



Name of Strategy / Policy: Data Sharing Policy

Date last updated: March 2009

Links to Council Priorities:

Priority	Linked Yes / No?
Environment – Civic Pride	No
Regeneration and Homes	No
Improving the Council	Yes
Community Safety	No

Links to Other Strategies and Policies

RIPA

Data Protection and Freedom of Information

Action Plan in this document?

No

Is progress on the action plan regularly updated?

n/a

Officer Monitoring

Andrew Smith is the Council's Data Controller

Member Monitoring

Name of cabinet portfolio holder responsible for over viewing progress of the Strategy / Policy (if applicable):

Member forum for agreeing the policy / strategy (if applicable):

Has it been subject to a Diversity Impact Assessment? Yes

Has it been subject to an Environmental Sustainability Impact Appraisal? n/a



Privacy Vs Data Sharing

This Guidance has been prepared jointly between Southend Borough Council and Castle Point Borough Council and sets out practical advice that will help those involved in information sharing between Departments and/or with External Organisations.

Those organisations who have agreed to comply with this guidance when sharing personal information are listed in Appendix F

Version Control

Date	Version	Reason	Owner	Author
15/2/2009	Draft 1	Outline Draft	Southend Borough Council - Jackie Groom	Indie Viknaraja
2/3/2009	Draft 2	Outline Draft	Castle Point Borough Council - Fiona Wilson	Fiona Wilson

This document is to be agreed and approved by:

Title	Approved by	Date
Southend Borough Council:		
Strategy & Performance Manager		
Corporate Director – Support Services		
Head of Legal Department		
Head of Customer Services		
Head of HR		
ICT Strategy Group		
Caldicott Guardians: Head of C&L - Sue Cook Head of ACS - Derek Sleigh		
Castle Points Borough Council:		
Operational Management Group		
Executive Management Team		
Cabinet		

Introduction

This document takes into consideration the Framework Code of Practice for sharing personal information issued by the Information Commissioners Office in October 2007 and will be subject to at least an annual review by the Head of Legal Services.

This document attempts to highlight the issues that need consideration when sharing information whether internally (between different departments) or with external organisations.

It can also be applied to authenticate one - off disclosure of Personal Information.

It outlines relevant legislation, considers issues of confidentiality and when consent is required so that information sharing can be based on solid reasoning, rather than finding reasons not to share.

Appendix D sets out a series of questions you should ask yourself which will enable you to evidence and justify sharing personal information to meet the objectives for which you seek to share that information.

Background

Local government is in a phase of transformation - this is a result of forces coming from both within and outside local government. Historically, local authorities have not used information in a joined up manner. Councils have been arranged in a silo fashion, with departments not working in a joined up manner.

Local government is changing the way it uses information. The aim of these changes is to provide more effective, efficient and seamless public services to their citizens. For example a person may be a tenant of the housing department, but also have financial needs for which they may apply for benefits, and that person may be in receipt of special relief in terms of council tax. To handle an enquiry from that person holistically, data from functional systems collected by Housing Services, Benefits and Council Tax may need to be accessed by front-line customer service staff within the authority. This may often be facilitated by the Council's CRM system First Contact.

This is simply an example of internal data sharing by the Council. Local authorities also share data externally with other councils and other public organisations such as the PCT or the Police.

However, legal questions have arisen over what data sharing councils can legally do under the current law. For example the use of CRM systems in councils has been questioned; customer friendly processes such as corporate change of name and address systems are challengeable; and for some data, such as council tax information (sometimes used as the basis for CRM systems) specific legislation prevents data sharing with other functions.

Many councils have taken a somewhat pragmatic approach to this situation by electing to move ahead on projects while attempting to minimise the risks of them being in breach of the law. However, for a public body it is not simply a process of risk/loss analysis of breaking the law as it is for the private sector, there is a bigger picture that needs to be considered. Can a local authority, which is responsible for enforcing various statutes, be seen flouting the law elsewhere? Some councils have expressed a concern that breaking privacy law would give them a serious problem with credibility and public perception.

Issues

The issues boil down to the question: what information can local authorities share, who can they share it with and in what circumstances?

To find a way in to this query, an initial step could be to divide the issues into Data Protection Act (DPA) issues and non-DPA issues. (There is, however, a crossover between the two areas because if an instance of data sharing is not lawful, it trips the first of the eight DPA principles - processing must be 'lawful'.) It is probably most useful to begin with non-DPA issues.

Non-DPA issues

Council Tax information

The Local Government Finance Act 1992 (LGFA) precludes use of Council Tax information for anything other than council tax. There are exceptions under the Data Protection Act in certain circumstances, i.e. where it may be used for criminal or fraudulent activity. Council Tax information is the closest thing most councils have to a complete dataset for their citizens and the land in their area. This makes Council Tax information an obvious base upon which council - wide CRM systems can be built. There are now in place certain shared systems that enable sharing of information through central databases i.e. LOCTA EXPERIAN.

Part 2A of the Audit Commission Act 1998 provides statutory authority for the Audit Commission to undertake a data matching exercise subject to a Code of Practice which involves Council Tax information and the Electoral Register. See **Appendix E**

Vires

Councils, being statutory bodies, must always be able to point to a statutory power that allows for each and every action they do. Thus, surprisingly, even if a citizen or client gives their 'informed consent' for their information to be shared, the Council must still point to a statutory power that allows it to share data in the way intended, otherwise it may be acting '**ultra vires**', or **without authority**.

As mentioned local government is in the process of joining up on three different levels: within councils, between neighbouring councils and council tiers, with local agencies and government departments on a local level.

A basic question can then be asked - do local authorities have statutory authority, or vires, to share information? But that question needs to be broken down at each level, in every instance finding statutory power to share data. Each service line must ask the question for any particular information sharing it is participating in, for each of the different organisations it is sharing information with. This is by no means a simple or straightforward task.

Data Protection Act issues

Local government is a unique type of organisation with a tremendous amount and variety of information which flows, both internally and externally. Probably the greatest challenge for local government is ensuring that the numerous data flows adhere to the eight principles in the DPA.

The Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are 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 territory or country 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.

In addition there are also principles governing information sharing:

- a) Justify the purpose(s) for each transfer of information.
- b) Do not use personally identifiable information, unless it is absolutely necessary.
- c) Use the minimum necessary personally identifiable information.

- d) Access to personally identifiable information should be on a strict need to know basis.
- e) Everyone should be aware of his or her responsibility to respect confidentiality.
- f) Information should generally only be shared with the informed consent of the individual.
- g) Personal identifiers should be removed unless specially needed.
- h) Technologies used in information sharing must be fully fit for the purpose.
- i) Individuals and organizations should understand and comply with the law.

An issue that is of particular note to local government is the interpretation under principle two of the DPA of the "purpose" for which information is gathered. Local government performs many different functions at a local level. It is not always clear whether information gathered for one purpose can be used by the council in performing its other duties.

Purpose

To provide guidance in a number of areas, to enable informed decisions to be made regarding sharing information both internally and externally. While at the same time complying with the legislation and requirements concerning the security and confidentiality ascribed to personal information.

Compliance with these guidelines will ensure compliance with the Data Protection Act 1998. Users must however also refer to any regulations or statutes relating to their service that might introduce additional restrictions or exemptions.

These guidelines are designed to set the minimum standard for sharing personal information. It is not designed to replace existing protocols where these meet or exceed the requirements of these guidelines. Although it does provide guidance for situations where there is currently no protocol in place.

Requirements for Fair and Lawful Processing

The first of the Data Protection Principles is that processing (including disclosure) must be fair and lawful and that at least one of the conditions for processing must apply. There are two sets of conditions Schedules 2 or 3 (**Appendix C**) and the relevant/correct set depends on whether or not the information is "sensitive" data. (**Appendix B**). Of these conditions Consent and Legal Obligation are most important.

- a) **The subject has consented.**
These guidelines require subject consent to have been obtained whenever this is possible (see "The Principle of Consent"). The subject should also have been told that the information is being held.

- (b) **It is required in the context of a contract or to form a contract with the subject.**

The subject is a party, or intends to be a party, to a contract and their consent has been obtained.

(c) **To comply with a non-contractual legal obligation.**

Examples: Employers are required to provide information to the Inland Revenue and some schools may be required to maintain details of test results. The local authority's obligation to perform a particular function should always be traced back to a statutory power or duty.

(d) **To protect the vital interests of the subject**

The use of this condition is restricted. It should be used if disclosure is necessary for matters of life and death or to prevent significant harm to the subject. For example, it could be used to provide information to a hospital on an allergic reaction to drugs.

(e) **For a public function.**

As exercised by the courts, the police or central government.

(f) **For the purpose of the legitimate interests of the organisation**

Only where the rights of the individual are not prejudiced for example: the right of privacy and / or the common law of confidentiality.

(g) **To comply with an Order of the Secretary of State**

The Principle of Consent

Obtaining consent from the subject is one of the conditions under Schedules 2 & 3 of the Data Protection Act 1998 that ensures fair and lawful disclosure of personal information. This guideline requires consent to be obtained when necessary, to ensure fair and lawful processing, unless it would compromise the objectives of using of other legal powers.

If the information is sensitive information (see Appendix B) there are more demanding requirements, in that consent must be explicit (i.e. in writing) and cannot be inferred (see below). If explicit consent is not given, disclosure must be carried out with appropriate safeguards to protect the rights and freedoms of the individual.

Explicit consent should always be:

- freely given and involve no coercion
- specific to certain information and not a general consent
- informed in as far as the subject should be aware of:
 - a) the purpose and use of the information
 - b) any way in which they might be affected

Inferred Consent

If reliance is to be placed on "inferred" consent to justify information exchange, this should be supported by clear and effective policies for informing subjects about what may happen to their information. For example, an information form may state that information provided may be passed to another agency for a declared purpose (which should be consistent with the main purpose of collection). If the subject responds and raises no objection then consent may be inferred. Where there is no response at all it cannot be inferred as consent. Consent also cannot be inferred for sensitive (**see Appendix B**) information.

Withheld Consent

If reliance is only to be placed on obtaining consent, and not on other powers, and the subject raises objections or withholds consent, these wishes must be respected.

Overriding Consent

The exceptional circumstances that override an individual's wishes can arise:

- when the information is required by statute or court order
- where there is a serious public health risk or risk of harm to other individuals,
- where it is in the public interest
- for the prevention detection or prosecution of crime.

Responsibilities of the Transferor

It is for the agency or department passing the information to be satisfied that consent has been obtained or obtain confirmation of the validity of the legal power that is to be used to facilitate exchange.

Individual Transfers

Specific consent is not required for each individual transfer of information performed.

Vulnerable People

Those providing services to adults and children, or vulnerable adults must balance their duties to protect subjects from harm and their general duty towards their service users.

Young people of 16 and over are regarded as adults regarding both consent and the duty of confidentiality; the same effectively applies to those under 16 "with the capacity and understanding to take decisions". For the rest it will be a person with parental responsibility.

For adults unable to give consent the decision should be taken by those responsible for providing care, taking carer's view into account with the subject's best interests being paramount.

Duration of Consent

Consent should generally be considered to have expired once processing is completely finished (that would include consent to annual processes for example). Consent should not be taken as given in perpetuity unless this has been made clear to the subject.

Fairness and transparency

Personal Information must be processed fairly. Processing won't be fair unless the person has, is provided with, or has readily available:

- Information about your identity
- Information about the purpose the information will be processed for and
- Any other information necessary to enable the processing to be fair

“Fair Processing Notices” or “privacy policies” are intended to inform people the information is about how it will be shared and what it is will be used for. The notice must be drafted in a way that the people it is aimed at will understand. Drafting notices for children and other whose level of understanding may be relatively low will required particular care and therefore you should adopt a plain easy to read approach. An example of Fair Processing Notices are attached (**see Appendix E**)

You must still decide whether a single fair processing notice is enough to inform the public of all the information sharing that you carry out as in some cases it would be good practice to produce a separate fair processing notice for a particular information sharing initiative. One such example is the National Fraud Initiative. (**see Appendix E**)

Staffing Issues

All organisations and departments must ensure that their employees understand any protocols produced and how to use it. Training in Data Protection and the information sharing will be necessary.

Security of Information

Departments must have the arrangements in place for safeguarding the security of information. This will include:

- **Organisational accountability:** Each information sharing arrangement should have a confidentiality guardian (for Social Care a Caldicott guardian) responsible for the protection of individual information.
- **Policies: for physical security,** security awareness and training, security management, information and IT security. (see IT Corporate Information Security Policy **Appendix A**).
- **Effective password protection:** for all information systems; users must not divulge their password or leave systems active while absent.

- **Policies:** to ensure that only minimum information is shared, for example different versions of letters or forms to different recipients.
- **Secure:** environmentally controlled locations for all personal files and confidential information when unattended e.g. locked cabinets or security protected computers.
- **Disposal:** each department should have a policy on the disposal of individual identifiable information. Redundant IT equipment should be disposed of via a Corporate Disposal Procedure(see **Appendix A**)
- **Rules for access:** to electronic and paper information and for exchanging information by telephone and fax.
- **Documentation:** of routine information flows and arrangements for anything outside these to be referred to confidentiality guardians.
- **Arrangements covering temporary staff:** and others such as independent researchers to whom access to information is agreed.
- **Arrangements affecting the passing of information to third parties:** such as other providers; these must incorporate the same principles as those outlined in these guidelines.
- **Requirements for external contractors:** e.g. window cleaners, regarding confidentiality.
 - **Requirements for external organisations** who are providing a service on behalf of SBC, e.g. managed services, partnerships etc. They may acquire the status of **Data Processors** and there is a legal obligation on the Authority to protect any Personal Information they process on our behalf (**see Appendix A**).

Access to Records

Subject's service users and employees have legal access rights to their records except where there are specific reasons to restrict access under the Data Protection Act 1998 (**see Appendix A** Supporting Documents and Guidance).

It is essential that the definitions of the exemptions be checked to ensure that they apply to the particular situation.

Legal Requirements

Common law duty of confidence

Personal information is subject to a common law duty of confidentiality where:

- a) The information has 'the necessary quality of confidence', i.e. it must not be something which is public property and public knowledge.

- b) The information must have been imparted in circumstance imposing an obligation of confidence.

While the Data Protection Act is concerned only with living identifiable individuals, the common law of confidentiality is generally felt to apply to the deceased also.

Data Protection Act 1998

Covers all "personal information" relating to living individuals that are held either on computer systems or "relevant" [structured] manual filing systems. From January 2005 the Freedom of Information Act changes the definition of manual information within the Data Protection Act to include unstructured information. It is a criminal offence to hold or disclose information in breach of the requirements of the Act.

The Computer Misuse Act 1990

Provides criminal sanctions against the unauthorised access or damage to computerized information.

Individual Service Regulations

Individual services may have legislation or government guidance that supplements the above laws. It is important that information sharers are fully aware of these.

Freedom of Information Act 2000

This Act places duties on public authorities to publish details of the information it holds and to publish and disclose information.

Code of Practice for Sharing Information

Using this Code of Practice will help employees to make sure that they address all the main data protection compliance issues that are likely to arise when sharing information. This in turn should help the Council and its staff to make well informed decisions about sharing personal information.

Appendix D sets out a series of questions you should ask yourself and to help the Council establishes good practice and to comply with the law in striking a balance between sharing personal information and protecting the people it's about.

Sharing information may involve two or more organisations sharing information between them or sharing information between various parts of the Council and the questions should be relevant for both aspects of sharing information.

Summary

Before any information about individuals is shared, the parties involved need to be satisfied that confidentiality will not be breached. A duty of confidence arises when one person discloses information to another (e.g. patient to clinician, client to social worker) in circumstances where it is reasonable to expect that the information will be held in confidence. Sources that help define confidentiality include:

- The Data Protection Act 1998
- Freedom of Information Act 2000

- The Human Rights Act 1998
- Common Law of Confidentiality
- Administrative Law.

A Protocol for the Secure and Confidential Sharing of Personal Information is available. This protocol which is based on the Essex Trust Charter will help cover as many scenarios as possible and will also provide a proactive framework built around a **desire** to share as opposed to a **need** to share. It has been structured to cover the following questions:

- What data do we want to share?
- With whom do we want to share it?
- Why do we want to share it?
- How can we justify sharing it?
- How do we comply with the law?

Appendix A

Supporting Documents and Guidance.

There are a number of procedures and guidance documents available on the Council's INTRANET in the Data Protection and Corporate Policy areas that support and reinforce these guidelines. The key ones have been identified below:

[Protocol for the Secure and Confidential Sharing of personal information between Organisations](#) – based on the Essex Charter (Draft Jan 2009)

[Data Protection Guidance Leaflet](#) (Jan 2009)

[IT Policy:](#)

[Secure transit of files – Code of Practice – Portable Computer Storage Devices](#)
– updated Dec 2008

[Acceptable Use Policy \(Draft\) – Remote Workers](#) – updated Jan 2009

[Data Processors](#) – organisations that carry out functions on behalf of the Authority

[Corporate Disposal Procedure](#)

In addition the Information Commissioners Office website provides a number of good practice and technical guides: www.ico.gov.uk

Appendix B

Sensitive Personal Data

The Act introduces categories of sensitive personal data, namely, personal data consisting of information as to:-

- (a) the racial or ethnic origin of the data subject
- (b) their political opinions
- (c) their religious beliefs or other beliefs of a similar nature
- (d) whether they are a member of a trade union
- (e) their physical or mental health or condition
- (f) their sexual life
- (g) the commission or alleged commission by them of any offence, or
- (h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Appendix C

Conditions in Schedule 2 and 3 to the Data Protection Act 1998

Conditions in Schedule 2:

- 1 The data subject has given consent to the processing.
 - 2 The processing is necessary for (a) the performance of any 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.
- 6(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.

Conditions in Schedule 3: (applies to Sensitive Personal Information)

- 1 The data subject has given explicit consent to the processing.
- 2 The processing is necessary for the purposes of exercising or performing a legal right or obligation in the context of employment.
- 3 The processing is necessary to protect the vital interests of the data subject or another in cases where consent cannot be obtained.
- 4 The processing is of political, philosophical, religious or trade union data in connection with its legitimate interests by any non-profit bodies.
- 5 The processing is of information made public as a result of steps deliberately taken by the data subject.

- 6** The processing is necessary in connection with legal proceedings or the seeking of legal advice.
- 7** The processing is necessary (a) for the administration of justice; (b) for the exercise of any function 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.
- 8** The processing is necessary for medical purposes and is carried out by medical professionals or others owing an obligation of confidence to the data subject.
- 9** The processing is necessary for ethnic monitoring purposes.
- 10** The personal data are processed in circumstances specified in an order made by the Secretary of State for certain purposes.

The Data Protection (Processing of Personal Data) Order 2000 (SI 2000 No 417) specifies a number of circumstances in which sensitive personal data may be processed such as for crime prevention, policing and regulatory functions (subject to a substantial public interest test); counselling (subject to substantial public interest test); insurance, equality monitoring in the area of disability and religious or other beliefs; and research. A further order relates to the processing of sensitive personal data by MPs and other elected representatives (The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002)

Appendix D

Sharing Personal Information Questionnaire

Data Protection Act 1998

Remember the law requires that any information sharing must be necessary and any information shared must be relevant and not excessive.

Retain the responses to this questionnaire with your records as evidence that you have assessed the benefits of sharing information against any negative effects such as erosion of personal privacy or likelihood of damage, distress or embarrassment being caused to individuals.

Name:

Dept./Service

(person seeking to share information)

Who will be responsible for dealing with compliance issues that may arise as a result of sharing personal information?

Name:

Deciding to Share Information

Question 1 Set out below why you want to share personal information and the benefits you expect to achieve: *what is the objective you hope to achieve and is sharing personal information proportionate or can information be anonymised or be in statistical formation instead such as demographic information*

Question 2 Appraise the likely effect of sharing this information on the people the information is about and their likely reaction: *Assess any benefits sharing information may bring to these people/person or likelihood of damage, distress or embarrassment that may be caused to these people/person. Any effect should be minimised and only provide the information that is necessary to achieve the benefit sought*

Likely effect:

Likely reaction:

Question 3 Have you considered alternatives to using personal information eg statistical information – set these alternatives out below and

reason why they were not adequate to achieve the benefits you expect to achieve: *anonymise information or as statistical formation instead such as demographic information*

Alternatives:

Reason these would not achieve benefits sought:

Question 4 Describe the information you need to share to achieve your objective, is any of the information sensitive information & the organisations that need to be involved:

Information:

Organisations:

Question 5 Outline relevant legal provisions that require or permit you to share information or prevent you from doing so: *local authorities may share information where it is necessary to carry out its functions however as a public authority local authorities are bound by the Human Rights Act 1998 in particular the right to respect or private and family life. Sharing information must be proportionate.*

Legal provisions:

Question 6 What are the issues that may arise as a result of sharing confidential or sensitive information: *the threshold for sharing confidential or sensitive information is higher because unnecessary or inappropriate sharing of this sort of information is more likely to cause damage, distress or embarrassment to individuals eg health records – see appendix B above*

Potential Issues:

Fairness and transparency

Question 7 Is the individuals consent for sharing information needed and if so how do you intend to obtained consent and what if consent is withheld: *In some instances data protection law provides that it is sufficient that a person knows about sharing of information eg National Fraud Initiative and Fair*

Processing Notices - see Appendix E below. If consent is required it must be specific, informed and freely given.

Is consent required?

What actions will be taken to obtain consent?

Is the information covered by a Fair Processing Notice, if not, would such a notice be appropriate in this instance? *The notice must be legible to the reader, understood and readily available and provide a comprehensive and accurate description of the information that is being share and with whom.*

Is there a Fair Processing Notice in existence: Yes/No

If yes: when was it last reviewed and Yes/No

Is it still appropriate: Yes/No

Is a Fair Processing Notice appropriate in this instance? Yes/No

Can you justify sharing information without a persons consent?

There may be cases where it is legitimate to share information without a persons knowledge or consent for example if a child is put at risk or to safeguard public safety in an emergency or it could prejudice a particular investigation

Yes/No

Reason:

Information Standards

Question 9 Is the information you are sharing adequate, relevant, not excessive, accurate and up to date? *You should check accuracy of information to avoid spreading inaccurate, irrelevant, out of date information and other problems cross systems. If possible information should be collated in a standard format to avoid mismatch or corrupted information especially in IT systems. If possible information you intend to share should be checked with the subject person prior to sharing the information.*

Is the information adequate, relevant, not excessive, accurate and up to date? Yes/No

Retention of shared information

Question 10 Have you specified the retention period for the shared information and if not specified a review period?

Information must not be kept for longer than it is necessary. The longer you retain it the greater the costs, risk and liabilities associated with retaining it and the difficulty of making sure the information remains accurate and up to date.

What retention provisions have you made when sharing information? *(ensure it is in line with your organisations retention policy)*

Security of shared information

Question 11 Have you satisfied yourself that the information you intend to share will be transferred securely and the recipient has accepted responsibility for security of that information.

It is the primary responsibility of the organisation providing the information to make sure the information will continue to be protected by adequate security once other organisations have access to it.

How have you satisfied yourself that the information is secure?

Are you employing another organisation to process information on the Council's *if so there must be a contract in place to make sure the information remains properly protected.*

Yes/No

If yes, date of the contract

Information Sharing Procedure

Question 12 Have you agreed a procedure for sharing information between yourself and the recipient? *Appendix G gives an example of a simple information sharing procedure*

Yes attached.

Appendix E

National Fraud Initiative 2008/2009 - Data Protection Statement

This Authority is required by law to protect the public funds it administers. It may share information provided to it with other bodies responsible for auditing or administering public funds, in order to prevent and detect fraud.

The Audit Commission appoints the auditor to audit the accounts of this Authority. It is also responsible for carrying out data matching exercises. Data matching involves comparing computer records held by one body against other computer records held by the same or another body.

Computerised data matching of personal information allows fraudulent claims and payments to be identified. Where a match is found it indicates that there is an inconsistency which requires further investigation. For the 2008-09 NFI exercise, the following personal data, which is to be extracted on 6th October 2008, will be provided to the Audit Commission:

- Payroll
- Trade Creditor's payment history and standing data
- Housing / Housing Benefits
- Students eligible for a loan
- Private supported care home residents
- Transport passes and permits (residents' parking / blue badges / concessionary travel)
- Insurance claimants
- Licenses - Market trader/operator, Taxi driver and licenses to supply alcohol

Personal data in these categories will be submitted to the Audit Commission from local computers using a secure electronic upload facility.

Access to the information provided will be on a strictly confidential and need to know basis and the information (including results of the data matching exercise) will be retained within the Audit Commission for the duration of the initiative. Auditors may decide to retain some data after this period for instance if they are needed for the purpose of continuing investigation or prosecution. All relevant data will be destroyed and rendered irrecoverable by the Commission after all processing is completed and all queries resolved. This will be done promptly and, in any event, within six months of the conclusion of the exercise.

The use of data by the Audit Commission in a data matching exercise is carried out with statutory authority under its powers in Part 2A of the Audit Commission Act 1998. It does not require the consent of the individuals concerned under the Data Protection Act 1998. Data matching by the Audit Commission is subject to a Code of Practice. This may be found at www.audit-commission.gov.uk/nfi.

For further information on the Audit Commission's legal powers and the reasons why it matches particular information, see www.audit-commission.gov.uk/nfi/fttext.asp or

contact Peter Yetzes, Head of NFI, Audit Commission, 1st Floor, Millbank Tower, Millbank, London SW1P 4HQ; telephone 0844 798 2222; email nfiqueries@audit-commission.gov.uk.

For further information about how the Council processes your personal data, please visit the Information Commissioner's website where you can view our current Notification Register with them, www.ico.gov.uk/Home/tools_and_resources/register_of_data_controllers.aspx

Level 1 – Summary Text - Example for Application Forms (for example, for benefits, housing tenancies, employment, market traders and taxi drivers)

This authority is under a duty to protect the public funds it administers, and to this end may use the information you have provided on this form for the prevention and detection of fraud. It may also share this information with other bodies responsible for auditing or administering public funds for these purposes.

Level 1 – Summary Text – Example for Payslips (for employees)

Please note that key payroll data may be provided to bodies responsible for auditing and administering public funds for the purposes of preventing and detecting fraud.

Level 1 – Summary Text – Example for Letters (for example, to pensioners, employees and tenants, where communication by newsletter, payslip and so on is not practicable)

This example has been drafted for pensioners; the words in [square brackets] should be amended accordingly for employees, tenants etc.

Dear {name [of pensioner]}

THIS LETTER IS FOR INFORMATION ONLY – YOU ARE NOT REQUIRED TO TAKE ANY ACTION

We are participating in an exercise to promote the proper spending of public money.

We are required by law to protect the public funds we administer. We may share information provided to us with other bodies responsible for auditing or administering public funds in order to prevent and detect fraud.

The Audit Commission currently requires us to participate in its anti-fraud initiative. For this initiative, we are providing details of [pensioners] so that they can be compared to information provided by other public bodies. This will ensure, for example, that [no pensions are being paid to persons who are deceased or no longer entitled, and that occupational pension income is being declared when housing benefit is applied for].

Sometimes wrong payments are made because of a genuine error. Previous exercises have uncovered instances of [pensioners] receiving too little [pension], resulting in the payments to [pensioners] being increased. These exercises, therefore, help promote the best use of public funds.

You do not need to respond to this letter. You may be contacted again in the future if the exercise suggests you are not receiving the correct amount of [pension]. Further information is available on our website at www.castlepoint.gov.uk. However, if you do have any questions, you should contact {name and contact details}, who can also provide hardcopies of information available on our website.

Level 2 – Condensed Text – to be published on the Council’s website

{This is an example level 2 notice and should be adapted by each organisation as necessary.}

This authority is required by law to protect the public funds it administers. It may share information provided to it with other bodies responsible for auditing or administering public funds, in order to prevent and detect fraud.

The Audit Commission appoints the auditor to audit the accounts of this authority. It is also responsible for carrying out data matching exercises.

Data matching involves comparing computer records held by one body against other computer records held by the same or another body to see how far they match. This is usually personal information. Computerised data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it indicates that there is an inconsistency which requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.

The Audit Commission currently requires us to participate in a data matching exercise to assist in the prevention and detection of fraud. We are required to provide particular sets of data to the Audit Commission for matching for each exercise, and these are set out in the Audit Commission’s guidance, which can be found at www.audit-commission.gov.uk/nfi.

The use of data by the Audit Commission in a data matching exercise is carried out with statutory authority under its powers in Part 2A of the Audit Commission Act 1998. It does not require the consent of the individuals concerned under the Data Protection Act 1998.

Data matching by the Audit Commission is subject to a Code of Practice. This may be found at www.audit-commission.gov.uk/nfi/codeofdmp.asp .

For further information on the Audit Commission’s legal powers and the reasons why it matches particular information, see <http://www.audit-commission.gov.uk/nfi/fptext.asp>. For further information on data matching at this authority contact {name and contact details}.

Appendix F

Example of a simple information sharing procedure

Procedure for sharing information between:

Name of Organisations:

1. Contact details

- 1.1. Named individuals in Council Department and recipient organisation

2. Types of information to be shared

- 2.1Report to be sent to These will always be marked **CONFIDENTIAL**.
- 2.2 Memoranda as required. These will always be marked **CONFIDENTIAL**
- 2.3 Crime reports may also be disclosed
- 2.4 Verbal information will be shared at meetings. This information will be either **RESTRICTED** or **CONFIDENTIAL**. Minutes should be classified according to the value of information in them.

3. How to handle the information

3.1 Transmission

- 3.1.1 **RESTRICTED** information can be transmitted over the telephone or sent by email. **CONFIDENTIAL** information must be sent in a double envelope with the protective marking shown on the inner one. If sent using other methods eg memory stick or CD this must be protected by an encryption.

3.1.2 Storage

- 3.1.2.1 All the information must be kept under lock and key when not in the personal custody of an authorized person. The “need to know” principle will be strictly enforced. **CONFIDENTIAL** information needs to be protected by two barriers, for example a locked container in a locked room
- 3.1.2.2 All the information held on IT systems must be protected to a standard at least equivalent to the Council’s Corporate IT Information Security Policy.

3.1.3 Release to third parties

- 3.1.3.1 No information provided by partners to these procedures will be released to any third party without the permission of the owning partner

Appendix G

Organisations who have adopted this Guidance when sharing personal data between them

Organisation	Date adopted
Southend Borough Council	
<p>Castle Point Borough Council</p> <p>Information on this Policy and procedures may be sought from:</p> <p>Fiona Wilson Head of Legal Services Castle Point Borough Council Council Offices Kiln Road Thundersley Benfleet Essex SS7 1TF</p> <p>Email: fwilson@castlepoint.gov.uk</p> <p>Or from the Council's Data Controller:</p> <p>Mr Andrew Roby Smith Strategic Director Improving the Council Castle Point Borough Council Council Offices Kiln Road Thundersley Benfleet Essex SS7 1TF</p> <p>Email: asmith@castlepoint.gov.uk</p>	