

Essex Trust Charter

Sharing information between partner organisations is vital for providing co-ordinated services. Also, sharing information can help to meet the requirements of statutory and local initiatives.

This charter is an agreement in principle to share information. The charter will be supported by specific sets of rules (known as information-sharing protocols) that set out the details of sharing information.

To make sure there is a safe and secure environment for sharing information, the organisations signing the Trust Charter agree to do the following.

- Encourage all members to share information, unless it is illegal to share it or they have not received appropriate permission.
- Develop processes for sharing good information management practices to help the organisations work together, and support the aims of the Essex Trust Charter through the Essex Information Group.
- Make sure that those people giving us information also give us permission to share it, when appropriate.
- Work towards a common set of goals for sharing information.
- Help to develop a brand for the Essex Trust Charter to improve the trust between the organisations involved and the people of Essex.
- Work towards British Standard 7799, the technical standard for information security.





| Contents | Page |
|---|-------------|
| Essex Trust Charter | 1 |
| Introduction | 2 |
| Guidance notes | 3 |
| Appendix A – A list of charter members | 5 |
| Appendix B – The Trust Charter, trust services, e-government and the law | 6 |
| Appendix C – Caldicott principles | 8 |
| Appendix D – Information-sharing framework | 9 |
| Appendix E – Guidelines for procedures | 10 |
| Appendix F – Personal information | 11 |
| Appendix G – Glossary | 12 |

*Essex Organisations
Working Together*

Introduction

We have drawn up the Essex Trust Charter to support information-sharing between local authorities and health organisations in Essex. The Essex Trust Charter provides a framework for secure information-sharing to give those who use electronic public services confidence that their personal information will be handled responsibly.



Guidance notes

- 1 Each charter member (see Appendix A) will be responsible for making sure that they put the Essex Trust Charter into practice and follow the Caldicott principles (see Appendix C). We will invite charter members to the meetings of the Essex Information Group (EIG), which take place every three months. Each charter member taking part may choose whether to chair meetings and provide administrative support for the EIG. The EIG will decide whether subgroups are needed to work on specific information-sharing initiatives.
- 2 To keep people informed of developments, we intend to hold a conference for charter members each year. This will provide an opportunity to compare Essex against relevant national, international and e-government initiatives.
- 3 Charter members who want to withdraw from this agreement at any time should write to the Information Sharing Information Security Manager at Essex County Council.
- 4 EIG will review this agreement each year on or around 1 April.
- 5 To encourage trust, charter members will actively share information between their agencies, if it is legal to do so. Within legal limits, people have the right to:
 - see information that is stored about them;
 - comment on it; and
 - have their information treated with appropriate confidentiality.

Charter members agree to meet the requirements of the Human Rights Act 1998 and the Data Protection Act 1998, along with any other relevant government recommendations, statutes and laws governing the specific areas of work covered by individual information-sharing protocols (sets of rules). Where details of individuals are being shared, charter members will follow the Caldicott principles. You can find details of the Caldicott principles in Appendix C and the full information-sharing framework in Appendix D.

- 6 The Essex Trust Charter does not mean that members must share all their information. Members can choose specific parts of the information-sharing framework (see Appendix D).
- 7 The information to be shared under the agreement will fall into four categories. They are:
 - Non-sensitive – non-personal or personal information that is not sensitive (see Appendix F).
 - Sensitive – sensitive personal information as defined by the Data Protection Act (DPA) 1998.
 - Simple – fixed information that is not open to interpretation (for example, date of birth).
 - Complicated – information that is open to interpretation or has legal implications (for example, details of contact with a social worker).



Here are some examples.

| Category | Class | Examples |
|-----------------|-------------------------------|------------------------------|
| 1 | Non-sensitive and simple | Statistical information |
| 2 | Non-sensitive and complicated | Change of address |
| 3 | Sensitive and simple | Ethnic background or beliefs |
| 4 | Sensitive and complicated | Crime and disorder or health |

- 9 For each subject area or information-sharing purpose, the charter member involved will develop a protocol. The standard format for this is shown in Appendix E. Some protocols may be combined to develop a common protocol. Each protocol will be supported by procedures, which will be developed to suit all the members involved.

*Essex Organisations
Working Together*



Appendix A – A list of charter members

The following organisations could sign up to the Essex Trust Charter.

Basildon and Thurrock University Hospitals NHS Trust
Basildon District Council
Basildon Primary Care Trust (PCT)
Billericay, Brentwood and Wickford Primary Care Trust (PCT)
Braintree District Council
Brentwood District Council
Castle Point and Rochford Primary Care Trust (PCT)
Castle Point Borough Council
Chelmsford Borough Council
Chelmsford Primary Care Trust (PCT)
Colchester Borough Council
Colchester Primary Care Trust (PCT)
Epping Forest District Council
Epping Forest Primary Care Trust (PCT)
Essex Ambulance Service NHS Trust
Essex County Council
Essex Fire and Rescue Service
Essex Police
Essex Rivers Healthcare NHS Trust
Essex Strategic Health Authority
Harlow District Council
Harlow Primary Care Trust (PCT)
Maldon and South Chelmsford Primary Care Trust (PCT)
Maldon District Council
Mid Essex Hospital Services NHS Trust
New Possibilities NHS Trust
North Essex Mental Health Partnership NHS Trust
Rochford District Council
South Essex Partnership NHS Trust
Southend Borough Council (Unitary)
Southend Hospital NHS Trust
Southend on Sea Primary Care Trust (PCT)
Tendring District Council
Tendring Primary Care Trust (PCT)
The Princess Alexandra Hospital NHS Trust
Thurrock Borough Council (Unitary)
Thurrock Primary Care Trust (PCT)
Uttlesford District Council
Uttlesford Primary Care Trust (PCT)
Witham, Braintree and Halstead Care Trust

Last updated: 31 July 2003. An up-to-date list of charter members will appear on the internet (www.EssexInformationSharing.gov.uk).



Appendix B - The Trust Charter, trust services, e-government and the law

- 1 The idea for a trust charter agreed by different organisations is taken from 'Trust Services: E-government Strategy Framework Policy and Guidelines' (Volume 3, September 2002). You can see a copy of this at www.e-envoy.gov.uk/assetRoot/04/00/22/47/04002247.doc
- 2 The Government's trust services framework shows the security measures required by the Cabinet Office. These measures will make sure that transactions can be properly traced, with named individuals responsible for them. The security measures are provided through a two-tier structure:
 - the Trust Charter itself; and
 - information-sharing protocols.
- 3 The main purpose of the Trust Charter is to give customers using electronic public services confidence that their personal information is being handled appropriately. Guidance on developing e-government trust charters is provided in the 'Trust Charter for Electronic Service Delivery'. You can see a copy of this at www.dca.gov.uk/consult/datasharing/datashare.htm#anna
- 4 E-government framework policies are an important part of the e-Government Interoperability Framework (e-GIF). You can see a copy of this at www.e-envoy.gov.uk/Resources/FrameworksAndPolicy/fs/en
- 5 The Office of the e-Envoy encourages local authorities and health organisations to work together to put a trust charter into practice so they can meet the requirements of the Data Protection Act 1998 and the Freedom of Information Act 2000.
- 6 Trust charters and information-sharing protocols must keep to the following legislation.
 - The Human Rights Act 1998 and the European Convention on Human Rights, which sets out the individual's right to privacy in correspondence.
 - The Data Protection Act 1998, which sets out requirements for handling and protecting personal information that organisations hold.
 - The Electronic Communications Act 2000, which sets out the appropriate use of electronic signatures.
 - The Interception of Communications Act 1985, which makes it an offence to intercept calls on a public phone system without the knowledge of the caller, unless a legal case is put forward to do so within specific time limits.



- The Regulation of Investigatory Powers Act 2000, which deals with the offence of interception and extends this to private networks. The Act also regulates access by employers to communications that their employees use.
 - The Wireless Telegraphy Act 1949, which controls the monitoring of radio transmissions.
 - The Police and Criminal Evidence Act 1984, which sets out the situations when the police are allowed to gather and use evidence from electronic communications.
 - The Computer Misuse Act 1990, which makes attempted or actual breaking into (or sabotaging) computer systems a criminal act.
 - The Public Records Act 1958, which sets out requirements for storing and maintaining documentary records of government activities.
 - The Official Secrets Act 1989, which sets out how government information is controlled.
 - The Freedom of Information Act 2000, which sets out the individual's rights of access to information held by local authorities and health authorities.
- 7 It is also important to follow technical standards to make sure that the information used when operating e-services is shared in a safe and secure environment. You can find details of the technical standards in the 'Security: e-Government Strategy Framework Policy and Guidelines'. You can see a copy of this at www.e-envoy.gov.uk/assetRoot/04/00/28/34/04002834.pdf
- 8 Information security standards BS7799 and ISO17799 are a code of practice with details of what needs to be taken into account when setting up secure information communications technologies (ICTs) — that is, ways of sharing information over the internet or phone. These technical standards provide a set of controls to make sure best practice for e-government trust services is followed. You can get information on the standards from the website of the British Standards Institute at www.bsi-global.com/index.xalter#

*Essex Organisations
Working Together*



Appendix C – Caldicott principles

Principle 1: Justify the purposes

Every proposed use or transfer of 'patient-identifiable or client-identifiable information' (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).

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

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

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

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

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

Only those individuals who need access to patient-identifiable or client-identifiable information should have access to it, and they should only have access to the information 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 information (clinical, non-clinical and non-health staff) are aware of their responsibilities to respect confidentiality of patients and clients.

Principle 6: Understand and follow the law

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

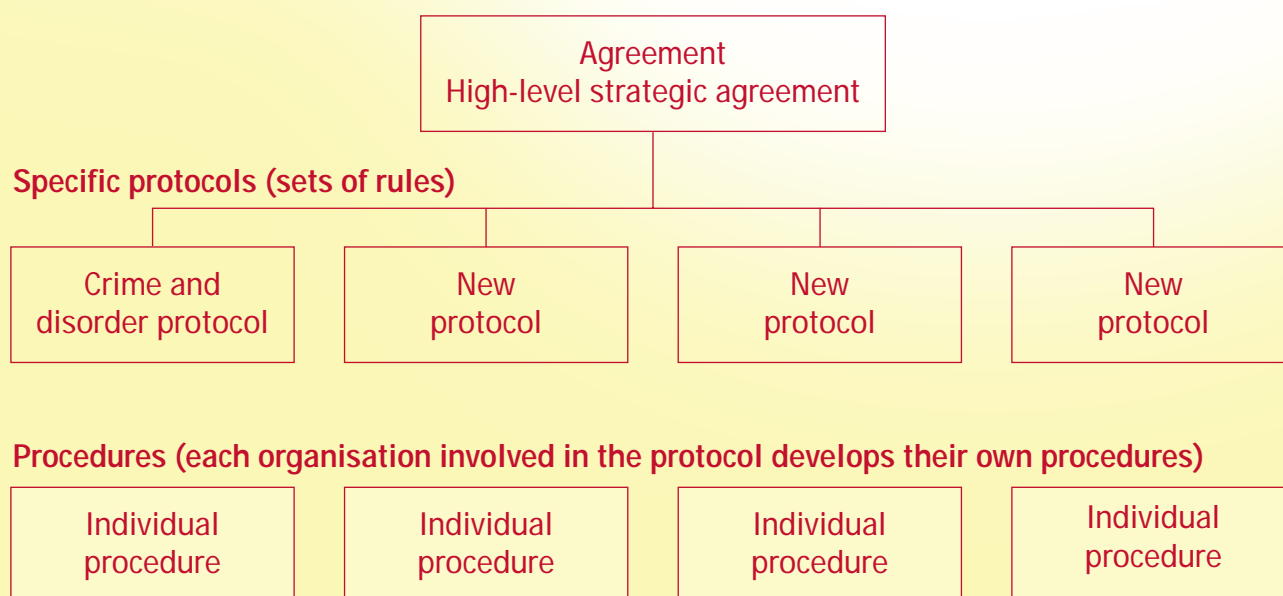
You can see the formal wording of the Caldicott principles at www.doh.gov.uk/ipu/confiden/guard/guardman.pdf



Appendix D – Information-sharing framework

This framework is based on central government guidance on trust charters.

Essex Trust Charter



Agreement: A county-wide multi-agency agreement.

- **Purpose:** A single guiding policy to encourage trust among people in Essex and between charter members to meet e-government requirements.
- **Strategic responsibility:** Essex e-Champions (see the glossary)

Specific protocols: Detailed multi-agency rules for specific areas of work or types of information-sharing (for example, crime and disorder).

- **Purpose:** To allow both personalised and non-personalised information to be shared as set out in legislation.
- **Responsibility:** These are multi-agency agreements and individual charter members involved are responsible for different areas.

Procedures: Detailed operational procedures for individual charter members.

- **Purpose:** To specify the processes for sharing and receiving information in line with relevant protocols.
- **Responsibility:** Each charter member will be responsible for their own procedures.



Appendix E – Guidelines for protocols

Each protocol should tackle all the areas listed below.

1 Legal duties and legislation

- Common law
- Article 8 of the Human Rights Act
- Data Protection Act 1984
- Data Protection Act 1998
- Caldicott principles
- Other relevant legislation

2 Managing the protocols

- Defining the responsibility for the protocol
- Involving the Caldicott Guardians
- Relationship to the Essex Trust Charter
- Charter members involved

3 Sharing information

- General principles, including the main purpose
- Details of information and ways of sharing non-personal information
- Details of information and ways of sharing personal information
- Data controllers, as defined in the Data Protection Act
- Information security
- Confidentiality and privacy
- How much information will be shared and who with
- Using the shared information for purposes that are different from the purpose for which it was originally shared
- Quality of the information
- Documents
- Reviewing, holding on to and destroying information
- Getting permission
- How the information will be shared so that it works within the systems in each of the organisations involved
- Common set of terms and language

In future it may be necessary to take account of:

- Person Name Standard BS8766; and
metadata (see the glossary).



Appendix F – Personal information

The Data Protection Act defines categories of sensitive personal data, that is, personal data made up of information on:

- a the racial or ethnic origin of the 'data subject' (the person whose information it is);
- b his or her political opinions;
- c his or her religious beliefs, or other beliefs of a similar nature;
- d whether he or she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- e his or her physical or mental health or condition;
- f his or her sexual life;
- g him or her committing, or allegedly committing, any offence; or
- h any proceedings for any offence committed (or alleged to have been committed), how the proceedings are finalised, or the sentence of any court in proceedings.

For the purposes of information-sharing under the Essex Trust Charter, non-sensitive personal information is information on individuals that is not defined in the Data Protection Act as sensitive.

*Essex Organisations
Working Together*



Appendix G – Glossary

Brand

A mark to show quality, ownership or a distinctive characteristic. The name of an organisation can also act as a brand.

e-Government Interoperability Framework (e-GIF)

The e-GIF sets out the Government's technical policies and standards for achieving better government using the internet. It is an important policy in the strategy for moving towards providing many government services electronically.

Essex e-Champion

A designated officer or elected member who leads work in his or her local authority towards providing services in Essex electronically. e-Champions work together to support council members and senior managers from all local authorities in developing strategies and setting priorities.

Intercept

To listen to.

Metadata

Structured information about an item of information (or 'data about data') which describes its content, quality, condition and other important characteristics.

Procedure

A series of actions which are followed in the defined order.

Protocol

A set of rules.

*Essex Organisations
Working Together*