



INFORMATION SHARING PROTOCOL

SEPTEMBER
2009

This Protocol will be reviewed
APRIL 2011

VERSION CONTROL SHEET

<i>Title:</i>	Information Sharing Protocol
<i>Purpose:</i>	To facilitate data sharing between partner signatories in the implementation of the Partnership Crime & Disorder Reduction Strategy 2008/2011 in the borough of Thurrock.
<i>Owner:</i>	Partnership Manager, Thurrock Community Safety Partnership micunningham@thurrock.gov.uk
<i>Approved by:</i>	Strategic Partnership Board
<i>Date:</i>	September 2009
<i>Version Number:</i>	2.0
<i>Status</i>	Draft Refresh
<i>Review Frequency</i>	Annually
<i>Next Review Date</i>	APRIL 2011

Review 2009 - Amendments/Changes

Ref	Changes/amendments	Date Amended
P2	Version Control Sheet and Review Changes	August 2009
1.2.	Inserted Seven Golden Rules – Government Guidance on Information Sharing – specifically in relation to the 'Every Child Matters' agenda.	May 2009
1.3.	Guidance from Information Commissioner's Office	May 2009
4.1.	ECFRS – Address changed from Rayleigh to c/o Hogg Lane, Grays, Essex.	June 2009
4.1	Inclusion of Chelmer Housing as a signatory	June 2009
4.1	Inclusion of Thurrock Thames Gateway Development Corporation as a signatory	August 2009
4.1	Inclusion of AEJ Management (Lakeside Retail) as a signatory	June 2009
4.2	Inclusion of Capital Shopping Centres (Lakeside) as a signatory	August 2009
4.4.	Statement on reasons for Review	August 2009
5.4	Health Data as defined in the DPA 98(Section 2(e) Sensitive Personal Data). – Ref. Appendix 8 (NEW)	June 2009
5.5.	Insertion of word 'consent' in sub-heading (for clarity)	May 2009
7.2	District Commander changed to Community Commander	June 2009
7.2	SPOC/Designated Officer for NHS SW Essex – changed from Locality Manager to Head of information Governance	June 2009
8.5.2	Reference to Appendix 8 (NEW)	August 2009
10.0	Cllr. Wendy Herd replaces Cllr. John Cowell as Thurrock Council representative for the Essex Fire & Rescue Authority	June 2009
10.0	Signature box changed to read "Thurrock and Brentwood Community Command."	June 2009
10.0	Additional Signature boxes inserted.	August 2009
App 1	Data Request Form replaced with current Essex Police template	August 2009
App 7	NHS Guidelines on Sharing sensitive and patient identifiable information by email	June 2009
App 8	Data Security and Encryption Guidelines	August 2009

CONTENTS

	Page No
1. INTRODUCTION	1
2. PURPOSE	2
3. SCOPE	4
4. PROTOCOL ADMINISTRATION	4
4.1. Signatory Partners to the Protocol	4 - 5
4.2. Commencement of the Protocol	6
4.3. Withdrawal from the Protocol	6
4.4. Review of the Protocol	6
4.5. Audit Arrangements	6
5. LEGAL COMPLIANCE	7
5.1. Overriding any duty of confidence	7
5.2. Necessity of the data sharing	7 - 8
5.3. Fair processing of the data	8
5.4. Justification for the provision of sensitive data	9
5.5. Proportionality	9
6. TYPES OF DATA TO BE SHARED	10
7. ROLES AND RESPONSIBILITIES	10
7.1. Partner Responsibilities	10
7.2. Single Point of Contact/Principal Designated Officer	11
8. PROCESS OF SHARING	12
8.1. Process	12
8.2. Sharing outside of the Protocol	12
8.3. Ensuring the accuracy of the data shared	12 - 13
8.4. Version control and Review, Retention and Disposal	14
8.5. Best Practice	14 - 15
8.6. Security of the data being shared	15
9. MISCELLANEOUS MATTERS	16
9.1. Indemnity	16
9.2. Rights of Data Subjects	16
9.3. Freedom of Information Act considerations	16
10. SIGNATURES	17 - 25
APPENDIX 1 DATA SHARING REQUEST FORM	26 - 27
APPENDIX 2 DUTY TO SHARE PRESCRIBED DATA	28 - 31
APPENDIX 3 RELEVANT STATUTES	32 - 34
<i>(Including the Eight Data Protection Principles)</i>	
APPENDIX 4 CALDICOTT PRINCIPLES	35
APPENDIX 5 DECISION MAKING FILTER	36
APPENDIX 6 SHARING OUTSIDE OF THE PROTOCOL	37
APPENDIX 7 NHS – SHARING SENSITIVE AND PATIENT IDENTIFIABLE INFORMATION	38 - 40
APPENDIX 8 DATA SECURITY AND ENCRYPTION - GUIDANCE	41 - 50

1. INTRODUCTION

1.1. This Protocol has been developed to:

- Document the specific purposes for which the signatory partners¹ have agreed to share data.
- Describe the roles and structures that will support the exchange of data between signatory partners.
- Set out the legal gateway through which the data is shared, including any reference to the Data Protection Act 1998, the Human Rights Act 1998 and the Common Law duty of confidentiality
- Describe the security procedures necessary to ensure compliance with legal and regulatory responsibilities including under the Data Protection Act 1998 and any partner specific security requirements.
- Ensure compliance with individual signatory partners' policies, legal duties and obligations.
- Ensure that Essex Police complies with the Code of Practice on the Management of Police Data made under the Police Act 1996 and the Police Act 1997.
- For the purposes of this Protocol the term 'Signatory partners' shall mean those named signatory partners as detailed in 4.1 and 10

1.2 Seven Golden Rules for information sharing

Recent Government guidance on information sharing in respect of the Every Child Matters agenda² has set out seven golden rules for information sharing. The golden rules are clear and concise, and can be applied equally to general information sharing principles. The seven golden rules for information sharing are detailed below and should be considered by all signatory partners when sharing information.

(1) Remember that the Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately.

(2) Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

(3) Seek advice if you are in any doubt, without disclosing the identity of the person where possible.

¹ Signatory Partners includes all Responsible Authority Partners (4.1 of document) and Co-Operating Bodies Partners (10. of document)

² HM Government Information Sharing: Guidance for Practitioners and Managers – www.ecm.gov.uk/informationsharing

(4) Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, the lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.

(5) Consider safety and well-being: Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

(6) Necessary, proportionate, relevant, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

(7) Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

- 1.3** The Information Commissioner’s Office has, in support of guidance to frontline practitioners³ for information sharing about an individual, stated the following, which signatory partners should be aware of:-

“All organisations can accomplish information sharing lawfully by adhering to governing legislation and the principles of the Data Protection Act whether an information sharing protocol is in place or not. An Information Sharing Protocol is a useful tool in some circumstances. It is not a legal requirement.

There are two distinct types of information sharing. Organisations may share large amounts of data with one or more partner organisations on a regular basis, or practitioners may share information with each other on an ad hoc basis as individual situations require.

An Information Sharing Protocol is a useful tool with which to manage large scale, regular information sharing. It creates a routine for what will be shared, when and with whom and provides a framework in which this regular sharing can take place with little or no intervention by practitioners.

It is not a useful tool for managing the ad hoc information sharing which all practitioners find necessary. Most importantly it is not intended to be a substitute for the professional judgement which an experienced practitioner will use in those cases and should not be used to replace that judgement.”

2. PURPOSE OF PROTOCOL

2.1. The purpose of this Protocol is to facilitate data sharing between partner signatories in the implementation of the Partnership Crime & Disorder Reduction Strategy 2008/2011 in the borough of Thurrock. Data sharing assists signatory partners to effectively prevent, detect and reduce crime and disorder throughout Thurrock. It is however, incumbent on

³ Department for Children, Schools and Families, August 2008

all signatory partners to recognise that any data shared must be justified on the merits of each case.

Data sharing between partner agencies is an integral part of achieving the targets as outlined in any crime detection or reduction strategy, as it enables informed decision making and subsequent action to achieve the strategy's objectives. However, signatory partners also have a legal duty to protect the rights of those individuals who may be affected by data sharing, hence the need for up-to-date and valid data sharing Protocols.

2.2. The purpose of the Thurrock Community Safety Partnership Data Sharing Protocol ("the Protocol") is to facilitate the transparent exchange of crime and disorder data that is necessary, relevant and proportionate, within the existing legislative data sharing framework between all signatory partners within The Thurrock Community Safety Partnership.

2.2.1. The Protocol sets out the details of sharing personal data in accordance with the Law. In accordance with the Data Protection legislation, partner signatories to this Protocol will be able to share data statutorily and informally, this can be through referrals, emails, and intelligence (not fact) provided that all documentation is appropriately marked e.g. as confidential/restricted. In cases where a more formal request is required, the "Data Sharing Request Form" shall be used (see Appendix 1) within the Thurrock Community Safety Partnership.

2.2.2. The Crime & Disorder Regulations 2007 which came into effect in August 2007 places an obligation on Signatory partners to share specific types of data. The detail of data each Responsible Authority signatory partner has a duty to share, is set out in Appendix 2 of this Protocol.

2.3. The Thurrock Community Safety Partnership will review this Protocol every 12 Months, and more frequently if any significant amendments to legislation or statutory notices arise. Signatory partners will be consulted on any significant updates or suggested amendments to the Protocol that arise from any review.

2.4. All signatory partners pledge to consult with organisations periodically on any policy and strategy relevant to common data sharing procedures.

2.5. This Protocol provides a range of benefits to all signatory partners which are detailed below:-

- An over-arching benefit, that enables signatory partners to improve their effectiveness in tackling crime and disorder in Thurrock.
- Enabling all signatory partners to do all that they reasonably can to reduce and *prevent* crime, disorder and anti-social behaviour in Thurrock.
- Enabling all signatory partners to reduce and prevent, incidents of violent crime in Thurrock, particularly those incidents that may be caused by drug and alcohol abuse.
- Enabling all signatory partners to reduce and prevent, incidents of hate crime, and crimes committed against the most vulnerable members of the community in Thurrock.

- Enabling the Community to feel assured and safe, in the knowledge that appropriate and timely data sharing between signatory partners could lead to the potential for crimes being prevented, that may otherwise have occurred without the appropriate data sharing.

3. Scope of Protocol

The scope of the Thurrock Community Safety Partnership Protocol includes all data shared statutorily (as detailed in Appendix 2), as well as all data shared informally as detailed in 2.2.1 above between all signatory partners. Data will not be shared where disclosure would prejudice ongoing proceedings or sensitive cases unless there is an overriding public safety requirement to do so.

This Protocol applies to all records created, received and maintained by the staff of The Thurrock Community Safety Partnership Signatory partners or those acting as its agents, in the course of Partnership business.

A record is defined as a document held in any format including (but not limited to) paper documents, audio recordings, electronic data or visual representations.

The Protocol shall be applicable to all staff/employees of Signatory partners.

4. PROTOCOL ADMINISTRATION

4.1. Signatory partners to the Protocol

Responsible Authorities

Essex Police (Thurrock)
Grays Police Station
Brooke Road
Grays
Essex RM17 5BX

Thurrock Council
Civic Offices
New Road
Grays
Essex RM17 6SL

Essex County Fire &
Rescue Service, Thurrock
& Brentwood Command,
C/o Fire Station
Hogg Lane
Grays
Essex RM17 5QS

NHS SW Essex
Phoenix Court
Christopher Martin Road
Basildon
Essex SS14 3EZ

Co-Operating Bodies

National Probation Service (Essex) Cullen Mill 49 Braintree Road Witham Essex CM8 2DD	Youth Offending Service 4 Quarry Hill Grays Essex RM17 5BT	Thurrock Drug, & Alcohol Action Team (DAAT) C/o Thurrock Council Civic Offices New Road Grays Essex RM17 6SL	Thurrock Community Voluntary Services The Beehive Voluntary & Community Resource Centre West Street Grays Essex RM17 6XP
Essex Police Authority c/o Thurrock Council Civic Offices New Road Grays Essex RM17 6SL	Federation of Small Businesses 1 Pump Farm Cottages Ongar Road Kelvedon Hatch Brentwood Essex CM15 0LA	Essex Fire Authority c/o Thurrock Council Civic Offices New Road Grays Essex RM17 6SL	S.E.R.I.C.C. The Hall West Street Grays Essex RM17 6LL
T.R.U.S.T. Thameside Complex Cromwell Road Grays Essex RM17 5PD	Victim Support Suite 4 The Chequers High Street Ingatestone Essex CM4 0GD	British Transport Police 25 Camden Road London NW1 9LN	Suffolk Heritage Avocet House Station Road Framlingham Woodbridge Suffolk IP13 9EE
Thurrock Womens' Aid PO Box 32 Thurrock Essex RM17 6HN	Brentwood Housing Association Ltd 594 Rayleigh Road Leigh on Sea Essex SS9 5HU	Family Mosaic Pembroke House Northlands Pavement Pitsea Essex SS13 3DU	Swan Housing Pilgrim House High Street Billericay Essex CM12 9XY
Springboard Housing Springboard House 2a Claughton Road London E13 0PN	Estuary Housing Association Ltd Centre Place Prospect Close Southend-on-Sea Essex SS1 2JD	ECHG North London Cluster Beck House 1 Upton Road Edmonton London N18 2LJ	Chelmer Housing Partnership Myriad House 23 Springfield Lyons Approach Chelmsford Essex CM2 5LB
Thurrock Thames Gateway Development Corporation Gateway House Stonehouse Lane Purfleet Essex RM19 1NX	AEJ Management (Lakeside Retail Park) The Junction 10 Lower Grosvenor Place London SW1W 0EN	Capital Shopping Centres (Lakeside) Lakeside Shopping Centre West Thurrock Way Thurrock Essex	

Signatories must also ensure that they comply with all relevant legislation.

4.2. Commencement of the Protocol

This Protocol shall commence upon date of the signing of a copy of the Protocol by the signatory partners.

The relevant data will be shared between signatory partners from the date the Protocol commences.

4.3. Withdrawal from the Protocol

Any partner may withdraw from this Protocol upon giving written notice to the other signatories. The partner must continue to comply with the terms of this Protocol in respect of any data that the partner has obtained through being a signatory. Data which is no longer relevant should be returned or destroyed in an appropriate manner.

4.4. Review of the Protocol

In accordance with the requirements of the Code of Practice for the Management of Police Data this Protocol will be reviewed six months after its implementation and annually thereafter.

The review will:

- Ensure the contact list is up-to-date
- Consider whether the Protocol is still useful and fit for purpose
- Identify any emerging issues
- Determine whether the Protocol should be extended for a further period (up to one year) or whether to terminate it

The decision to extend or terminate the Protocol, and the reasons, will be recorded.

It has been decided to extend this Protocol for a period of 18 months to March 2011 in line with current 3 year strategic plans. Additional space for further signatures within this 18 month period has been accommodated.

4.5. Audit Arrangements

As part of the requirements of the Code of Practice for the Management of Police Data; Essex Police will maintain a Data Sharing File in respect of this Protocol.

This file (which may be electronic or paper based) will contain:

- Record of Essex Police data disclosed
- Record of data disclosed to Essex Police
- Decision or justification to disclose or not disclose
- Access and vetting list
- Notes of meetings with signatory partners
- Details of recent correspondence and phone calls
- Record of any review of the Protocol

Similar arrangements can be put in place by other signatory partners, if they choose.

5. LEGAL COMPLIANCE

Sharing crime and disorder data in accordance with the Protocol is lawful under the following statutes which can be found in Appendix 3:

- Schedules 2 and 3 of the Data Protection Act 1998
- Sections 5, 6, 7, 17 and 115 of the Crime & Disorder Act 1998
- Section 97 of the Police Reform Act 2002
- Article 8 of the Human Rights Act 1998
- Common Law (Duty of Confidence)
- Caldicott Principles – (See Appendix 4)

5.1. Overriding any duty of confidence

There is an inherent duty of confidentiality attached to all data that may be shared within activities undertaken by all the signatory partners in order to tackle issues relating to crime and disorder.

This duty of confidentiality exists whether the data is personal or non-personal and regardless of the reason for sharing the data.

Common Law stipulates that the following reasons justify sharing confidential data about a person:

- a) When consent is obtained from the person who is identified as the subject in the data (wherever possible, practicable, or appropriate the permission of the Data Subject should be obtained);
- b) When the law or a court orders that the data must be shared;
- c) When it can be demonstrated that disclosure is considered to be more in the best interests of the public than confidentiality, e.g:-
 - Where there is a public interest or a public health interest
 - Where there is a risk of death or serious harm risk to person(s);
 - When disclosure is necessary to detect, prevent or prosecute serious crime;
 - Where an individual's health is at serious risk (either the person identified in the data or another person);
 - Where it is identified as being in the interest of the person concerned.

We agree that we will only disclose sufficient data to enable our signatory partners to carry out the relevant purpose for which the data is intended. This we will determine on a case-by-case basis.

5.2. Necessity of the data sharing

All decisions to disclose data must be made on a case-by-case basis and in every instance the level of that disclosure may be different. Only the Data Controller⁴ of an organisation can agree to disclose to another organisation, following a senior manager of the same

⁴ Under the Data Protection Act a "Data Controller" is a person who determines the purposes for which, and the manner in which, personal data is to be processed. This may be an individual or an organisation and the processing may be carried out jointly or in common with other persons.

organisation agreeing in advance that the disclosure is lawful. To determine whether data should be disclosed the senior manager and Data Controller must compare legislative authority alongside the following issues (but not exclusive to): relevance of the data request, proportionality, data quality, potential data sharing with third parties, method of disclosure, conditions of disclosure, and details on the decision making process.

Each signatory partner undertakes to ensure that it complies with all relevant legislation, the Protocol, and its own internal data sharing policies. Signatory partners are recommended to seek their own legal advice, where necessary, where complex data sharing issues arise.

Signatory partners pledge to consult with organisations periodically on any policy and strategy relevant to common data sharing procedures.

5.3. Fair processing of the data

The Data Protection Act 1998 requires the fair processing of personal data unless an exemption applies. The most likely exemption to being 'fair' is the sharing for the prevention and detection of crime, apprehension or prosecution of an offender.

An example of this would be where data is being shared about an individual without their knowledge; however, disclosure of that fact would be likely to prejudice the investigation.

Any organisation may request crime and disorder data from a Relevant Authority so long as that organisation can demonstrate that the data will be used to assist with achieving the overall aim of prevention, detection and reduction of crime and disorder in Thurrock.

5.3.1. – Personal Data Shared

In addition to non-personal statistical data, personal data that may be shared under the Protocol on a case-by-case basis includes:

- a) Personal Details necessary to ensure the accurate identification of data subjects such as name, address (including postcode), age, occupation/school and identification of immediate family;
- b) Data about the past or current activities, such as places frequented and associates, to enable research or surveillance of the data subject thus informing decision making about action to be taken to prevent or deter suspected offending;
- c) Offending History relevant to the purpose for which it is being shared which is necessary in order to assess likelihood of offending and to carry out risk assessment for the various agency practitioners who might be involved.
- d) Personal Opinions of Professionals, which are necessary to inform decision making around likelihood of offending and the assessment of risk to individuals. Any such data will be clearly marked that it is an opinion and where possible on what basis that opinion is formed.

From time to time specific crime reducing initiatives, focussing on particular crimes or group of offenders, may be required. Examples may include 'Hate Crime', 'Domestic Abuse & Sexual Violence' 'Anti Social Behaviour' or 'Priority and Prolific Offenders'. This Protocol covers such initiatives if their purpose is to reduce crime and disorder, irrespective of whether the initiative is local or central Government led.

5.4. Justification for the provision of sensitive personal data

Sensitive personal data is data about an individual that relates to: -

- the commission or alleged commission of an offence;
- proceedings relating to an offence;
- physical or mental health condition (DPA98 S2(e)).

The Data Protection Act 1998 requires that one or more conditions under Schedule 3 of the Act must be satisfied before sensitive data is subject to sharing for the purposes of this Protocol. See Appendix 7.

5.5. Proportionality/Consent

Those signatory partners to this Protocol which are public authorities are satisfied that the nature of the data to be shared under this Protocol and the manner of such sharing is compatible with the requirements of the Human Rights Act 1998: having particular regard to the exemptions to the right to respect of family life set out within Article 8(2) of the European Convention of Human Rights.

Where appropriate and possible, explicit consent should be obtained from the data subject for the disclosure of personal data to take place, in accordance with the Data Protection Act 1998. This consent must be freely given, after the consequences are made clear to the person from whom permission is being sought. However, Signatory partners agree that disclosure without consent is lawful if certain conditions are met. For example, personal data may be shared when made anonymous, or to ensure the performance of public functions or legal obligations.

If it is essential, that personal data held under a duty of confidence must be disclosed, the data subject's consent must be obtained. Occasionally, an individual may refuse to give consent to share their data. Therefore, the grounds on which consent can be overridden must be considered. Disclosure of sensitive data may occur if it falls within the defined category of *public interest*.

Where necessary, the Data Controller is responsible for ensuring that data subjects are advised that their personal data is being or may be shared.

6. TYPES OF DATA TO BE SHARED

Data shared should be information that is statutorily required to be shared, by each of the relevant signatory partners to this Protocol as set out in Appendix 2. The informal sharing of general information can take place as detailed in 2.2.1 of this Protocol.

7. ROLES AND RESPONSIBILITIES

7.1 Partner Responsibilities

The Thurrock Community Safety Partnership will act as document owners, with the named signatories having accountability for implementation within individual organisations.

The intended recipients of the data shall be any authorised officer / member of staff of any of the Partner organisations party to this Protocol.

7.1.2 Each Partner organisation should have, in existence, a Data Sharing Co-Ordination folder that must contain:

- Record of data disclosed
- Decision or Justification to disclose or not disclose
- Access and vetting list
- Notes of meetings with signatory partners
- Details of recent correspondence and phone calls

7.1.3 It shall be the responsibility of managers in each of the Partner organisations to:

- Ensure that staff adhere to the Flow Chart Process as detailed in Appendix 5 of this Protocol
- Provide their own guidance to staff on the processes for data sharing and the levels to which data can be shared;
- Support staff to share data appropriately;
- Provide a system for recording decisions on whether or not to share data;
- Ensure that the process of sharing data is adhered to by both those in a supervisory and user capacity;
- Ensure that staff who have a responsibility for sharing data are trained accordingly.
- Identify a co-ordinator to manage the Co-Ordinating folder.

7.1.4 It shall be the responsibility of supervisors in each of the Partner organisations to:

- Support staff to share data appropriately;
- Audit, on an ad hoc basis, the decision to share made by users, including the necessity, accuracy and adequacy of data shared;
- Checking whether the decision to share meets a policing purpose or other legal duty or power;
- Ensuring that data being shared does not compromise any police operation, business interest, or the safety of others;

- Ensuring that a risk-assessment process is adhered to by the user when making a decision to share data.

7.1.5 It shall be the responsibility of users in each of the Partner organisations to:

- Ensure that data is relevant, accurate and adequate for the purpose for which it is being shared;
- Ensure that when personal data is shared, the requirements of the Data Protection Act and the common law duty of confidence have been fulfilled;
- Apply a risk assessment where the sharing is carried out with the signatory partners in the voluntary or private sectors who do not have a statutory purpose to share data;
- Record any decision to share or not to share in accordance with the Protocol;
- Ensure that the data being shared meets a policing purpose or is lawfully disclosable for a statutory purpose and is proportionate and necessary.

7.2 Single Point of Contact/Designated Officer

Each partner will appoint a single point of contact (SPOC)/ Principal Designated Officer (PDO) who will be a manager of sufficient standing and who will have a co-ordinating and authorising role. A partner may also appoint a supervisor or manager to deputise for the SPOC/PDO.

The following post-holders are the SPOCs/PDOs, or Deputies, for the partner organisations who will be responsible for data protection, security and confidentiality, and compliance with all relevant legislation.

POST	ORGANISATION
District Commander, Thurrock	Essex Police
Head of Public Protection	Thurrock Council
Community Commander, Thurrock	Thurrock & Brentwood Command – Essex Fire & Rescue
Head of Information Governance	NHS South West Essex

Queries on the document should firstly be referred to your own organisation's SPOC and then the Thurrock Community Safety Partnership – Safer.Thurrock@thurrock.gov.uk

The specific responsibilities of the above are:

- Making sure the named party abides by this Protocol
- Ensuring relevant staff are fully aware of their responsibilities
- Appointing other staff to act in their absence
- Controlling the release of the data and maintaining its integrity
- To decide on a case-by-case basis if and why a public interest overrides a duty of confidence
- Keeping a data sharing file (or similar), which holds all the partner's data sharing documents in general
- Ensuring any changes to the SPOC/PDO are confirmed in writing to TCSP

8. PROCESS OF SHARING

The data may only be used for the purpose/s set out in this Protocol.

Signatory partners to this arrangement will respond to any notices from the Data Commissioner that imposes requirements to cease or change the way in which data is processed.

8.1. Process (Confidentiality & Disclosure Purposes)

For confidentiality and disclosure purposes, The Thurrock Community Safety Partnership will share data in the following two ways:-

Method 'A'

- At formal meetings when a disclosure and confidentiality statement will be read out and signed by all present
- Through each agencies' relevant referral forms
- Through documentation which should be appropriately marked as either confidential and/or restricted

All informal data sharing will be conducted in the above-mentioned ways.

Method 'B'

Formal data sharing shall be undertaken using the prescribed "Data Sharing Request" form as referred to in 2.2.1 of this Protocol and shown in Appendix 1.

It is acknowledged that most data will be shared under Method 'A'.

8.2 Sharing Outside of the Protocol

When signatory partners are sharing data outside of the Protocol the process to share requires that a set of questions be posed, in accordance with best practice and prudence. These questions are detailed in Appendix 6 of the Protocol.

8.3 Ensuring the accuracy of data shared

8.3.1 The Thurrock Community Safety Partnership, and individual signatory partners are responsible for ensuring that any data they share is accurate and, where necessary, kept up to date.

8.3.2. Usability implies that a record can be 'located, retrieved, presented and interpreted'. Integrity refers to a record being complete and unaltered. Records must be protected against unauthorised alterations by means of good security practice (e.g. access permissions) and authorised alterations to records must be traceable, as well as being explicitly indicated through version control (see below – 8.4)

8.3.3. Freedom of Information Act 2000

Records that are to be made available via the Freedom of Data Act 2000, from any Partner, should be clearly marked as such. As part of the general move towards transparent government and accountability to the public, it is vital that all records are made as easily retrievable as possible, ensuring that responses to Freedom of Data access requests are processed within the statutory timescales.

8.3.4 Data Protection Act 1998

The Thurrock Community Safety Partnership's objective is that personal data is managed in accordance with the eight data protection principles⁵ and is available for subject access requests within the required time frame.

8.3.5 Auditing

Records management processes and procedures must support Partner Agencies' Audit Services requirements. All record keeping systems must be able to display a clear audit trail.

On the part of Thurrock Council, as a Partner to this Protocol, its Audit Services Department undertake a program of work each year to test the completeness, validity and accuracy of records held within Departments.

8.3.6 Vital Records / Emergency Planning

All Partner Agencies must ensure that they have vital records management and emergency planning procedures in place in support of data shared between signatory partners.

Within the Council for instance, vital records management and emergency planning is an important aspect of records management. They are part of the Council's wider business continuity and risk management regime. All individuals of Thurrock Council have a responsibility to ensure that:

- Records (whatever their medium or format) that are vital to the Council in the event of an emergency or essential to its continuation of business are identified and sufficiently protected.
- Measures are in place to prevent disasters compromising the records and record keeping systems.

Similar measures should be in place in all Signatory Partner organisations.

⁵ See Appendix 2(1)

8.4 Version Control

Effective version control is essential to good records management practice. It is particularly vital where electronic documents are stored in a shared area where they may be updated by a number of different users. Whenever any alteration is made to a record, it must be allocated a new version number. These should use consecutive numbering in a standard format (i.e. V1.0, V1.0.1, V1.0.2, V2.0).

8.4.1 Review, Retention & Disposal

Efficient management of records is essential in order to:

- Support the Partnership's core business activities
- Comply with legal and regulatory obligations
- Provide a high quality service to our customers

This policy provides a framework for the management of The Thurrock Community Safety Partnership records.

8.5 Best Practice

Records should be managed in accordance with the Lord Chancellor's code of practice on the management of records under section 46 of the Freedom of Data Act.

The guidelines produced by the Records Management Society and National Archives should be used as an aid to assist with best practice.

8.5.1 Record creation and record keeping

All records must be authentic and reliable. An authentic record is one that can be proven:

- to be what it purports to be,
- to have been created or sent by the person purported to have created or sent it, and
- to have been created or sent at the time purported

A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

Each signatory partner must have in place a record keeping system which documents its activities and allows for quick and easy retrieval of data. This must include:

- Classification of records into a logical and consistent hierarchy
- Allocation of appropriate metadata consistent with the Government Metadata Framework
- Consistent version control procedures
- Consistent and appropriate security classification of records
- Clearly documented authorship and ownership of records
- Usability and integrity of records

8.5.2 Retention and disposal

All record-keeping procedures must support the corporate document retention policies of each Partner agency.

Confidential or sensitive documents must be disposed of securely, in accordance with corporate document retention policies of Partner agencies.

Signatory partners should ensure, when sharing data that the data is communicated in a manner that is confidential (i.e. Encrypted emails, or paper copies that are marked "Confidential – To be opened by addressee only). Fax machines are not a secure way of transmitting and sharing data between organisations and should not be used.

Disposal of confidential data should be disposed of through the use of cross-cut shredding machines or returned securely to the original sharing partner.

See Appendix 8 for Thurrock Council's Data Security and Encryption Guidance

8.6 Security of the data being shared

The data must be stored securely and deleted/destroyed when it is no longer required for the purpose for which it is provided. This can either be returned to the original sharing partner or shredded, using cross-cut shredding machines.

The data shared (unless it is data where there is a duty to share), must not be disclosed to any third party without the written consent of the partner that provided the data; unless it is disclosed under a statutory obligation or by Essex Police for a policing purpose.

Signatories of this agreement recognise that the sharing of personal data and other information may expose that information to risk of accidental or deliberate misuse or inappropriate disclosure. Signatories are committed to reducing such risks and acknowledge that any deliberate use or further disclosure of personal data shared under this agreement in a manner inconsistent with this agreement is likely to be regarded as a criminal offence under Section 55 of the Data Protection Act 1998. Where there are concerns regarding information exchanged under this protocol they will be communicated to the relevant organisation's staff responsible for handling/investigating data protection and information security complaints.

All Signatory partners may refer to Thurrock Council's and/or Essex Police's Document Retention Policy, and Records Management Policy and the NHS 'Records Management Code of Conduct' for further Guidance.⁶

For the purposes of good practice all SPOC's/PDO's with the Partnership should have, readily available to them, a copy of each of the above Policies.

⁶ Document Retention and Records Management Policies available from Thurrock Council, Essex Police and SWEssex PCT

9. MISCELLANEOUS MATTERS

9.1 Indemnity

Signatory partners to this Protocol are aware that the deliberate or reckless disclosure of personal data (obtained under this Protocol) to other organisations or persons may amount to a criminal offence under section 55 of the Data Protection Act 1998.

Signatory partners to this Protocol indemnify Essex Police (to include the Chief Constable of Essex Police, his officers and staff and the Police Authority) against any costs, damages and expenses it incurs in connection with and arising from legal claims (of whatever nature) against Essex Police arising from this Protocol, to include, but not limited to, claims arising from an alleged breach of this Protocol, misuse of the data or wrongful disclosure by the Partner and breach of confidentiality, save where the claim arises directly and solely because of the negligence of Essex Police.

9.2 Rights of data subjects

Signatory partners will comply with subject access requests in compliance with the relevant legislation. Where the relevant data has been provided by a third party or signatory partner; that party or partner should be notified as soon as possible of the request and in any event before responding to the request.

9.3 Freedom of Information Act Considerations

If required, Signatory partners should seek the advice of the Freedom of Information Officer, in their respective Corporate Support departments.

10. SIGNATURES

By signing this Protocol, all signatory partners accept responsibility for its execution and agree to ensure that staff are trained so that requests for data and the process of sharing itself is sufficient to meet the purpose of this Protocol.

Signed on behalf of Essex Police (Thurrock, S.W. Division)

.....

Name: **IVOR HARVEY**

Title: **SUPERINTENDENT, NEIGHBOURHOODS AND POLICING**

Date:

Signed on behalf of Thurrock Council

.....

Name: **BOB COOMBER**

Title: **INTERIM CHIEF EXECUTIVE**

Date:

Signed on behalf of NHS SW Essex

.....

Name:

Title: **DIRECTOR OF PUBLIC HEALTH**

Date:

Signed on behalf of Essex Fire & Rescue Service (Thurrock and Brentwood Community Command)

.....

Name : **MICK OSBORNE**

Title: **COMMUNITY COMMANDER**

Date:

Signed on behalf of Essex Police Authority:

.....

Name: **CLLR. WENDY HERD**

Position: **THURROCK COUNCIL REPRESENTATIVE FOR ESSEX POLICE AUTHORITY**

Date:

Signed on behalf of Essex Police Authority:

.....

Name: **CLLR.**

Position: **THURROCK COUNCIL REPRESENTATIVE FOR ESSEX FIRE & RESCUE AUTHORITY**

Date:

Signed on behalf of National Probation Service (Essex)

.....

Name: **ALEX BAMBER**

Position: **ASSISTANT CHIEF OFFICER, ESSEX PROBATION**

Date:

Signed on behalf of Thurrock Youth Offending Services

.....

Name: **JAY MERCER**

Position: Head of Children, Youth & Family Services

Date:

Signed on behalf of Thurrock Drug & Alcohol Action Team

.....

Name (*Please print*): **LUCY MAGILL**

Position:

Date:

Signed on behalf of Thurrock Community Voluntary Services

.....

Name (*Please Print*).....

Position:

Date:

Signed on behalf of Thurrock Business Forum Secretariat

.....

Name (*Please print*):

Position:

Date:

Signed on behalf of Essex Fire Authority

.....

Name (*Please print*):

Position:

Date:

Signed on behalf of S.E.R.I.C.C.

.....

Name (*Please Print*) **SHEILA COATES**

Title:

Date:

Signed on behalf of T.R.U.S.T.

.....

Name (*Please Print*) **RUTH JUETT**

Title:

Date:

Signed on behalf of Victim Support

.....

Name (*Please Print*):

Title:

Date:

Signed on behalf of Thurrock Women's Aid

.....

Name (*Please Print*) **ERIKA JENKINS**

Title:.....

Date:.....

Signed on behalf of British Transport Police

.....

Name (*Please Print*):.....

Title:.....

Date:.....

Signed on behalf of Suffolk Heritage Housing Association

.....

Name (*Please Print*):.....

Title :.....

Date:.....

Signed on behalf of Family Mosaic Housing Association

.....

Name (*Please Print*):.....

Title:.....

Date:.....

Signed on behalf of Swan Housing Association

.....

Name (*Please Print*):.....

Title:.....

Date:.....

Signed on behalf of Springboard Housing Association

.....

Name: (*Please Print*)

Title:.....

Date:.....

Signed on behalf of Estuary Housing Association

.....

Name (*Please Print*):.....

Title:.....

Date:.....

Signed on behalf of Brentwood Housing Association Ltd

.....

Name (*Please Print*) :.....

Title :.....

Date:.....

Signed on behalf of English Churches Housing Group

.....

Name (*Please Print*) :.....

Title:.....

Date:.....

Additional signatory boxes for new signatories.

Signed on behalf of

CHELMER HOUSING GROUP

Name (*Please Print*) :.....

Title:.....

Date:.....

Signed on behalf of

CAPITAL SHOPPING CENTRES (LAKESIDE)

Name (*Please Print*) :.....

Title:.....

Date:.....

Signed on behalf of

AEJ MANAGEMENT (LAKESIDE)

Name (*Please Print*) :.....

Title:.....

Date:.....

Signed on behalf of

THURROCK THAMES GATEWAY DEVELOPMENT CORPORATION

Name (*Please Print*) :.....

Title:.....

Date:.....

Signed on behalf of

Name (*Please Print*)

Title:

Date:.....

Signed on behalf of

Name (*Please Print*)

Title:

Date:.....

Signed on behalf of

Name (*Please Print*)

Title:

Date:.....

Signed on behalf of

Name (Please Print)

Title:

Date:.....

Signed on behalf of

Name (Please Print)

Title:

Date:.....

Signed on behalf of

Name (Please Print)

Title:

Date:.....

Signed on behalf of

Name (Please Print)

Title:

Date:.....

**APPENDIX 1
REQUEST FOR DISCLOSURE OF PERSONAL DATA**

.....

Our Reference:

.....**Sequential No:**

Date:

To (Authority):

From: **Designation:**

Organisation: **Address:**

Fax No:

Name: **Male/ Female** **D.O.B:**..... **Age:**

Address:

.....

..... **Place of Birth:**

Information Required

Please tick relevant category and provide details of the purpose for which the data is to be used. I confirm that the information requested is relevant/in accordance with the Thurrock Community Safety Partnership Crime Reduction Strategy.

Prevent crime	
Detect Crime	
Prevent Disorder	
Detect Disorder	
Prevent Nuisance	
Prevent Annoyance	

.....
.....
.....
.....

Signed:.....

Information supplied: Yes/ No* (please delete).

If YES summary of information supplied:

.....
.....

Reasons for information being supplied:

.....

Expiry date (date at which data disclosed may no longer be used):

Can any innocent victim, witness, or person other than the person named above, be identified if this information is disclosed?

*If **NO** why information was not supplied:*

.....

.....

Signed:

The use of this information for any secondary purpose is prohibited without the consent of the Data Holding Authority and/ or the consent of the data subject

APPENDIX 2

Crime & Disorder Regulations 2007 Prescribed Data Regulations 2007 No.1831 (England and Wales)

These Regulations came into force on 1st August, 2007. They describe the nature of the data to be shared between signatory partners within each local government area⁷ under the new duty to share depersonalised electronic data.⁸

This data must be shared at least quarterly, with a three-month window (*data period*) within which the data disclosure must take place. The duty to share will commence on 1st October 2007 – with the first ‘*data period*’ running from 1st October 2007 – 31st December 2007. So, responsible authorities are required to have shared the data described below at least once by 31st December 2007. This data will need to cover the three-month period prior to 1st October 2007.

In each instance, responsible authorities are only required to provide such data as they already possess. There are no requirements to collect *additional* data.

Data to be provided by each Responsible Authority

1.1. Thurrock Police must provide data *that it holds* in relation to:

Crime Category		
(a) anti-social behaviour incidents	Data on incidents, and the time, date and location of each of those incidents.	In accordance with the National Incident Category List in the National Standards for Incident Recording Instructions for Police Forces in England And Wales 2007 / 2008.
(b) transport incidents		
(c) public safety/welfare incidents		
Crime sub-category		
(a) Burglary (b) Criminal damage (c) Drug offences (d) Fraud and forgery (e) Robbery (f) Sexual offences (g) Theft and handling stolen goods (h) Violence against the person (i) Other offences	Data on incidents, and the time, date and location of each of those incidents.	In accordance with the Home Office Notifiable Offences List (July 2007)

⁷ Under Section 17A of the Crime and Disorder Act 1998

⁸ Police and Justice Act 2006

1.2 The Thurrock & Brentwood Fire & Rescue Service must provide data *that it holds* in relation to:

Incident Type	Data Required	Standards
(a) Deliberate primary fire (excluding deliberate primary fires in vehicles)	Time, date and location of each crime.	In accordance with Fire Statistics United Kingdom 2005.
(b) Deliberate primary fire in vehicles		
(c) Deliberate secondary fire (excluding deliberate secondary fires in vehicles)		
(d) Incidents of violence against employees of the fire and rescue authority	As above (including the purported location of malicious alarms)	In accordance with Fire Statistics, United Kingdom 2005
(e) Malicious false alarms to the fire and rescue services.		

1.3. Thurrock Council must provide data *that it holds* in relation to:

9.1.1. Incident Type	Data Required	Standards
Road traffic collisions.	Time, date and location; the number of adults and children killed, seriously injured and slightly injured in each of those collisions	N/A
Permanent or fixed term exclusion from state primary and secondary schools.	The age and gender of each of the pupils subject to exclusion; the names and addresses of the schools from which those pupils have been excluded and the reason for their exclusion.	N/A
Racial Incidents.	Time, date and location of racial incidents.	In accordance with Best Value Performance Indicators 2005/06 as defined by the ODPM ⁹

⁹ Office of the Deputy Prime Minister – now Department for Communities and Local Government (DCLG)

Incidents of anti-social behaviour identified by the authority.	The category, time, date and location of each incident.	In accordance with the National Incident Category List in the National Standards for Incident Recording Instructions for Police Forces in England and Wales for 2007 / 2008 or any other system for classifying asb used by the authority at August 2007.
Incidents of anti-social behaviour reported to the authority by the public.	The category, time, date and location of each incident.	

1.4. The South West Essex Primary Care Trust (the whole or any part of whose area lies within the area) must provide data *that it holds* in relation to:

Block	Data Required	Standards
(a) Assault (X85-Y09) (b) Mental and behavioural disorders due to psychoactive substance use (F10-F19) (c) Toxic effect of alcohol (T51) (d) Other entries where there is evidence of alcohol involvement determined by blood alcohol.	The general postcode address of persons resident in the area admitted to hospital, the date of such admissions and the sub-categories of each admission within the blocks.	In accordance with the International Classification of Diseases, Tenth Revisions (ICD-10) World Health Organisation.

Health Issue	Data Required	Standards
Persons admitted to hospital in respect of domestic abuse.	The general postcode address of persons resident in the area, and the date of such admissions.	Section 2.2. <i>Responding to domestic abuse: a handbook for health professionals</i> Department of Health December 2005.
Mental illness outpatient first attendances	Number of first attendances	
Persons receiving drug treatment.	Number of persons receiving such treatment.	
Ambulance Service calls to incidents relating to crime and disorder.	Time and date of calls and the category of such incidents.	Using any system for classifying crime and disorder used by that authority.

APPENDIX 2 Cont'd

Data on standards of data sharing:

Key Terms:

Depersonalised data: data that does not contain “personal data”.¹⁰

Personal data: data that would allow identification of a living individual – either from the data alone, or in combination with other data that the owner possesses or is likely to possess in the future.

(Typically, this would relate to data such as name, date of birth, address etc., but could include other data that would be likely to identify an individual. For example: ethnicity if the individual was one of a few ethnic minority residents in an area, or gender or age where this would allow the individual to be identified).

Personal Data also includes any expression of opinion about an individual, and any indication of the intentions of an organisation / other person in respect of that person.

- The administration of justice
- Maintaining public safety
- The apprehension of offenders
- The prevention of crime and disorder
- The detection of crime
- The protection of vulnerable members of the community
- Disclosure is necessary to support action under the Crime & Disorder Act
- Any disclosure must have regard to specific statutory restrictions on disclosure.

¹⁰ Within the meaning of the Data Protection Act 1998.

APPENDIX 3

RELEVANT STATUTES

Data Protection Act 1998

Schedules 2 and 3 of the Data Protection Act 1998 describe the conditions where data sharing of personalised data is lawful. For instance, the Act outlines that data sharing is lawful when consent is acquired from the person whose data is included in the data, where there is a legal obligation for the data to be shared and where it is necessary for the administration of justice. A full description can be found at: <http://www.essexdatasharing.gov.uk/Protocolguidappa.htm>

Crime & Disorder Act 1998 (Disclosure of data)

Section 115 provides a power to exchange data where disclosure is necessary to support the local Crime and Disorder Strategy or objectives outlined within it, which must be primarily aimed at reducing crime and disorder in accordance with the Act's provisions. Whilst Section 115 provides a power to share data - it does not contain an overriding requirement to disclose. Nor, does this power override other legal obligations such as the common law duty of confidence, the requirements of the Human Rights Act, compliance with the Data Protection Act (1998) or other relevant legislation governing disclosures.

Section 5 of the Crime & Disorder Act places a legal obligation on County, Unitary and District Councils, and Police¹¹ to produce crime and disorder strategies for their areas. 'Responsible authorities' are obligated to work in partnership with every police authority, probation committee, health authority or "other person or body of a description for the time being prescribed by order of the Secretary of State".

Schedule 9(5) of the Police and Justice Act 2006 now makes it a duty for these agencies to share depersonalised data.

Common Law (Duty of Confidence)

There is an inherent duty of confidentiality attached to all data that may be shared within activities undertaken by the Signatory partners in order to tackle issues relating to crime and disorder.

This duty of confidentiality exists whether the data/data is personal or non-personal and regardless of the reason for sharing the data.

Common Law stipulates that the following reasons justify sharing confidential data about a person:

- a) When consent is obtained from the person who is identified as the subject in the data (wherever possible, practicable or appropriate the permission of the Data Subject should be obtained);
- b) When the law or a court orders that the data must be shared;

¹¹ Collectively defined as 'responsible authorities'

c) When it can be demonstrated that disclosure is considered to be more in the best interests of the public than confidentiality. For example:

- Where there is a public interest or a public health interest;
- Where there is a risk of death or serious harm risk to a person(s);
- When disclosure is necessary to detect, prevent or prosecute serious crime;
- Where an individual's health is at serious risk (either the person identified in the data or another person);
- Where it is identified as being in interest of the person concerned

Human Rights Act 1998

The key principles of Article 8 are:

1. Everyone has the right to respect for their private and family life, their home and the privacy of their correspondence.
2. There shall be no interference by a Relevant Authority with this right except as in strict accordance with:
 - The law:
 - a) In the interests of national security.
 - b) In the interests of public safety.
 - c) The economic well-being of the country.
 - d) The prevention of crime or disorder.
 - e) The protection of public health or morals.
 - f) The protection of the rights or freedoms of others.
3. Any interference shall be proportional to the aims of the disclosure.

APPENDIX 3 (1)

THE EIGHT DATA PROTECTION PRINCIPLES

The DPA 1998 sets out 8 data protection principles that must be adhered to by data controllers when processing data:

1. Personal Data shall be processed fairly and lawfully.
2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.
8. Personal Data shall not be transferred to a country or territory outside the European Economic Area (EEA) 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.

APPENDIX 4

Caldicott Principles

Principle 1: Justify the purposes

Every proposed use or transfer of 'patient-identifiable data' (where the individual can be identified) within or from an organisation should be clearly defined and inspected. Continuing uses should be regularly reviewed by an appropriate person (known as the Caldicott Guardian). The Caldicott Guardian within The Thurrock Community Safety Partnership being Mr. Colin Slasberg.

Principle 2: Don't use patient-identifiable or client-identifiable data unless it is absolutely necessary

Patient-identifiable or client-identifiable data should not be used unless there is no alternative.

Principle 3: Use the minimum necessary patient-identifiable or client-identifiable data

If using patient-identifiable or client-identifiable data is essential, each individual item of data should be justified with the aim of reducing the possibility of an individual being identified.

Principle 4: Access to patient-identifiable or client-identifiable data should be on a strict need-to-know basis

Only those individuals who need access to patient-identifiable or client-identifiable data should have access to it, and they should only have access to the data they need to see.

Principle 5: Everyone should be aware of their responsibilities

Action should be taken to make sure that those handling patient-identifiable or client-identifiable data (clinical, non-clinical and non-health staff) are aware of their responsibilities to respect confidentiality of patients and clients.

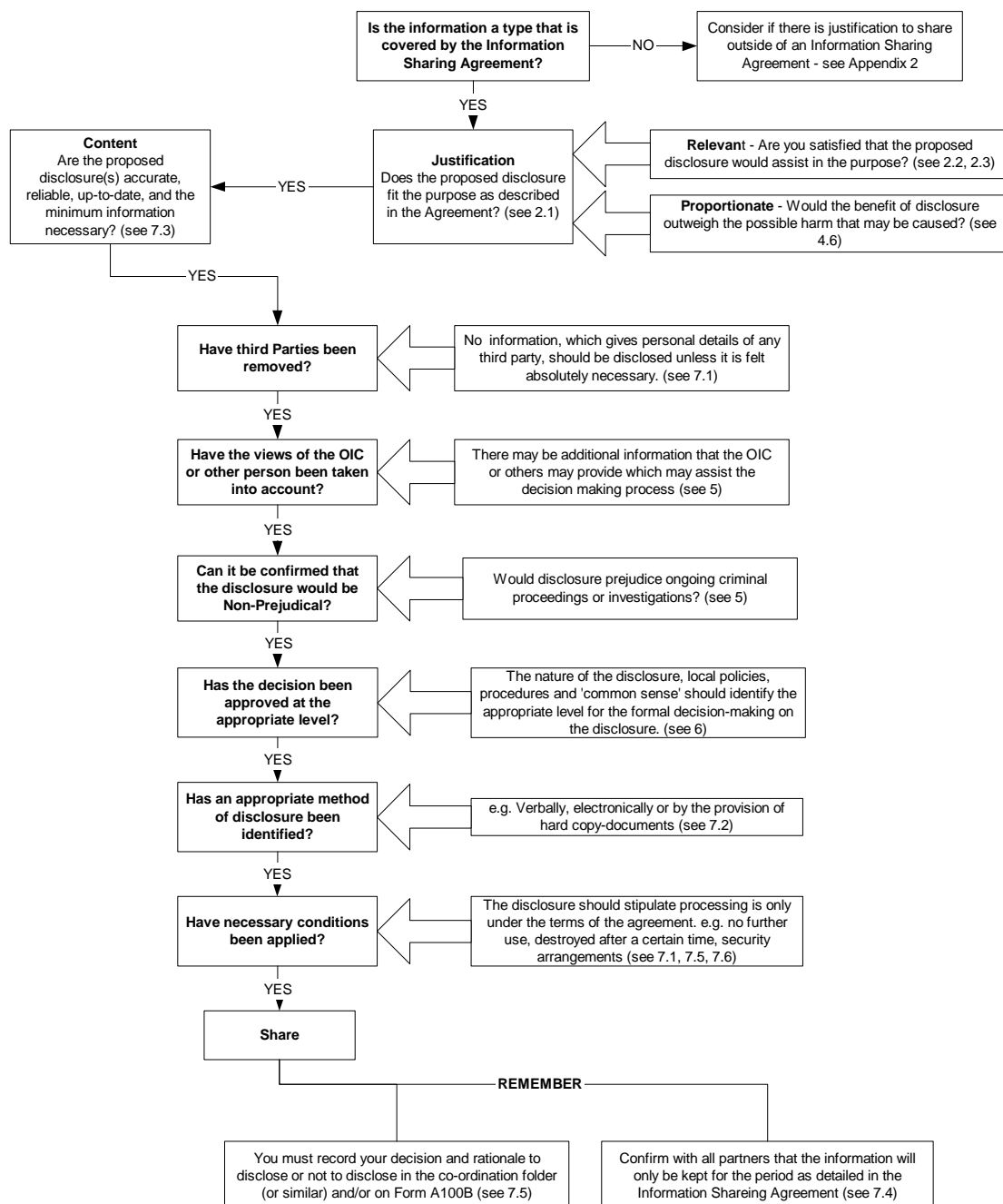
Principle 5: Understand and follow the law

Every use of patient-identifiable or client-identifiable data must be legal. Someone in each organisation should be responsible for making sure that the organisation meets legal requirements.

You can see the formal wording of the Caldicott principles at www.doh.gov.uk/ipu/confiden/guard/guardman.pdf

Appendix 5 – Decision Making Filter

This filter is designed to assist decision makers in determining, on a case by case basis, whether data of a particular type can be shared under the auspices of the data sharing Protocol (ISA) or Protocol.



APPENDIX 6 – Sharing Outside of the Protocol

1. Who is asking for the data?
2. Have you recorded their name, position, organisation and contact details?
3. Have you verified the identity of the person requesting the data?
4. What data is being asked for? What purpose will it be used for?
5. Is the data being requested, personal data?
6. Has a legal gateway or a policing purpose to share data been established?
7. If yes, how do they want the data?
8. When do they want the data?
9. Record your decision, how you made it and what data was shared.

APPENDIX 7

Sharing sensitive and patient identifiable information by email (NHS)

NHSmail (*.nhs.net)

In line with the NHS Chief Executive's directive NHSmail is a secure national email service which enables the safe and secure exchange of sensitive and patient identifiable information within the NHS and with local/central government.

All user connections to the service are encrypted. The service operates out of multiple secure, government-rated data centres to provide maximum levels of resilience and it has been independently assured by the Communications Electronic Security Group (CESG) process – the Information Assurance arm of GCHQ process.

Using NHSmail ensures the message is readable by authorised recipients, does not require any special software and removes the need to encrypt or password protect attachments.

Across the NHS

NHSmail is available at no cost to every NHS organisation in England and Scotland providing easy access to patient data across the NHS without the need to encrypt any content between NHSmail users.

Using NHSmail to email central and local government

Email sent to the communities below will be securely routed by NHSmail over the Government Secure Intranet (Gsi) if they are sent to the specified formally accredited secure email services. Content does not need to be encrypted.

Secure email domains in Central Government:

- *.gsi.gov.uk
- *gse.gov.uk
- *gsx.gov.uk

The Police National Network/Criminal Justice Services secure email domains:

- *.police.uk
- *.pnn.police.uk
- *.scn.gov.uk
- *.cjsm.net

Secure email domains in Local Government/Social Services:

*.gcsx.gov.uk

Emailing contacts outside of the NHS and central/local government

Regular Information Flows

NHSmail users that have a requirement to regularly exchange sensitive and patient identifiable information outside of the NHS/Government/Social Services can do so via the NHSmail third party programme. For further information please contact feedback@nhs.net

Infrequent Information Flows

NHSmail users that infrequently need to sensitive or patient identifiable message flows outside of the NHS/Government/Social Services should use the S/MIME tool. For additional information on S/MIME and how to use it, please see the NHSmail portal Training and Guidance pages in the section 'National and local policy and procedure.'

Encrypted attachments and NHSmail

Encrypted attachments are blocked by the NHSmail service and a number of government email systems, to avoid the risk of computer viruses being sent or received. Any attempts to bypass encrypted security controls in NHSmail must be avoided. The NHSmail antivirus software will remove encrypted attachments, but should an encrypted attachment bypass the antivirus software, subsequent automatic detection updates will automatically remove the attachment of any historic item.

Local NHS Email Services (*.nhs.uk)

The transmission of patient identifiable information to or from a local NHS email system (*.nhs.uk) should not be regarded as secure. As the transmission can involve messages being routed over the internet, the use of additional encryption solutions is required.

Not only should the sender ensure that they use a suitably encrypted method to send the patient information, but that the receiving system is also running as a secure service so that the patient information remains confidential.

Encryption Standards for Local Solutions

A comprehensive technical good practice guideline overview of 'Approved Cryptographic Algorithms' (techniques for encoding data) has been produced by NHS Connecting for Health and is available for download at:

<http://nww.connectingforhealth.nhs.uk/infrasec/gpg/acs.pdf>

However, when using a local encryption solution, encrypted attachments cannot be scanned for 'malware' (viruses for example) – creating a significant risk of virus infection and covert channelling.

When sending patient data, NHS organisations should undertake a local risk assessment on each email system they send to in terms of its secure operation/availability and the method of information exchange. The outcome of the risk assessment must be reported to the organisation's Board for each email system patient data is sent to, so that the Board is appropriately accountable for the decision to accept any data vulnerability/virus infection.

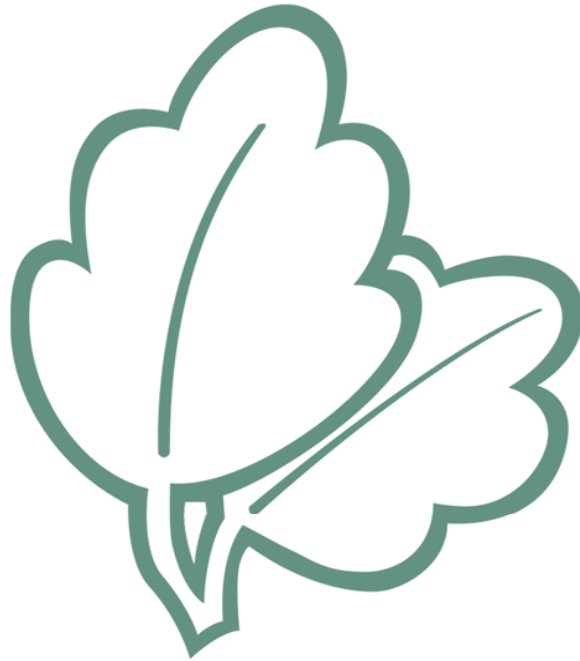
Appendix 8

Data Security and Encryption – Guidance (*Thurrock Council example*) July 2009

Signatories to the Thurrock Community Safety Partnership Information Sharing Protocol should be fully aware of Data Security and Encryption best practice guidelines. Some organisations signing this Protocol will have in place their own Data Security and Encryption guidelines, however, for those who do not, Thurrock Council's guidance should be followed as an example of best practice.

[Attached]

Data Security and Encryption



Version Control Sheet

<i>Title:</i>	Data Security and Encyption
<i>Purpose:</i>	To advise staff of the councils policy and procedures regarding data security and encryption
<i>Owner:</i>	Information Manager lhensley@thurrock.gov.uk 01375 652500
<i>Approved by:</i>	Corporate HR, Equality and Cultural Change Board
<i>Date:</i>	July 2009
<i>Version Number:</i>	1.0
<i>Status:</i>	Draft
<i>Review Frequency:</i>	Every 2 years
<i>Next review date:</i>	July 2011

Introduction

Information/data security is vital to Thurrock Council in the delivery of services to residents, businesses and visitors. The availability, integrity, security and confidentiality of information held is essential to ensure compliance with the Data Protection Act.

It is important that citizens are able to trust the Council to hold personal information securely when obtaining and holding information. This policy is designed to provide an appropriate level of protection to the information and data for which the council is responsible for.

Background

There are eight data protection principles in the Data Protection Act which the Council are required to comply with. They are sometimes referred to as the “principles of good information handling”. The principles apply to all personal information and principle 7 is a fundamental principle that covers the security of personal information.

Following the recent highly publicised losses of personal data by various Government agencies Thurrock has implemented encryption and secure data transfer software as an enabler to ensure that Council's data can be secured during electronic transfer and to prevent such data being intercepted.

The Council has gone to great lengths to ensure that the methods offered to partner organisations for the sharing of data are as secure and flexible as possible.

Scope

The scope of this policy is:

- To ensure that staff are made aware of the encryption and secure transfer processes that are now in place within the Council.
- To ensure that staff are made aware of the importance and need to hold personal information securely (both electronic and manual records).
- To ensure staff are fully aware of their responsibilities when storing personal data and confidential business information on portable media devices such as laptops and memory sticks.

Encryption and Secure Data Transfer

All staff should be aware of and comply with the following:

- *Do not email sensitive personal data to an external contact unless the information can be encrypted (or a secure data transfer process is used)* - Email can be an insecure delivery and storage mechanism so it is unsuitable for transmitting or storing personal data. The Council has implemented a data transfer/encryption solution and this should be used to send personal data off-site. Contact the Information Management Team for more information regarding the use of the encryption and secure data transfer solutions (email addresses with thurrock.gov.uk are safe to use as long as this address is used at both ends of the transfer).
- *If you need to send personal data within or outside of the Council then contact the Information Management Team about secure delivery mechanisms* - Personal data should only be sent when absolutely necessary, and must be delivered securely. In some cases information can be anonymised to prevent identification of individuals (e.g. remove names and address and use a shared code reference instead that is known by the recipient). The Information Management Team can provide advice on how this can be best achieved.
- *If you are in any doubt about whether data is 'personal data', or how to get laptops and transportable media encrypted then contact the Information Management Team for advice* - The Information Management Team can provide advice on whether any data you have would be regarded as personal data. This team can also provide advice on encrypting files and how to securely transport files to contractors and partners.

Security of data held on portable devices (such as laptops and memory/USB sticks)

The use of portable devices are subject to extra requirements because of the increased security risk these devices pose to information held by the Council.

All staff should be aware of and comply with the following guidelines:

- *Do not store personal data or confidential business information on unencrypted transportable media* - Transportable media is basically anything that can easily be removed from the office, so things like USB memory sticks, CDs, DVDs, floppy disks, etc should not contain unencrypted personal data.
- *If you are a Blackberry user you must make sure that your Blackberry is password protected to protect and secure personal and confidential data* - Within the Council there are two Blackberry models in use and instructions are available that show users how to enable a password on

a Blackberry. If you need assistance with this then contact the ICT helpdesk.

- *Do not store personal data or confidential business information on an unencrypted laptop* - Laptops are an easy target for thieves and it is very easy to access data from a laptop, even if they don't know your password, so you should not store any personal data on an unencrypted laptop. The Council are implementing a solution to encrypt data on laptops.
- If a portable device is shared amongst several users then a procedure (e.g. a log showing where the device is) must be in place to record the whereabouts of the device at all times.
- Security of the device is the responsibility of the user at all times.
- Lock the device away in a secure place when it is not in use
- Be aware of the additional security risks if leaving your device unattended or travelling with your device
- Do not install any software on the device – this must only be carried out through the ICT Helpdesk
- Do not connect the device to any foreign networks e.g. dial up modem, Bluetooth, Wireless etc
- Personal Use of Mobile Computing Device - Access to Council computing devices is only given for the purposes of undertaking council business. Personal record keeping, correspondence or games are prohibited, whether undertaken in personal time or not.
- Loss or Theft of a device - Incidents involving the loss or theft of a mobile device owned by the council should be reported immediately to the Information Manager.

General Data Security

All staff should be aware of and comply with the following guidelines:

- *Never give your password to anybody* - If you believe somebody else knows your password, please change it immediately and inform the Information Management Team if you think there may be a problem.
- *Do not store personal data or confidential business data on your PC hard drive or windows desktop* - Data stored on your C: drive or on your windows desktop is insecure. All files containing personal data must be stored on network drives with access on a need to know basis.
- If you move personal records away from your base location then these records must be held securely at all times.
- *If you currently have personal data, which is stored insecurely, you must secure it immediately* - You must remove any personal data from insecure locations. We would recommend you password protect any Word or Excel documents and store them on the secure network drive.
- *If you become aware of any loss of personal data or confidential business data you must contact the Information Management Team immediately* - The loss of any personal data is a serious matter and must be reported without delay, providing as much detail as possible.

- *If you become aware of any personal data that is not stored securely report this to the Information Management Team immediately* - This could be manual records stored in filing cabinets that are not locked.
- *Do not store personal data or confidential business information on a private PC, private laptop or personal transportable media* - Under no circumstances should personal data ever be stored or transported on non-business equipment/media. Those staff that work from home (and who cannot comply with this) should contact the Information Management Team for advice.

Standards for Secure Document Management

As an employee or agency worker, it is your responsibility to maintain the security of information owned or held by Thurrock Council by ensuring that it is accessible to those authorised to access it, and that it is not accessible to anyone else. An important aspect of this security is achieved through the storage of information. These standards apply equally to manual records, electronic records and emails.

All staff should be aware of and comply with the following guidelines:

- All records (manual and electronic) must be held securely. Records and ICT equipment (that contain records/data) must not be left in insecure locations (e.g left in vehicles).
- You should store documents to allow access to authorised users and appropriately restrict unauthorised users. This can be achieved through information technology (IT) security controls on network folders, documents and files or physical measures on rooms, cupboards or cabinets.
- You should not store confidential and non-confidential documents under the same access control.
- You should regularly review (at least annually) stored documents, files and folders in line with the Council's document retention policy.
- When disposing of documents, files or folders, then this must be undertaken securely.
- If you are responsible for shared documents, you should ensure that you understand your responsibilities and have the skills necessary to control access appropriately.
- If you are a Manager then it is your responsibility to ensure that all documents created or stored within your service area are appropriately managed in line with the principles of the Data Protection Act.

Key Points to note:

- The Authority's data and information is valuable and must be protected at all times.
- Users should be conversant with and comply with this policy and all ICT/Information Security policies including supporting policies/practice guides.
- Suspected breaches of the policy must be brought to the attention of a line manager, Information Manager or the Head of ICT immediately.
- Breach of the ICT policy or failure to report a breach could result in disciplinary action.

