging of a fee for dealing with a request is discretionary, it is the Council's policy to make such a charge for each request received.

4.8 The Act allows the Council to seek further information from a data subject in respect of a Subject Access Request, where this is reasonably required in order to assist the identification and location of the personal information requested. As applicants will not necessarily be aware of the different ways in which the Council might hold personal data, the Data Protection Officer will undertake this process as part of the validation of a Subject Access Request, if required.

4.9 The timescale prescribed by the Act for the Council to comply with a Subject Access Request is forty calendar days, and this period will normally start from the date on which the authority receives the request. However, if one or more of the following has not been provided by the data subject, the forty-day period will not commence until the outstanding item(s) has been submitted to the Data Protection Officer:

(a) the administration fee;
(b) any information required to validate the identity of the data subject;
(c) written authority from the data subject where another person is applying on their behalf;
(d) a certified power of attorney or court of protection order (where applicable); or
(e) any information reasonably required to identify and locate the personal data requested (if required).

4.10 Subject Access Requests will not be progressed until all relevant information has been received by the Data Protection Officer. Incomplete requests, or those that do not satisfy the requirements set out above, will not be considered by the Council.

4.11 The receipt of a valid Subject Access Request will be acknowledged by the Data Protection Officer, who will also advise the data subject of the date by which a response to the request will be made. Full searches of all relevant file/record systems and databases will be instigated, in order to identify and locate relevant personal information.

4.12 Whilst searches may be limited to specific service areas if the data subject has indicated that the Subject Access Request relates to a specific type of personal information, directorate data protection representatives will search all computer systems and relevant (see Section 4) manual systems for personal data. All computer systems must be checked, including non-networked (e.g. stand-alone PC's and laptops etc.) systems. Subject Access Requests for 'all personal data' will require full searches by all service directorates.

4.13 If it is clear that data identification and provision is likely to exceed the date by which a response to the Subject Access Request is to be made, or if there is likely to be a delay in dealing with the request for any other reason, the Data Protection Officer will contact the data subject to explain the reason for the delay and the expected date for issue of the response.

5. IDENTIFICATION OF PERSONAL DATA

5.1 A Subject Access Request only applies to the provision of personal data. This is any information which relates to a living individual who can be identified from that data alone, or in conjunction with other data held by the Council. Personal data includes any expression of opinion about an individual and any indication about the intentions of the authority or a third-party in respect of the individual.

5.2 The Council must provide information in response to a Subject Access Request only to the extent that it is personal data relating to the data subject. The subject access provisions of the Act specifically relate to the following ways in which personal data may be held by a data controller:

Information processed by electronic means

This is generally information held on computer systems. However, this category does not exclusively relate to computerised information.

Information recorded with the intention that it be processed by electronic means

This is information recorded in writing, with the intention of it being subsequently entered into a computer record.

Information forming part of a 'relevant filing system'

This is manual information stored in a systematic way, structured by reference to individuals or criteria relating to individuals, which allows ready access to data about a specific data subject.

Information forming part of an 'accessible record'

This is information such as the Council's housing records, for which specific access rights were in place prior to the introduction of the Act.

Other information held by a public authority

This is information held by the Council that does not fall within any of the above categories.

5.3 Directorate data protection representatives will undertake full searches of all relevant electronic systems and databases, and all structured manual filing systems in use within their respective directorate or service area, in order to identify personal information relating to the data subject. In responding to a Subject Access Request, directorate representatives should recognise that their service area may not be the only function that has had dealings with the data subject. Checks should therefore be made with other relevant service areas as appropriate, to identify any additional information held.

5.4 The identification of manual information held about a data subject may depend on the nature of the individual's involvement with the Council, and computerised information about an individual may indicate if manual personal data is likely to be held. If file records are stored at off-site locations, it is important that directorate data protection representatives ensure that all relevant files are located and searched for personal data. Personal data contained in system archives must be supplied in response to a Subject Access Request, if they contain information not held on (or which is different to) live systems.

5.5 The Act provides no exemption from the disclosure of 'embarrassing' or other non-factual data or comments contained in documents such as file notes, and such information will generally have to be disclosed in response to a Subject Access Request. It is a criminal offence for the Council to alter, block or destroy information, with the intention to prevent the disclosure of personal information to a data subject.

5.6 The Council must provide personal data held within any email, in response to a Subject Access Request. Although email systems may be difficult to search, all email containing personal data relating to the data subject must be supplied to the Data Protection Officer. Where necessary, a data subject may be asked to provide additional information to help locate personal information believed to be held within email systems, for example to identify matters such as the author, recipient, date and subject matter of the relevant email correspondence.

5.7 The Council's future email archive facility ('Mimecast') will store all email for a defined period, in line with general document retention periods. Once implemented, it will be possible for a

centralised search of Mimecast email records to be made by the Data Protection Officer in response to a Subject Access Request. Appropriate governance controls will be in place for such searches of the Mimecast system, which will be recorded and reported to the Chief Internal Auditor.

5.8 Images captured by the Council's CCTV systems may need to be provided in response to a Subject Access Request. However, it is not necessary to supply such information unless a data subject has specifically requested the disclosure of CCTV footage. Subject Access Requests involving the provision of CCTV images will be dealt with by the Data Protection Officer in conjunction with the Safer Communities Manager, who is responsible for the operation of Council's CCTV systems.

5.9 Personal data contained within a recording of a telephone call made to or by the Council, may need to be provided in response to a Subject Access Request. Any request involving the provision of personal data from recorded telephone conversations will be dealt with by the Data Protection Officer in conjunction with the Assistant Director of Resources (ICT and Facilities Management), who is responsible for the operation of the Council's telephony systems. The Council does not currently routinely record incoming or outgoing telephone calls, although this facility may be introduced in the future.

5.10 Requests for personal data contained within other audio recordings such as interviews under caution, will be treated in the same way as for telephone calls. This data may be provided in the form of a copy of the actual recording, or through the preparation of a written transcript.

5.11 Directorate data protection representatives will provide relevant personal information in response to a Subject Access Request, within the timescale identified by the Data Protection Officer.

6. SUBJECT ACCESS REQUESTS – COMPLETION

6.1 Once all relevant personal data relating to a Subject Access Request has been identified and located by the directorate data protection representatives, the Data Protection Officer will assess the content of the information for:

(a) third-party information;
(b) unintelligible terms; or
(c) personal data that is covered by an exemption to the Act (see Section 7).

6.2 If at this stage, any personal information is found to be inaccurate, amendments will not be made before the information is provided to the data subject. As part of the response to the Subject Access Request, the data subject will be informed that the Council is aware of the inaccuracy and has taken steps to amend or annotate the original data.

Third-party information

6.3 The Act acknowledges the right of a third-party to privacy where they can be identified from another individual's personal data, and specifies a number of criteria which aim to balance the right of access against a third-party's right to privacy. Personal data relating to the data subject which also identifies a third-party will therefore be withheld from the response to a Subject Access Request unless:

(a) the third-party has consented to its disclosure; or
(b) it is reasonable in all the circumstances (see below) to comply with the request without the consent of the third-party; or
(c) the third-party identifiers can be removed from the personal data so that the information can still be disclosed to the data subject.

6.4 Even if the third-party has not consented to the disclosure of their data, the personal data will not automatically be withheld from a response to a Subject Access Request. The reason for the refusal will be considered by the Data Protection Officer, to determine whether it is reasonable in all the circumstances to withhold information that would identify the third-party. If it is determined that data identifying a third-party should not be provided in response to a Subject Access Request, only that information which identifies the third-party (either explicitly in a document or as the source of the information) will be withheld. This approach may require documents to be edited, either by redacting third-party identifiers, or by retyping the information with third-party details omitted.

6.5 In practice, it may be difficult to remove third-party identifiers from documents, as the subject matter of the information may mean that the data subject is still able to infer the identity of the third-party. When deciding whether it is reasonable to disclose third-party information without consent, the Data Protection Officer will consider the following:

(a) any duty of confidentiality owed to the third-party (i.e. the nature of the data and whether the third-party provided the information on an understanding of confidentiality);
(b) any steps taken to obtain the third-party's consent;
(c) whether the third-party is capable of giving consent; and
(d) any express refusal of consent by the third-party and the reason for the refusal.

6.6 Third-party information revealed as part of a Subject Access Request that relates to an officer of the Council acting in an official capacity (most commonly this will be the names of employees), will generally be disclosed in response to the request. However, the Data Protection Officer will consider whether the names of staff should be redacted, in circumstances where it is considered appropriate to do so. This approach will generally only be applied where disclosure might put an employee at risk.

Unintelligible Terms

6.7 A data subject is entitled to be provided with a copy of their personal data in an intelligible form, with a full explanation of any codes, abbreviations or technical terms contained in the information. The Data Protection Officer will seek clarification where necessary of any such codes, abbreviations or technical terms etc., contained within personal data provided by directorate data protection representatives. If the data subject is a child or someone who lacks the mental capacity, relevant information may need to be explained in simpler terms than when dealing with an adult.

7. EXEMPTIONS TO THE RIGHT OF ACCESS

7.1 The right of subject access is generally regarded as one of the most important aspects of data protection legislation. The Act contains some limited exemptions to the right of access, which provide for personal information to be withheld from a response to a Subject Access Request. The main exemptions from the duty to provide subject access, are as follows:

Disproportionate effort

7.2 This exemption only relates to the provision of copies of personal information, and does not apply to the effort required to locate the personal data. The Council will still be required to allow an individual to view personal data even if a copy cannot be provided, and the following matters will be considered in the application of this exemption:

(a) the cost of providing the information requested;
(b) the length of time likely to be taken to provide the information; and
(c) how difficult it may be for the information to be provided.

7.3 These issues will be balanced against the effect that withholding the information would have on the individual making the Subject Access Request. The greater the adverse effect, the less likely it is that the exemption could be applied.

Repeated requests

7.4 There is no requirement for the Council to comply with a Subject Access Request which is identical or similar to a previous request from the same person, unless a 'reasonable interval' has elapsed. The following matters will be considered in the application of this exemption:

(a) the nature of the information requested;
(b) the purposes for which the information is processed; and
(c) the frequency with which the information is updated.

7.5 Caution will always be exercised with regard to this exemption, as a data subject may have only requested specific personal data in an initial Subject Access Request, whilst a subsequent request could be for other or different personal information.

Crime and taxation

7.6 The Act contains categories of exemption from some of the subject access provisions in relation to the following 'crime and taxation purposes':

(a) the prevention or detection of crime;
(b) the apprehension or prosecution of offenders; and
(c) the assessment or collection of any tax or duty.

7.7 Personal data may be withheld from a response to a Subject Access Request where disclosure would be likely to prejudice (i.e. significantly harm) any of the crime and taxation purposes. The exemption is likely to apply in circumstances where the Council is prosecuting an individual who may have committed an offence, or where the authority is working with the Police or other prosecuting body.

7.8 There must be 'a substantial chance rather than a mere risk that in a particular case the purposes (i.e. the investigation or assessment/collection) would be 'noticeably damaged' by the release of personal data. Information will therefore only be withheld from a Subject Access Request where it is clear that current or future processing would be prejudiced by such disclosure. Non-disclosure of personal data in response to a Subject Access Request will only affect the prejudicial information, and other data which will not prejudice an investigation will be disclosed as normal.

Health, education and social work

7.9 The Act provides limited reasons for withholding personal data contained within health, education and social work records from a response to a Subject Access Request, although these exemptions are likely to be of limited relevance to the Council. The application of certain categories of these exemptions requires the Council to consult appropriate health or other professional agencies responsible for the care and/or support of a data subject, and there is no discretion to disclose personal data without authority from the relevant agency.

References

7.10 Confidential references written by the Council for the purposes of education, employment or service provision are exempt from the right of subject access, although this exemption does not apply to references that the authority has received. If a data subject requests access to references supplied to the Council, regard may need to be given to the application of the third-party data exemption.

Management information

7.11 Personal data processed for the purposes of management forecasting and/or planning activities relevant to the Council's business operations, is exempt from the right of subject access. This exemption applies only to the extent that disclosure would be likely to prejudice the business or other activity of the authority.

Negotiations

7.12 Personal data which contains the intentions of the Council in relation to negotiations with the data subject are exempt from the right of subject access, to the extent that disclosure would be likely to prejudice the authority's position in those negotiations. Information about negotiations that have ended are not exempt, unless it can be shown that other on-going negotiations would be prejudiced by disclosure.

Legal advice and proceedings

7.13 Personal data that consists of information, in respect of which a claim to legal professional privilege could be maintained, may be exempt from disclosure in response to a Subject Access Request. Legal professional privilege applies to confidential correspondence between the Council and its legal advisors (internal or external) for the purposes of obtaining legal advice, and this exemption will only be applied in consultation with the Director of Corporate Support Services.

7.14 The Data Protection Officer will consider and apply relevant exemptions on a case-by-case basis. If personal data is withheld under any exemption, the reasons for the non-disclosure (including the exemption relied upon) will be documented, so that the Council can justify its response to the request if challenged. Where an exemption applies only in part, all personal information that is not exempt will be disclosed. The application of an exemption will be explained, to the extent that this is possible, in response to a Subject Access Request.

8. SUBJECT ACCESS REQUESTS – RESPONSE

8.1 The Data Protection Officer will issue responses to all Subject Access Requests, including all information statutorily required to be provided to comply with a request. The provision of information concerning decisions taken in respect of the data subject by automatic means, is generally unlikely to apply to Subject Access Requests considered by the Council.

8.2 All such responses will be fully and completely documented, including the reasons for the non-disclosure of any personal information. The Data Protection Officer will complete a 'Subject Access Request Decision Record' for every request, retaining in all cases:

(a) the original Subject Access Request and any subsequent correspondence;
(b) any draft response and amendments to the request (where relevant);
(c) a copy of the final decision and response to the request, including any personal data disclosed; and
(d) the reasons for each such decision, including the reason for non-disclosure of personal information or the particular exemption that has been applied.

8.3 The recording of the decision of the Data Protection Officer in respect of a Subject Access Request is important, in case a challenge is made to the Council's disclosure of personal information. This could be in the form of a complaint to the authority or the ICO, and the record will be of assistance if it is subsequently necessary to justify the Council's response to the request, or if a further similar Subject Access Request is received. The Data Protection Officer will deal with any queries about the Subject Access Request; including exemptions relied upon to withhold information.

8.4 The Council's response to a Subject Access Request will include an explanation of the searches made to deal with the request, and the personal information identified and located by such searches, in order to help the data subject understand whether they have received all the information they have requested. All personal data provided will be marked 'Data Subject Copy' prior to release, to assist (if necessary) the identification of the source of any further disclosure of the personal information.

8.5 In circumstances where a child has made a Subject Access Request, the Council will respond directly to the child themselves.

9. SUPPLY OF PERSONAL DATA

9.1 The data protection principles of the Act require that appropriate technical and organisational measures be taken against unauthorised or unlawful disclosure of personal data. Accordingly, the Council will ensure that the arrangements by which personal data is disclosed are appropriately secure, given the nature of the data concerned in any particular circumstance.

9.2 The Council's preferred method for the provision of personal data is by personal collection by the data subject, from the Civic Offices. Disclosure in person will be permitted where an appointment for collection has been arranged with the Data Protection Officer, and appropriate identification is produced for inspection (if required). In these circumstances, the data subject will be required to sign and date a 'receipt' for the completed response to the Subject Access Request, a copy of which will be retained by the Data Protection Officer.

9.3 Whilst e-mail is not a totally secure method of communication, it is recognised that the nature of Subject Access Requests may be such that it is appropriate for requests to be responded to by e-mail. Responses to Subject Access Requests will be made by email at the discretion of the Data Protection Officer, and only where specifically required by the data subject. Responses to Subject Access Requests required by other electronic means (e.g. file upload), will be considered by the Data Protection Officer in consultation with the Assistant Director of Finance and ICT (ICT).

9.4 Personal data will be sent through the normal post at the discretion of the Data Protection Officer, and only where specifically required by the data subject. Where considered necessary, a recorded delivery service will be utilised in this respect. The disclosure of personal data in response to Subject Access Request will not be made by the Council by telephone or facsimile transmission, in any circumstances.

9.5 If a data subject makes a request to a view their personal data rather than receive copies of relevant information, appropriate arrangements will be made by the Data Protection Officer, including the removal of any exempt information that might be contained within electronic records. In circumstances where a data subject has specific needs in relation to language or disability, arrangements will be made to present the personal information in a suitable manner.

9.6 Where a child is deemed able to make a Subject Access Request, the Council will respond directly to the child.

10. DATA PROTECTION OFFICER

10.1 The designated Data Protection Officer can be contacted as follows:

Data Protection Officer,
Epping Forest District Council,
Governance Directorate,
Civic Offices,
High Street,
Epping,
Essex, CM16 4BZ.

☎ (01992) 564180
✉ performance@eppingforestdc.gov.uk

11. DOCUMENT HISTORY

11.1 The Data Protection Officer is responsible for the maintenance of this protocol. The effectiveness of the protocol will be reviewed after relevant legislative changes, new case law, or revised guidance published by the ICO.

Prepared/Revised	Written by	Agreed/Authorised	Details of Change(s)
September 2013	S. Tautz (Data Protection Officer)	Corporate Governance Group (25/9/13)	Initial release of protocol. Published to website and intranet.
April 2014	S. Tautz (Data Protection Officer)	S. Tautz (Data Protection Officer)	Protocol updated as required to reflect new senior management structure. Republished to intranet and website.