



Waveney District Council  
Serving the Community

Policy Document

# Data Protection Act

1998



## 1. Statement of Intent

Waveney District Council intends to fulfil all its obligations under the Data Protection Act 1998. The Council will ensure that all notifiable processing is appropriately notified and will conduct a periodic review and update of the register entries. It is the aim of the Council that all appropriate staff are properly trained, fully informed of their obligations under the Data Protection Act 1998 and are aware of their personal liabilities, relating to the law and the disciplinary procedures of the Council.

Individuals whose information is held and processed by the Council can be assured that their personal data will be treated with all due care. It is possible that other legislation may (at times and under certain conditions) override Data Protection law – individuals should note that the Council intends to fulfil all of its legal responsibilities.

This policy document applies only to information covered by the Data Protection Act 1998 and will be updated/amended as necessary according to the laws of England and Wales.

The Council will comply with other legislation which interacts with the Data Protection Act 1998 and will produce updates to the Policy document and initiate staff training/awareness where appropriate.

## 2. Fair Obtaining/Processing

The Council will, as far as is practicable, ensure that all individuals whose details we process are aware of the way in which that information will be held, used and disclosed. Individuals will, where possible, be informed of the likely recipients of the information – whether the recipients are internal or external to the organisation. If a person feels they have been deceived or misled as to the reason for which their information was collected, they may use the Council's Compliments and Complaints Procedure.

Collection forms requiring personal information will contain a "fair obtaining" statement giving details of the likely uses of the information. Where information is collected in person or by telephone, the employee asking for the details will tell the individual how those details will be used. People are free to ask the person collecting the information why they want the details and what they will be used for.

If an individual's details are going to be used in "auto-decision" processing (where a computer decides something based on a score or other information) the person will be told about how the system works and whether the decision can be challenged.

## 3. Data Uses and Processes

The Council will not use or process personal information in any way that contravenes its notified purposes or that would constitute a breach of Data Protection law. Any new purposes introduced will, where appropriate, be notified to the individual and – if required by the law – their consent will be sought. A copy of the appropriate notification document is available from the Council's Data Protection Officer. Alternatively, copies of the notification documents are available from the Office of the Information Commissioner's web page @ [www.dataprotection.gov.uk](http://www.dataprotection.gov.uk).

All staff using personal data within the Council will be trained on the uses and disclosure of information. The disclosure policy sets out the reporting structure so that all purposes and disclosures throughout the Council are co-ordinated and consistent. All new purposes are documented and notified to the Office of the Information Commissioner.

## 4. Data Quality and Integrity

The Council will not collect data from individuals where that information is excessive or irrelevant in relation to the notified purpose(s). Details collected will be adequate for the purpose and no more. Personal information collected which becomes irrelevant or excessive will be deleted/destroyed.



Information will only be held for as long as is necessary for the notified purposes(s) – after which the details will be deleted. Where details of individuals are stored for long-term archive or historical reasons and where it is necessary to retain the personal detail within the records it will always be done within the requirements of the legislation.

The Council will ensure, as far as is practicable, that the information held is accurate and up to date. It is the intention of the Council to check wherever possible the details given. Where a person informs the Council of a change of their own circumstances, such as home address or other non-contentious data, their record(s) will be updated as soon as possible. Where the individual requests that information be changed and it is not possible to update it immediately, or where the new information needs to be checked for its accuracy or validity, where possible, a marker will be placed on the disputed record indicating the nature of the problem. The Council and the individual will attempt to reach an amicable agreement on the dispute but where this is not possible the Council's Compliments and Complaints Procedure may be implemented.

## 5. Technical and Organisational Security

The Council has implemented appropriate security measures as required under the Data Protection Act 1998. In particular, unauthorised staff and other individuals are prevented from gaining access to personal information. Appropriate physical security is in place with visitors being received and supervised when possible within the Council buildings where information about individuals is stored. The general public visiting the Council buildings should not feel that the measures are restrictive or oppressive, the measures are there to protect the Council's data.

Computer systems are installed with user password controls and, where necessary, audit and access trails to establish that each user is fully authorised. In addition, employees are informed about overall security procedures and the importance of their role within those procedures.

Security arrangements are reviewed regularly, all reported breaches or potential weaknesses are investigated through the audit process and, where necessary, further or alternative measures will be introduced to secure data.

All staff are informed and frequently reminded about the limits of their authority on disclosing information both inside and outside the Council. Details will only be disclosed on a needs basis within the Council. Disclosure of information will be in accordance with the Data Protection Act and the Council's Disclosure Policy. Any unauthorised disclosure will be dealt with under the Council's Disciplinary Procedures.

## 6. Subject Access/Subject Information Requests

Any person whose details are held/processed by the Council has a general right to receive a copy of their own information. There are a few exceptions to this rule, such as data held for child protection, crime detection / prevention purposes, but most individuals will be able to have a copy of the data held on them. Any codes used in the record will be fully explained, any inaccurate, out of date, irrelevant or excessive data will be dealt with under the procedures outlined in Section 4 of this policy, Data Quality and Integrity.

The Council will attempt to reply to Subject Access Requests as quickly as possible and in all cases within the 40 days allowed by the Data Protection Act, unless the data subject is notified otherwise. Repeat requests will be fulfilled unless the period between is deemed unreasonable, such as a second request received so soon after the first it would be impossible for the details to have changed. A subject access/information request should be submitted on the appropriate forms, together with a fee as detailed in the Council's Fees and Charges Book. This will ensure that the Council has the required information to be able to conduct a data search and to fulfil the request. In some cases, especially with requests not submitted on the correct form, further information may be required from the requester, which may delay



the start of the 40-day maximum time limit.

## 7. Relevant codes of practice/procedures within the Council

Separate codes of practice exist within the Council in respect of the following types of processing:

(a) **Data matching** (Appendix A)

(b) **Personnel records, inc. Sensitive data & Ethnic Monitoring**

The Council's Code of Practice for the use of personal data in employer/employee relationships is based on the Draft Code of Practice prepared by the Office of the Information Commissioner.

(c) **Internet and e-mail usage, website monitoring** (this is part of the Communications Policy)

(d) **Advice to Councillors** (Appendix B)

(e) **Security policy**

The Council produces an IT Security Policy which is in the process of being updated. In it, it states:

### **"The Importance of IT Security**

"Information relating to most of the Council's functions is now readily available to authorised users within all department.

"It is this ability to access information that is both a strength and a weakness. To be useful, the data must be accurate and available when required. It must only be available to those who are authorised and have a need to access it.

### **"Security Policy Objective**

"In particular, the Policy is required to ensure that computer based information is stored and used in a safe and secure manner.

"The IT Security Policy is needed to protect not only the Council's data but also the users of that data. A number of Acts of Parliament cover the use of computer programs and data." The Acts listed include the Data Protection Act 1998.

Copies of the IT Security Policy are available from the ICT Section.

(f) **Use of Council Tax Data for other purposes within the Council** (Appendix C)

(g) **Procedure for Handling Requests to disclose information** (Appendix E)

(h) **Compliance with the Act for those working away from the office**

The Council's Home Working Policy is in draft only, but the authority is investigating the procedures of allowing employees to work from home where practicable. The draft Policy states requirements for security of data both on computer and paper, especially mentioning that equipment and data should not be accessed or visible to other members of the family. Copies of this Policy, entitled "Home Working Policy", together with the employee's guide, entitled "Your Guide to Home Working" are available from Human Resources.

(i) **Data retention policies** (Appendix F)



- (j) **Compliance monitoring** (this function will be carried out by Internal Audit in line with the recommendations of the Data Protection Audit Manual)
- (k) **Use of Violent Warning Markers** (this is contained in the Customer Alert List Policy and Procedure)
- (l) **CCTV** (this is contained in the CCTV Code of Practice and Operation Manuals)
- (m) **Leaflet – Your Right to Know** (Appendix H)
- (n) **List of Data Protection Forms** (Appendix I)
- (o) **Use of Images** (Appendix J)

## **8. Further Information, Enquiries and Complaints**

The Council's Data Protection Officer is the first point of contact on any of the issues mentioned in this policy document. The Data Protection Officer will be responsible for dealing with all internal and external enquiries. Where possible, requests for information should be in writing. **All** complaints should be written, dated and should include details of the complainant as well as a detailed account of the nature of the problem. The Council will attempt to complete internal investigations in line with the time limits in the Compliments and Complaints Procedure.



## DATA MATCHING

### External services

The main data matching exercise carried out by The Council is the National Fraud Initiative (NFI) which is carried out annually under the auspices of the Audit Commission. A biennial NFI handbook, e.g. “National Fraud Initiative 2000 Handbook” indicates what data the Office of the Information Commissioner considers can be matched.

The Audit Commission is revising the Code of Data Matching Practice to ensure full compliance with the latest Data Protection and Human Rights Legislation by all NFI participants, and it is the Council’s intention to comply with these recommendations. In the meantime authorities are reminded of the following steps to be taken in relation to each type of dataset submitted:

- ▶ Discussion with staff associations or other representative bodies to inform them that payroll data is to be used or used again
- ▶ Notification to individual pensioners that the exercise is to be carried out
- ▶ Prominent inclusion on Housing Benefit claims and tenancy applications that data held by the authority will be used for cross system and cross authority comparison purposes for the prevention and detection of fraud
- ▶ Similar wording to be included in documentation relating to local licensing systems of other relevant applications which are to be included in NFI\_2000.

### Internal Data Matching

The Council’s Internal Audit Service carry out data matching of internal systems, i.e. not with any other authority or agency, as part of its Audit Plan. The systems reviewed would include those identified by the Audit Commission as part of the NFI. The difference is that such checks can/will be done more regularly than biennially.



## ADVICE TO COUNCILLORS

The Data Protection Act 1998 became law on 1 March 2000. It requires any person or organisation holding personal information relating to any living individual in computer or manual files to process that data within the principles set out in the Act. A copy of the eight Principles of the Data Protection Act 1998 is attached. In most cases, the person or organisation holding the data will also have to notify with the office of the Information Commissioner.

### Definitions

The owner of the data who notifies the Information Commissioner the purposes for which the data will be used is called the Data Controller. The **Data Controller** is responsible for the security of the data and has to ensure that all principles of the Act are complied with.

The **Data Subject** is the identifiable living individual to whom the data relates.

**Processing** covers the complete life-cycle of the data from collection to destruction.

**As elected Councillors you will probably access personal data while undertaking the following roles:**

- ▶ As members of the Council carrying out your committee work.
- ▶ Acting on your own behalf to process personal data.
- ▶ Acting on behalf of a political party.
- ▶ Acting on behalf of a constituent to investigate a complaint.

To help you understand which data you may be given access to, it is important for you to identify which role you are carrying out.

### As members of the Council carrying out Committee work.

To enable you to carry out your role you will be supplied with the data necessary for you to make decisions. The Data Controller is the Council and you will have access to and process personal data with the same restrictions as employees. The data supplied can only be used for that specific purpose.

For example, you may be a member of a Housing Committee which needs to make a decision relating to a specific tenant, in this case you would only get information relating to the tenant in question, and not have access to all records on the housing system.

### When you are acting on your own behalf to process personal data.

You may hold information on a computer at home or in a card index system to timetable surgeries or progress complaints made by local residents. In this case you, personally, will be the Data Controller and may need to notify under the Act.

Even if you do not need to notify under the Act you should comply with the requirements of the eight Data Protection principles.



### Acting on behalf of a political party

The Data Controller will be the political party supplying you with the data and you are entitled to rely on the data protection notification made by the political party.

### Acting on behalf of a constituent to investigate a complaint

When requesting personal data you will need to identify the purpose for which it is required. The request should be made in writing and a copy of the form is attached. The data are supplied for one specific purpose only and must not be used for any other purpose. Any data supplied to you must be treated with the utmost confidence and filed/stored securely and when the need for it has ceased it should be destroyed in an appropriate way. To minimise bureaucracy the Information Commissioner has decided that unless the data are of a particularly sensitive nature you will not have to obtain the data subject's consent as she will rely on the integrity of the individual councillor not to request data unless they are acting on behalf of a constituent.

### Offences for mis-use of data

The Data Protection Act contains a number of criminal offences:

- ▶ Processing personal data which has not been notified to the Information Commissioner.
- ▶ Making disclosures of personal data which have not been authorised by the Data Controller
- ▶ Disclosing data in a way it was not originally intended

The Information Commissioner is taking a very firm line with the way in which data can be used. A Councillor has recently been taken to Court for obtaining a copy of a database containing details of recipients of Free Bus Passes and using the information on his home computer to send a mailshot for party political reasons; he was fined £500 with £780 costs.

### Notification

A booklet has been produced by the Data Protection Office called **Notification Exemptions, A Self Assessment Guide**. This gives guidance on whether you need to notify and how to notify.

Notification can be done on-line by contacting <http://www.dpr.gov.uk/notify/1.html> and selecting the Councillor template under Purposes, or by telephoning the Data Protection Office on 01625 545 740 to request a form. Notification costs £35 and is valid for twelve months.

### Security

This is a very important part of the Data Protection Act and not protecting the privacy and integrity of personal data is a criminal offence. You need to have password controls in place if you keep data on a computer and data should be protected from third parties (including family and friends), if you use a laptop it should never be left unattended in a car. The Council has its own security measures in place, but you will need to have your own procedures in place if you are notifying as a Data Controller.



## **Compliance with the Act**

The Council is currently reviewing its policies and procedures.

## **Further information**

Obviously the above information is only a brief overview of the Data Protection Act and further information can be obtained from

Waveney District Council's Data Protection Officer

or

The Office of the Information Commissioner  
Wycliffe House  
Water Lane  
Wilmslow, Cheshire, SK9 5AF

Tel: 01625 545700

Fax: 01625 524510

E-mail: [Mail@dataprotection.gov.uk](mailto:Mail@dataprotection.gov.uk)

Home page: [www.dataprotection.gov.uk](http://www.dataprotection.gov.uk)



## Use of Council Tax data for other purposes within the Council

Historically, Council Tax information has been used as a general source of information throughout the Council. The issue of whether or not this can be considered lawful was raised by the Data Protection Working Party and in order to clarify the situation, it was decided to ask Counsel's opinion. A copy of this opinion is available from Legal or the Data Protection Officer.

As a result of Counsel's opinion the following restrictions will be placed on the use of Council Tax data:

- ▶ Council Tax data is not available for general use throughout the Council.
- ▶ Council Tax information may be disclosed on a case by case basis if it can be shown that there is a Statutory Provision which permits disclosure of the information. Any officer requesting information from Council Tax will be expected to cite the relevant Statutory Provision. The procedures for releasing this information are contained in the Procedure for Handling Requests to disclose information. This will also apply to any Third parties requesting information.

Council Tax data may also be released for the following reasons:

- ▶ Prevention or detection of crime
- ▶ Prosecution and apprehension of offenders
- ▶ Assessment or collection of any duty or tax



## DISCLOSURE POLICY INC. SUBJECT ACCESS REQUESTS

### Disclosing data to Third Parties

The Council can disclose personal data in certain circumstances, where it is permitted to do so by law. The most common examples of where the Council can disclose information are outlined below. However the Council may also be able to disclose in other specified circumstances but these should be referred to the Data Protection Officer for their view before disclosure.

### Disclosure requests

Requests for information should be made in writing, unless there are exceptional circumstances, and a copy of the form to be completed is attached at the end of this document. Copies are available from the Portfolio Administration Managers. Some departments that receive a large number of requests for information have specific forms to meet their requirements and copies are attached to this document.

The form asks for reasons why data should be disclosed. This is very important. The Council must be given a proper reason by the person or organisation requesting the data in order to release the data. The Officer making the disclosure must be satisfied that this is a valid reason. If you are not sure – seek advice from your Line Manager or Data Protection Officer.

Copies of all completed Disclosure Forms need to be kept by the Line Manager disclosing the information, together with details of the information which the Council has disclosed or reasons why the Council has not disclosed the information.

### Common reasons for disclosing data

- ▶ Prevention or detection of crime
- ▶ Prosecution and apprehension of offenders
- ▶ Assessment or collection of any tax or duty
- ▶ In the vital interests of the data subject
- ▶ Disclosures required by law or made in connection with legal proceedings

### Urgent Requests

Sometimes there may not be time to complete a Disclosure Form before the information is released. The Council is prepared to accept requests verbally providing a faxed request is sent to the relevant Line Manager within 2 hours of the request. Verbal requests must be logged on receipt of the call and there must be a valid reason for disclosing the data. Verbal requests then follow the same procedures as written requests.

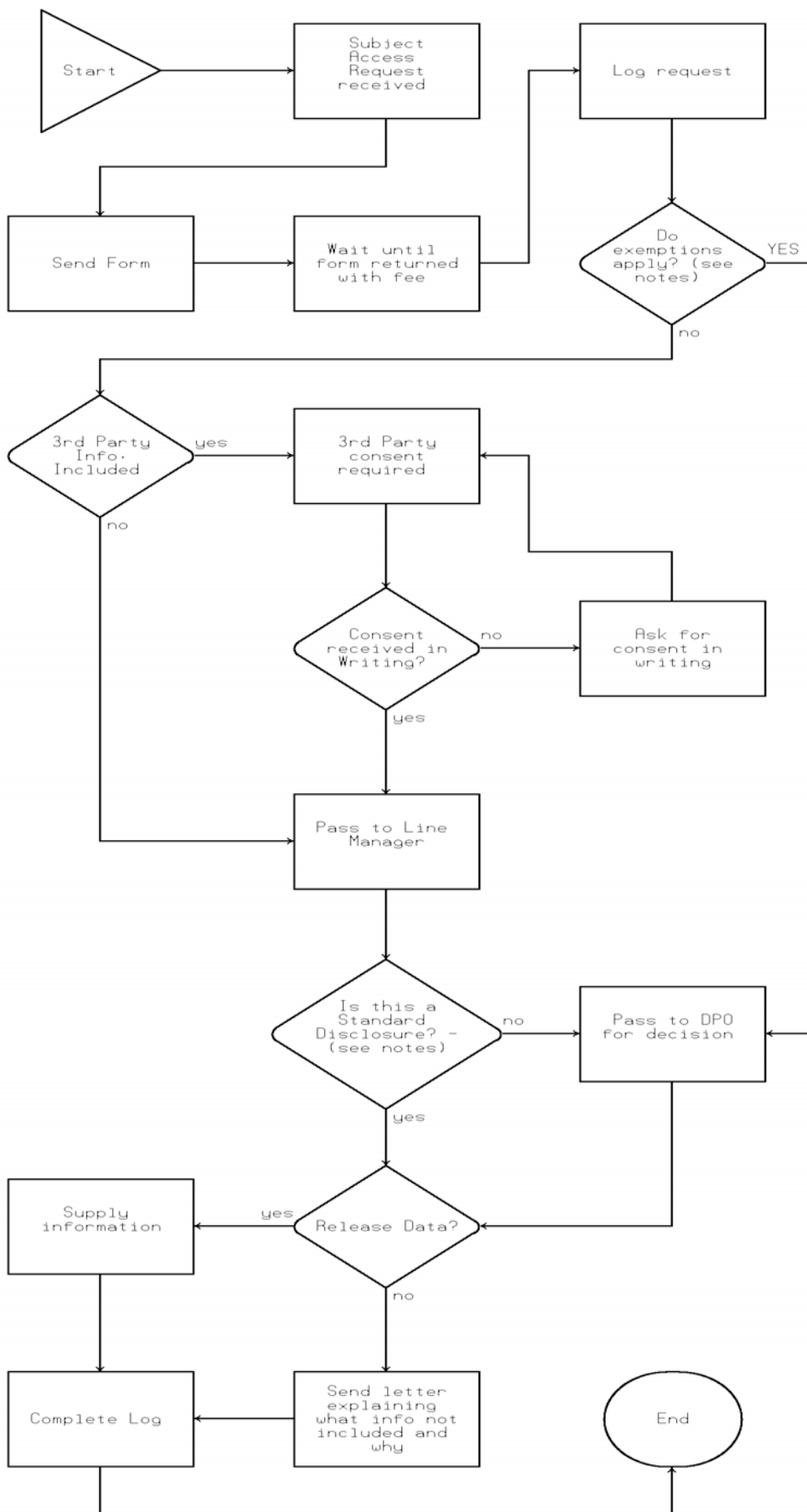


## **Subject Access requests**

The Data Protection Act provides that, subject to certain exceptions, a data subject can request access or a copy of the personal information that we hold about them.

They must do this on a Subject Access Request Form, which should be submitted with the appropriate fee. The Council must then provide the data within 40 days of receiving the request and fee. If the Council is unable to supply the information for any reason the data subject will be advised in writing.

The Subject Access Request Forms are available from the Portfolio Administration Managers. Further information on subject access rights is contained in the leaflet entitled "Personal Information – Your Right to Know". (Appendix H)





## Procedure for Handling Requests to Disclose Information

### Introduction

The Data Protection Act 1998 gives all individuals (Data Subjects) the right to see and obtain a copy of any information that is held about them by others. This right applies to anyone about whom the Council holds information – staff, ex-staff, residents, service users, suppliers, Contractors, etc. The Council is required to provide the information no matter who the data subject is. To exercise this right, Data Subjects make what is known as a **Subject Access Request**. The Council is legally obliged to respond to requests within 40 days. To fail to do so is a breach of the Act and could lead to a complaint to the Information Commissioner.

The Council may also receive requests from third parties for information about data subjects. The Council terms these requests **Agency Subject Access Requests**.

### What is the difference between a Subject Access Request and an Agency Subject Access Request?

#### Subject Access Request

A Subject Access Request is a request made by the Data Subject for information about themselves and the Data Subject does not have to give a reason for requiring the information.

#### Agency Subject Access Request

The Council can disclose personal data, in certain circumstances, where it is permitted to do so by law, to third parties. The most common examples of where the Council can disclose information are outlined below.

- ▶ Prevention or detection of crime
- ▶ Prosecution and apprehension of offenders
- ▶ Assessment or collection of any tax or duty
- ▶ In the vital interests of the data subject
- ▶ Disclosures required by law or made in connection with legal proceedings
- ▶ A request by an elected member for information about a constituent on whose behalf they are working
- ▶ With the written consent of the data subject or on production of a Power of Attorney

The Agency Subject Access Request form asks for reasons why data should be disclosed. **This is very important**. The Council must be given a proper reason by the person or organisation requesting the data in order to release it. The Officer making the disclosure must be satisfied that this is a valid reason. If you are not sure – seek advice from your Line Manager or Data Protection Officer.

The Council may also be able to disclose in other specified circumstances but these should be referred to the Data Protection Officers for their view before disclosure.

These requests can come from a variety of sources, e.g. the Police, a solicitor acting on behalf of a Data Subject, Fraud Investigation agencies.

## Procedures for handling Subject Access Requests



This procedure is to assist staff to respond to a request from a Data Subject for information that the organisation holds about them. A list of officers nominated by their Corporate Manager is attached.

The Policy Portfolio Administration Manager will be monitoring the requests to ensure that they are all dealt with within the 40-day deadline. This has been decided so that requests which ask for information from more than one system can be distributed as soon as the request has been received rather than get delayed in a department while part of the request is being dealt with. Initially the requests are to be monitored for completion using the Tasks facility within Groupwise. A separate Groupwise address – Data Protection – has been set up for this purpose.

### **Step 1 – Receiving a valid request**

Requests made in person or by telephone. If the Data Subject makes a request for their record in person or by telephone, advise him or her that requests must be made in writing and provide them with a copy of the Subject Access Request form (by hand or post) together with a letter (See Example Letter 1).

### **Step 2 – Recording the request**

The completed form, fee, and relevant identification, should be returned to one of the two Portfolio Administration Managers. The Portfolio Administration Manager will check that the form has been completed with sufficient details to enable the data to be found. Once sufficient data has been supplied to enable the request to be processed the Portfolio Administration Manager will record the date and pass a copy of the form to the relevant Line Manager(s) to enable them to process the request. An email Task, with a 20-day completion date, will also be sent to the Line Manager so that we can ensure that we meet the deadline. Details of how the task is to be set up are attached with the recommended wording for the task.

The Task will appear in the Mail Box. As soon as it has been accepted it will move to the Task list and show in the Calendar until completed.

Fees – The Council is permitted to charge a fee of up to £10 for a Subject Access Request, and it is our policy to make this charge.

The statutory 40-day deadline period for responding begins once all the information required to start processing the request has been received. The Act makes no allowances for holiday periods or public holidays.

### **Step 3 – Acknowledging, clarifying and verifying the request**

Send the Data Subject a standard letter of acknowledgement within seven days of receipt of the form and fee (See Example Letter 2).

Record the date you sent the acknowledgement letter and the date and outcome of any other contacts with the Data Subject, using the back of the Subject Access Request form.

The right of Subject Access applies whatever the motive of the data subject for seeking the information. You are not permitted to ask the data subject why they require the information. Even where the data subject tells you about their intention to use the data, for example, for legal action, this does not entitle you to refuse.



#### Step 4 – Finding and checking the requested information

Search for the requested data on the relevant databases, computer or email systems or in your paper filing systems. Print out or photocopy all the requested information, then:

- ▶ Check the material for any references to third parties and delete, block, retype or get consent in writing
- ▶ Check that any explanations, for example of codes or acronyms, are included
- ▶ Decide whether there are grounds for withholding any information under the Exemption (See Section entitled Subject Access Request Exemptions)
- ▶ Record what material you withhold and the exemptions you have used

#### Step 5 – Preparing to release the information

Prepare a letter (See Example letter 4) to accompany the information you intend to release. In this letter you should describe:

- ▶ The personal data
- ▶ The purposes for processing the data
- ▶ Information about the people or organisations to whom you might disclose the data

Provide, if you have it, information on the sources of the personal data.

Ensure that you add your contact details, so that the Data Subject can advise you whether he or she thinks that any information is inaccurate or incomplete.

#### Step 6 – Responding where no information has been found

If no information has been found, send a letter to the data subject indicating this, or, if none of the data can be released, state that there is no information you are required to give (See example letter 3). There is no requirement to explain the reason for withholding information.

#### Step 7 – Finalising the request

Once you have sent off your final correspondence to the Data Subject, record the date you finalised the request on the back of the request form. Keep all documentation on file for a maximum of two years in case any further action is required. Advise the Portfolio Administration Manager the date that the information was released by completing the Groupwise task. This is done by clicking on the completed box at the bottom right-hand corner of the task. The Portfolio Administration Manager will update the master copy of the request.

If the Data Subject indicates that the information about him or her is inaccurate or claims that the processing causes them damage or distress, liaise with the Data Protection Officer and investigate.



## Subject Access Request Exemptions

You are permitted to withhold the following:

▶ Information that is likely to prejudice any of the following purposes:

- prevention or detection of crime
- the apprehension or prosecution of offenders
- the assessment or collection of any tax or duty

▶ Confidential references given by a staff member to a prospective employer

▶ Certain records relating to health, education and social work

▶ Any records of the intentions of the organisation in negotiations with the data subject

▶ Information which is subject to legal professional privilege

▶ Information that would lead to self-incrimination

Ensure that you record any information that you have decided to withhold, noting which exemption you are relying upon.

## Where the requested information identifies other people

Where the requested information identifies other people you need to consider whether to release that information to the Data Subject. There are three actions you can take:

▶ Edit the information so as not to reveal the third party's identity, eg blocking out the text

▶ You can obtain the third party's consent to the disclosure if it is reasonable to do so

▶ You can decide that it is reasonable to disclose the information to the data subject without the third party's consent. However, if you chose this option you need to consider:

- Whether you owe the third party a duty of confidence
- What steps you have taken to get their permission
- Whether the third party is capable of giving consent
- Whether the third party has expressly refused consent
- Whether the information is of particular importance to the data subject

(The European Court of Human Rights has ruled that in certain circumstances the individual's right of access to information is so important that their rights override the third party's rights to confidentiality.)



## Procedures for handling Agency Subject Access Requests

This procedure is to assist staff to respond to a request from a Third Party for information on a Data Subject. It is recommended that Line Managers act as the contact within their area for all Agency Subject Access Requests.

This type of request is likely to come from:

- ▶ Another local authority
- ▶ Police investigating a crime
- ▶ DSS
- ▶ An internal investigation
- ▶ HM Customs and Excise
- ▶ A solicitor acting on behalf of a data subject
- ▶ A family member acting on behalf of a data subject with the data subject's consent.

Some of the reasons for granting this type of request are:

- ▶ The prevention or detection of crime
- ▶ The apprehension or prosecution of offenders
- ▶ The assessment or collection of any tax or duty

Those sections who receive a large quantity of requests from a specific third party may wish to supply the third party with some blank forms to enable these requests to be processed without delay.

### Step 1 – Receiving a valid request

Requests made in person or by telephone. The request must be made in writing; a copy of the Agency Subject Access Request form (sample attached) should be supplied to the third party.

If the request is from, say, one family member on behalf of another family member, then the Data Subject should also sign the request form, unless a Consent form has already been signed.

### Step 2 – Recording the request

The completed form should be returned to the Manager of the Section from whom the data is requested. The Line Manager should record the date of receipt of the form.

We do not make a fee for this information.

There is no statutory deadline period for responding to this type of request. However, speed of response will often depend upon the reason for the request.



## Urgent Requests

Sometimes there may not be time to complete a Disclosure Form before the information is released. The Council is prepared to accept requests verbally providing a faxed request is sent to the relevant Line Manager within 2 hours of the request. Verbal requests must be logged on receipt of the call and there must be a valid reason for disclosing the data before the written request is received. Verbal requests then follow the same procedures as written requests.

### Step 3 – Verifying the reason for the request

Before allowing the data to be disclosed, the Line Manager must be satisfied that there is a valid reason for requesting the data. Any queries on whether or not the data should be disclosed should be discussed with the Data Protection Officer. The reasons for releasing the data or not should be noted.

The reason for those requesting information from the Council Tax system should be backed-up by stating the Statutory regulation which would authorise this access.

### Step 4 – Finding and checking the requested information

Search for the requested data on the relevant databases, computer or email systems or in your paper filing systems. Print out or photocopy all the requested information, then:

- ▶ Check the material for any references to third parties and delete, block, retype
- ▶ Check that any explanations, for example of codes or acronyms, are included
- ▶ Decide whether there are grounds for withholding any information.
- ▶ Record what material you withhold and the exemptions you have used

### Step 5 – Preparing to release the information

Prepare a letter (See Example letter 4) to accompany the information you intend to release. In this letter you should describe:

- ▶ The personal data

Ensure that you add your contact details, so that the Third Party can advise you whether he or she thinks that any information is inaccurate or incomplete.

### Step 6 – Responding where no information has been found

If no information has been found, advise the Third Party that no data has been found or none of the data can be released.

### Step 7 – Finalising the request

Once you have released the information update the request record. Keep all documentation on file for a maximum of two years in case any further action is required.



## Example letters

### Example Letter 1 – Request for Information/Verification details/Fee

Thank you for your recent enquiry about access to data under the 1998 Data Protection Act. In order that we can meet your request, we would be grateful if you could complete and sign the attached application form and return this to us together with proof of identity as specified in the form, together with the fee of £10.

Upon receipt of your Subject Access Request form we will use the information supplied by you to search our files and systems for the data relating to you that you have requested. Our findings will be forwarded to you *by recorded delivery/available for you to view (whichever is appropriate)*, within 40-days of the receipt of the completed form and fee.

### Example Letter 2 – Acknowledgement

Thank you for returning the completed application form for access to your information under the 1998 Data Protection Act. We also acknowledge receipt of the fee of £10 and the information you have provided by way of proof of your identity.

Arrangements have been made to use the information supplied by you to search our files and systems for data relating to you. Our findings will be *forwarded to you by recorded delivery/available for you to view, (whichever is appropriate)* on or before the *deadline date*.

### Example Letter 3 – No relevant information found

Further to our letter of *dd/mm/yy*, we have completed the search of our files and systems for data relating to you.

Based on the details supplied by you on our application form, we can confirm that no information required to be supplied, under the Data Protection Act 1998, has been identified.

We trust you are satisfied with our findings, however, please do not hesitate to contact us if you would like to discuss this further.

### Example Letter 4 – Information enclosed

Further to our letter of *dd/mm/yyyy*, we have completed the search of our files and systems for data relating to you.

Based on the information supplied by you on the Subject Access Request form, the enclosed information has been traced (*and transcribed into an easy-to-read format for your convenience*).

*Insert paragraph about any inaccuracies etc. discovered.*

Also enclosed are details about the purposes for which the enclosed information is processed, its source and any recipients to whom the information may have been disclosed.

We trust you are satisfied with our findings, however, please do not hesitate to contact us if you would like to discuss this further.



## Suggested wording for the task:

### Subject Access Request

#### We have received a Subject Access Request from

*Insert full name*

*Insert full address*

Requesting a copy of the personal data we hold on him/her in

*Insert name of system*

A copy of the Subject Request Form has been despatched to you in the internal mail today.

Can you please process this request *by date*, using the Council's "Procedure for Handling Requests to disclose information".

When you have finished dealing with the request please update this Groupwise task as completed (by clicking in the completed box at the bottom right-hand side of the screen) to advise the Policy Administration Manager, so that the request can be closed.

### To set up the Task

Proxy to the Data Protection User

Click on Insert Task

Select File, Properties

Select Send Options

Set Priority to High

Click on Reply requested

Set no of days to **20**

Click on OK

Select Status Tracking

Click on Return Notification

When Accepted and

When Completed

Click on OK

Send to relevant officer with a Blind copy to Data Protection



<b>Department</b>	<b>Nominated Officer</b>
Human Resources	Jill Elsworthy
Payroll	Jill Elsworthy
Tenancy Services: Inc Rent Accounting, Estates Management, Sheltered Housing Housing Maintenance-	David Howson
Property Services	David Jessop
CCTV	John Bunyard
Housing Allocations Homelessness Housing Advice Housing Strategy/Enablement	Alan Keely
Policy	Robert Holmes
Council Tax	Chris Sharman
Benefits (Council Tax and Housing)	Julie McCarthy
Food & Safety Housing Grants Environmental Health Pest Control	Andrew Reynolds



## DATA RETENTION POLICIES

Internal Audit has produced a report entitled “Storage of Records” in which they list retention periods. These retention periods are not specified by the Data Protection Act, but by other legislation, and would be enforceable under the Data Protection Act principle 5 – personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

### Storage of Records

#### 1. Introduction:

Stated retention periods are generally from the end of the financial year to which the documents relate.

Audit	Period
Permanent File Information	Indefinitely
Working paper files	Until next audit (unless of a special nature, e.g. fraud)

Council Tax / NNDR / Community Charge	Period
Valuation/Banding lists	Indefinitely
Valuation Officer's Directions	Indefinitely
Charges information, etc.	6 years
Computer Log print-outs	2 years
Correspondence	6 years

Housing Benefit	Period
Claim forms, supporting documents and correspondence	3 years
Payment listings	6 years

Creditors	Period
Copy Orders	3 years
Delivery Notes	12 months
Periodical Payments Register (Dead Cases)	3 years
Paid Invoices	6 years
Paid Cheques/Copy Cheques	Held by bank
Bank Statements	6 years
Petty Cash Claims	6 years
Petty Cash Claims (Departmental Copy)	1 year
Improvement Grant Cheque (Requisition Copies)	1 year



<b>Contract Records</b>	<b>Period</b>
Register of Tenders/Quotations	Indefinitely
Contract Documents (under seal)	12 years
Contract Documents (not sealed)	6 years
Unsuccessful Tenders/Quotations	1 year
Final Account Documents	12 years
Contracts Register	Indefinitely
Contract Payment Certificates (Office Copies)	1 year

<b>Rent Records</b>	<b>Period</b>
Giro Payment Stubs	1 year
Rent Computer Records	6 years
House Files	6 years

<b>Salaries and Wages</b>	<b>Period</b>
Time Sheets	3 years
Taskpay/Bonus Sheets	3 years
Overtime Claims	3 years
Car Allowance Claims	3 years
Pay-rolls	6 years
Inland Revenue Returns	6 years
National Insurance Returns	6 years
Staff Files (Contract of Employment, Sickness records etc.)	7 years from termination of employment
Copy Cheques/Paid Cheques	6 years
BACS Control Records	6 years
Members Allowance Claims and Payment Records	12 years

<b>Costing</b>	<b>Period</b>
Stores Requisitions	1 year
Stock Records	1 year
Vehicle Running Sheets	1 year
End of Year Expenditure and Income Records	6 years
Rechargeable Works Orders	6 years
Journal (transfer) details	1 year



<b>Housing Act Advances</b>	<b>Period</b>
Payment Records	3 years
Mortgage Documentation	1 year from redemption date

<b>Income - General</b>	<b>Period</b>
Periodical Income Register	3 years
Sundry Debtor Accounts	3 years from final payment
Income Returns from departments	3 years
Income Returns (Departmental copies)	1 year
Cash Office Documentation	3 years
Completed Receipt Books, etc.	3 years
Completed Paying-In Books	3 years
Till Rolls, "Z" clearances, etc..	3 years
Car Loan Repayments and other Payments by Instalment	1 year from final payment
Car Park Summaries, etc..	3 years
Excess Charge Notice Copies	3 years
Concessionary Fares Returns	3 years
Chief Executive Licences, etc..	3 years
Receipt Books (Dept. Copies)	1 year from last issue
Cemetery Receipts/Certificates (Office Copies)	Indefinitely

<b>Accounting - General</b>	<b>Period</b>
Bank Statements	6 years
Receipts and Deposits Book	6 years
Post-dated Cheques Records	6 years
Returned Cheques Records	6 years
Cheque Usage Records	6 years
Insurance Policies (Public & Product liability)	Indefinitely
Insurance Claims (dependent on type)	3-31 years from settlement
Year End Final Accounts	6 years
Estimate Working Papers	3 years
Annual Report and Accounts (Central Service's Dept. Copy)	Indefinitely
Budget Book (CeS Dept. Copy)	6 years
Parish Council Precept Documentation	6 years



<b>Loans</b>	<b>Period</b>
Register of Temporary Loans	Indefinitely
Register of Bonds	Indefinitely
Copy Certificates	6 years from redemption
Copy Cheques/Paid Cheques	6 years

<b>Computer Records</b>	<b>Period</b>
Data Files held on Floppy/Hard disks	Retain as per written records or until hard copy produced for record purposes
Computer Logs	6 years
Control Reports	3 years
Vet Listings	3 years
Update Reports	3 years
Microfiche	As per written records

<b>Licences</b>	<b>Period</b>
Hackney Carriage Licences & Associated Information }	3 years from date of expiry of Licence
Copy Taxi Vehicle Licence }	
Copy Drivers Licence }	
Private Hire Vehicle & Operator's Licence }	

<b>General</b>	<b>Period</b>
Council Minutes	Indefinitely
Deed Packets	Indefinitely
Financial Regulations/Standing Orders	Indefinitely
Land Charges Copy Certificates	6 years
General Correspondence Files	Indefinitely depending on contents

This list is not exhaustive, contact Internal Audit for other areas.



## List of Data Protection Forms/Leaflets

Form/Leaflet Title	Ref No.
<b>Customer Alert List:</b>	
Policy	<b>CP-56</b>
Declaration	<b>CP-41</b>
Report Form	<b>CP-42</b>
<b>Data Protection Forms:</b>	
Data Subject Consent Form	<b>CP-53</b>
Change of Address Form	<b>CP-54</b>
Leaflet – Your Right to Know	<b>CP-37</b>
<b>Requests for information:</b>	
Request for information from Elected Member	<b>CP-55</b>
Subject Access Request Form	<b>CP-39</b>
CCTV Subject Access Request Form	<b>CP-40</b>
Request for Council Tax Information	<b>CP-57</b>
Request for information from Electoral Roll	<b>CP-52</b>
Agency Subject Access Request Form	<b>CP-38</b>
Request for Housing Benefit information	<b>CP-58</b>
Request for information from DVLA	<b>CP-59</b>
Policy on use of Images	<b>CP-455</b>
Verbal consent for use of image	<b>CP-456</b>
Consent for use of image of subject under 18 years	<b>CP-457</b>
Consent for use of image of subject	<b>CP-458</b>