



Trafford Children and Young People's
Service Information Sharing Toolkit Tier 8

Privacy, Confidentiality and Consent Practical Guidance

January 2008



Trafford Healthcare **NHS**
NHS Trust

Trafford **NHS**
Primary Care Trust

Trafford CYPS brings together council and health services to improve outcomes for children, young people, their families and schools.

Contents

1. Introduction.....	3
1.1. General	3
1.2. Scope of Privacy, Confidentiality & Consent	3
2. Key Features of Privacy, Confidentiality & Consent Documents	4
2.1. General	4
2.2. Language aimed at the appropriate audience.....	4
2.3. Layout and appearance aimed at the appropriate audience.....	4
3. Privacy Statements/Fair Processing Notices	5
4. Confidentiality Statements	6
5. Consent Form	7
APPENDIX 1 Consent Form Template.....	9
APPENDIX 2 Confidentiality Agreement Template	10
APPENDIX 3 Third Party Confidentiality Agreement Template	11
APPENDIX 4 Confidentiality Agreement for Multi-Agency Meetings Template.....	14

1. Introduction

1.1. General

- 1.1.1. This Service Users Privacy, Confidentiality & Consent document is the fourth (Tier 8) element of the Toolkit. It will cover the range of processes and documentation that will directly impact upon the expectations and rights of service users in regard to the use of their personal information
- 1.1.2. Whenever organisations collect personal information they must ensure that all their service users have been made aware of who they are (i.e. the name of the organisation), why they need peoples personal information (i.e. the purpose(s)), the type of personal information they gather, its source(s), what they will do with it (including under what circumstances it may be shared), when they will dispose of it, how it will be safeguarded and what their (service user) individual rights are in respect of privacy, confidentiality, consent and access and how these may be exercised.
- 1.1.3. In order for this to have validity with service users it must be relevant to their particular circumstances and the support provided to them at that point in time; i.e. it should be *service specific*. So, for example, a multi-sector organisation (e.g. local authority) should not produce one over-arching statement of the way it protects all personal information but should produce separate statements for each of its services so that service users can clearly see within a specific context why their information is needed and what will happen to it.
- 1.1.4. However, where organisations have come together in partnership to work with a common group of service users for a specific purpose(s), as described in an associated Information Community Agreement/Operational Arrangement, then an agreed set of standard processes and documents (e.g. Privacy Statement/Fair Processing Notice, Consent Processes, etc) should be put in place across those organisations.
- 1.1.5. If an organisation believes that these areas are already covered within their existing policies and procedures documents then it would be sufficient to give a summary with relevant cross-references. Those documents, including any examples specifically aimed at service users, should then be made available to all other partners by whatever means are appropriate.

1.2. Scope of Privacy, Confidentiality & Consent

- 1.2.1. This is a difficult area to formally structure, especially as the Toolkit is a 'generic' set of documents capable of being used by all services working in all sectors that will necessitate differing processes and documents each aimed at a slightly different service user audience.
- 1.2.2. However, with this in mind this Tier 8 document aims to provide operational managers and practitioners, as well as specialist support officers, with a suggested key features structure that could be applied to 'Privacy Statements'/'Fair Processing Notices', 'Confidentiality Statements' and 'Consent' processes which will support the appropriate 'Information Community Agreement(s)/Operational Arrangement(s)'.
- 1.2.3. It is good practice to involve the service users and any specialist support officers in the development of this, as well as those managers and

practitioners who have negotiated and agreed the relevant 'Information Community Agreement(s)/Operational Arrangement(s)' and who are involved in their practical application.

2. Key Features of Privacy, Confidentiality & Consent Documents

2.1. General

- 2.1.1. This section describes the common key features considered to be 'good practice' for single or multi-agency 'Privacy Statements'/'Fair Processing Notices', 'Confidentiality Statements' & 'Consent Forms'.
- 2.1.2. Sections 3 to 5 following describe the key elements that should be included within each of the specific documents.
- 2.1.3. All of these documents should be short and concise; readers do not want to be overwhelmed with a mass of detail. However, they should be told where they can get more information should they wish.
- 2.1.4. All should be designed to reflect the service user's perspective rather than the organisation's/practitioner's.

2.2. Language aimed at the appropriate audience

- 2.2.1. A balance has to be struck between the length and level of detail and its accessibility. Key concepts should be explained concisely and without the use of abbreviations, complex language or jargon. Where these documents are for multi-agency working then concepts should be worded in such a way as to avoid referring to any particular agency.
- 2.2.2. Techniques that should be considered include the use of bullet pointed lists of key aspects or a question and answer format to break the information into small contextualised chunks. These can be followed by more detailed explanations of the same issues where necessary. This will make a statement/notice/consent form accessible to people with a range of reading/cognitive skills.
- 2.2.3. Ensure that, where appropriate, the statements/notices/consent forms are made available in other languages and formats (e.g. on tape, large print or Braille). Their availability should be made clear on the 'primary' statements/notices/consent forms.

2.3. Layout and appearance aimed at the appropriate audience

- 2.3.1. The use of colour and fancy layout can be a two edged sword. A 'Privacy Statement'/'Fair Processing Notice' must be accessible to the relevant audience (i.e. children, young people, adults and their families) but not at the expense of content or credibility.
- 2.3.2. Ideally text should be split into regions using (coloured) boxes or appropriate sourced original images (for children/young people consider coloured balloons). This can serve to both improve the legibility of the document and, provided the appropriate images have been used, its appeal to its target audience.
- 2.3.3. However, it is important to recognise that too 'busy' a layout, insufficient contrast, small type size and high text density all contribute to making the material less accessible particularly to people with visual impairments.

- 2.3.4. If images of people are to be used on the statements/notices/consent forms they should represent a range of cultural and ethnic groups appropriate to the service being delivered (e.g. remember to use images of children/young people on documents aimed at them).

Trafford Employees must consider the guidance available in the Corporate Communications Strategy when producing any leaflet

3. Privacy Statements/Fair Processing Notices

A 'Privacy Statement'/'Fair Processing Notice' must contain the following elements:

3.1. Who you (the organisation/partners) are

- 3.1.1. Explain who you and, if appropriate, other partners are. This may seem obvious but it is a requirement of the Data Protection Act 1998 that people are informed of the identity of the data controller or controllers.

3.2. Why you need people's personal information

- 3.2.1. Explain why the information you are asking for is necessary for you to provide the service required. This will demonstrate how you comply with the 3rd data protection principle that data should be adequate, relevant and not excessive. Consider also whether the information will be used for any secondary purposes such as statistical analysis or staff training and include these.

3.3. What sort of personal information you will be gathering and storing

- 3.3.1. Explain what information you will be gathering (e.g. Name, Address, DOB, School, Ethnicity, Needs, etc) and how this will be securely stored (e.g. manual files, computer databases, etc).
- 3.3.2. Also explain how you will treat the two different types of service user information 'Personal' and 'Sensitive' and whether, for example, there are different consent processes attached.
- 3.3.3. Finally, explain where you are obtaining from (e.g. direct from service users, from parents, other practitioners, schools, etc).

3.4. Who can access it

- 3.4.1. Explain who is able to access a service users information and under what circumstances. If access to certain information is restricted to certain organisations and/or practitioners then this should be stated.

3.5. What you will do with it (including sharing & consent)

- 3.5.1. Explain how you will use the information to provide a service or services including whether their information will be passed to another organisation and whether they have a choice about it.
- 3.5.2. If information is shared with other organisations explain why (e.g. to provide better integrated services) and if they have a choice make sure that it is clear that they can say 'no'.
- 3.5.3. If they choose not to allow their information to be shared or withdraw their consent then the leaflet should explain the possible consequences of this but in a manner that is not judgmental or could be perceived to be 'bullying'.

3.5.4. If information is shared without people's knowledge and/or consent (e.g. the law says we must or it is to produce statistics) then this should be mentioned.

3.6. When you will dispose of it

- 3.6.1. Explain how long information will be kept for and the procedures for its destruction. This will allow you to demonstrate compliance with the 5th data protection principle that data should not be kept for longer than is necessary.
- 3.6.2. There will be circumstances when it would not be practical to say when data is destroyed (e.g. when it could enable fraud). In such cases a general assurance will be sufficient.

3.7. How you will safeguard & maintain it

- 3.7.1. Explain how information will be protected from unauthorised access or disclosure. This will allow you to demonstrate compliance with the 7th data protection principle.
- 3.7.2. Also explain how you ensure information is accurate and up-to-date (e.g. any regular updating or validating exercises you carry out, service user requests for inaccurate data to be corrected, etc). This will allow you to demonstrate compliance with the 4th data protection principle that information is accurate and up-to-date.
- 3.7.3. This section should be as non-technical as possible but should provide a general reassurance on staff's commitment to security and confidentiality and to the security of IT systems.

3.8. How people can check the information you hold on them

- 3.8.1. Explain to service users their subject access rights, including letting them know how they can ask for inaccurate information to be corrected, or tell them where they can get further details on this and if a charge will apply.
- 3.8.2. Also explain who can exercise those rights; i.e. any competent person in their own right if aged 12 years or more, parents/responsible adults on behalf of children (under 12 years) or parents/responsible adults on behalf of those considered not being competent.

3.9. How people can get more information and complain

- 3.9.1. Give full contact details of who people can go to if they want further details on your information handling policies or to make a complaint.
- 3.9.2. Also include details, where appropriate, of any public facing information channels where this and other related material may be accessed (e.g. organisation websites, one-stop shops, etc).

4. Confidentiality Statements

- 4.1. Not all organisations feel that they require separate 'Confidentiality Statements' either because they see no operational justification for them or they feel that the requirements are delivered via other information channels such as the 'Privacy Statement'/'Fair Processing Notice' or their 'Consent' processes.
- 4.2. Others have very specific requirements and practices such as the NHS & Social Care as enshrined in their 'Confidentiality Code of Practice'.

- 4.3. Where it is felt necessary or desirable to produce a 'Confidentiality Statement' then the following elements are recommended for inclusion:
- 4.3.1. Who you (the organisation/partners) are. Explain who you and, if appropriate, other partners are.
 - 4.3.2. Why you need people's personal information. Explain why the information you are asking for is necessary for you to provide the service required.
 - 4.3.3. What is the Common Law Duty of Confidentiality? Explain what the 'Common Law Duty of Confidentiality' is and its meaning in regard to information sharing.
 - 4.3.3.1. Also explain that the duty is not an absolute right and the circumstances in which it may be overridden.
 - 4.3.4. What are the obligations on individual practitioners working for you? Explain what is expected of your staff and the steps taken to avoid unauthorised access to, or inappropriate disclosure of, personal information.
 - 4.3.5. How can people get more information and complain? Give full contact details of who people can go to if they want further details on your information handling policies or to make a complaint.
 - 4.3.5.1. Also include details, where appropriate, of any public facing information channels where this and other related material may be accessed (e.g. organisation websites, one-stop shops, etc).

5. Consent Form

A 'Consent Form' is a *legally binding* document designed to record informed consent and must be understood by the person signing them. It must contain the following elements:

5.1. General Information

- 5.1.1. Details of the organisation seeking the consent (name, address, logo, etc)
- 5.1.2. Details of the service user from whom consent is sought (name, address, DOB, UID, etc)
- 5.1.3. Details of the organisation(s) with whom the information is to be shared (name, address, service type, etc)
- 5.1.4. An unambiguous declaration (standard statement) from the service user agreeing to the information sharing (ideally this should be at the end of the consent document)
- 5.1.5. A place for the service user, and or their parent/responsible adult, and practitioner to sign and date the document

5.2. What information is to be shared?

- 5.2.1. Explain what information is to be shared in a clear and unambiguous manner. If possible define and list the information to be shared; including if the personal identifiable information is in the form of image or voice recordings.
- 5.2.2. If consent is restricted to specific information (e.g. personal or sensitive) and/or specific organisations then this must also be made clear.

5.3. With whom is information to be shared?

- 5.3.1. Explain with whom information is to be shared ideally listing the agreed agencies.
- 5.3.2. If any agencies are to be explicitly excluded from this information sharing then this must also be made clear.

5.4. Why is information to be shared?

5.4.1. Explain the reasons for sharing information with organisations. Ensure that it is clear and concise and that it has a positive focus highlighting that the objective is to improve services for the child, young person, adult and their families.

5.5. Is there a time limit to the consent?

5.5.1. Explain whether the consent is for a fixed period (e.g. 12 months from agreement), is determined on a case-by-case basis or has regular review period.

5.5.2. In all of these the time limit must be clearly and unambiguously stated on the form.

5.6. How to withhold/withdraw consent?

5.6.1. Explain how consent may be withheld or withdrawn and the possible consequences of these.

5.6.2. However, you must ensure that the wording does not 'bully' a service user into believing that consent must be given. The explanation must be clear and non-judgemental and it may be contained in a more specialised document such as a 'Privacy Statement'/'Fair Processing Notice'.

5.7. How to obtain advice on information sharing?

5.7.1. Explain how to obtain advice on information sharing. This could be achieved by simply providing pointers to more detailed information leaflets such as 'Privacy Statements'/'Fair Processing Notices' or providing the details of a professional who can give such advice and support.

APPENDIX 1

Consent For Information storage and information sharing:

By signing this document, I understand that information about me will be stored on paper and electronically and used for the purpose of providing services to:

Me

The child/ young person for whom I am Parent/Carer

Name of Child/young person:

.....

Their DoB.....

Trafford CYPS will seek to renew this consent every 12 months or if my circumstances change significantly (which ever occurs soonest). Should I decide to withdraw my consent to share my information, then I understand that by doing so I may not receive all the services I may require to support my needs.

However I also understand that confidential information sometimes has to be shared without my consent to:

- Protect children, young people or adults from risk of significant harm;
- Prevent or detect a crime; or
- Prevent an unjustified delay in making enquiries about allegations of significant harm.

Unless there is risk to me or my family, Trafford CYPS will inform me if they have to share my information in these circumstances.

I can obtain more information on why and how Trafford CYPS processes information from one of the following guides:

- Sharing Information, a Guide for Service Users, Parents & Carers
- Sharing information, a Guide for Young People

I **agree/disagree*** to this information being shared between children & young people's services and relevant external agencies to support the delivery of services to me/my family.

Signed

Name

Date

***delete as appropriate**

APPENDIX 2

Confidentiality Information Agreement

This Agreement should be signed by all staff in Trafford CYPS, Primary Care Trust, Healthcare Trust, those on placements within these organisations and partners granted permission to access SAP. It should be signed in conjunction with reading the 'Trafford CYPS/HCT/PCT Information Sharing and Confidentiality Policy and Guidance' which details the principles and legal context staff should be aware of and follow when sharing and processing information. The purpose of data protection legislation is to regulate the way that personal information is processed about individuals, whether held on computer or in a manual filing system. For the purpose of this document, those services within Trafford CYPS shall be referred to as 'CYPS', and those within either the Primary Care Trust or Health Care Trust shall be referred to as 'Trust'

Your Responsibilities

Confidential information shall include all information related to Trafford CYPS, Primary Care Trust, Health Care Trust and CYPS Safeguarding Children Service. This includes all confidential records, reports, documents and other information which is collated, acquired and presented. It also covers information held on IT databases.

- Information will be processed and shared in accordance with the Data Protection Act 1998.
- Information Sharing is only permitted where specific consent is obtained from the service user or where an information sharing protocol and/or matrix is in place. Information Sharing can occur without consent in certain circumstances i.e. Child Protection matters (See Trafford CYPS/HCT/PCT Information Sharing & Confidentiality Policy and Guidance for clarification).
- Where IT access to a database has been permitted, under no circumstances must information held on that database be shared with any other colleagues, unless they have authorization to hold the information. Information in any format should only be accessed regarding your caseload or designated duties, unless you have delegated authority to access particular systems as part of your job.
- Where SAP is accessed by partners, they should record any enquiry they make onto the system appropriately to ensure there is an audit trail of users and their access.
- Trafford CYPS reserves the right to audit, investigate, monitor, access, review, and disclose information related to your use of the organisation's information systems at any time, with or without advance notice to you and with or without your knowledge.
- When your employment or association with Trafford CYPS/Trust ends, you will not access any Trafford CYPS/Trust information systems that you had access to; legal action may result if you do.
- You will not divulge to any third party any confidential information belonging to your employing organisation or any other partner agencies or individuals.

You should ask your supervisor for clarification if there are any items you do not understand before signing this agreement. Your signature below acknowledges that you have read and understood this agreement and realise it is a condition of your employment/ association with Trafford CYPS/Trust. A copy of this signed agreement will be made available to you at your request.

Sign Name.....

Print Name.....

Date.....

APPENDIX 3

Confidentiality Agreement for Third Party Agents

1 Who are third parties covered by this agreement?

Third parties are located on-site for a period of time as defined within their contract, they include:

- Contractors
- Inspectors employed for serious case files reviews
- Consultants

The third party agent, supplier or contractor undertakes:

- To treat as confidential all information which may be derived from or be obtained in the course of the contract or which may come into the possession of the contractor or an employee, servant or agent or sub-contractor of the contractor as a result or in connection with the contract; and
- To provide all necessary precautions to ensure that all such information is treated as confidential by the contractor, his employees, servants, agents or sub-contractors; and
- To ensure that he, his employees, servants, agents and sub-contractors are aware of the provisions of the Data Protection Act 1998 and BS7799 and that any personal information obtained from Trafford CYPS, Health Care Trust* or Primary Care Trust shall not be disclosed or used in any unlawful manner; and
- To indemnify Trafford CYPS, Health Care Trust or Primary Care Trust* against any loss arising under the Data Protection Act 1998 caused by any action, authorised or unauthorised, taken by himself, his employees, servants, agents or sub-contractors.

All employees, servants, agents and/or sub-contractors of the third party agent or Contractor will be required to agree to and sign a confidentiality statement when they come to any of Trafford CYPS, Health Care Trust or Primary Care Trust* sites where they may see or have access to confidential personal and/or business information.

2 **Supplier Code of Practice** (based on example from Introduction to Data Protection in the NHS (E127) and BS7799)

- 1 The following Code of Practice applies where access is obtained to Trafford CYPS, Health Care Trust or Primary Care Trust* personal data/information, as defined within the Data Protection Act 1998.

- 2 The Supplier must certify that his organisation is registered appropriately under the Data Protection Act 1998 and legally entitled to undertake the work proposed.
- 3 The Supplier must undertake not to transfer the personal data/information out of the EEA unless such a transfer has been registered, approved by Trafford CYPS, Health Care Trust or Primary Care Trust* and complies with the Information Commissioners guidance on Safe Havens.
- 4 The work shall be done only by authorised employees, servants, or agents of the third party or contractor who are aware of the requirements of the Data Protection Act 1998 of their personal responsibilities under the Act to maintain the security of Trafford CYPS, Health Care Trust or Primary Care Trust* personal data/information.
- 5 While the data/information is in the custody of the third party agent or contractor it shall be kept in appropriately secure means.
- 6 Any data/information sent from one place to another by or for the third party agent or contractor shall be carried out by secure means. These places must be within the supplier's own organisation or an approved sub-contractor.
- 7 Data/Information which can identify any service user/employee of Trafford CYPS, Health Care Trust or Primary Care Trust* must only be transferred electronically if previously agreed by Trafford CYPS, Health Care Trust or Primary Care Trust*. This is essential to ensure compliance with strict controls surrounding the electronic transfer of identifiable personal data/information and hence compliance with the Data Protection Act 1998 and BS7799. This will also apply to any direct-dial access to a computer held database by the supplier or their agent.
- 8 The data/information must not be copied for any other purpose than that agreed by the third party agent or contractor and Trafford CYPS, Health Care Trust or Primary Care Trust*.
- 9 Where personal data/information is recorded in any intelligible form, it shall either be returned to the Trafford CYPS, Health Care Trust or Primary Care Trust* on completion of the work or disposed of by secure means.
- 10 Trafford CYPS, Health Care Trust or Primary Care Trust* will expect an escalation process for problem resolving relating to any breaches of security and/or confidentiality of personal information by the third party agent or Contractor employee and/or any agents and/or sub-contractors.
- 11 Any security breaches made by the third party agent or Contractor employees, agents or sub-contractors will immediately be reported to the Caldicott Guardian of Trafford CYPS, Health Care Trust or Primary Care Trust*.

Certification form:

Name of third party
Agent or Contractor: _____

Address of third party
agent or Contractor: _____

Telephone number: _____

E-mail details: _____

On behalf of the above organisation I certify as follows:

- The organisation is appropriately registered under the Data Protection Act 1998 and is legally entitled to undertake the work agreed in the contract agreed with Trafford CYPS, Health Care Trust or Primary Care Trust* .
- The organisation will abide by the requirements set out above for handling any of Trafford CYPS, Health Care Trust or Primary Care Trust* personal data/information disclosed to my organisation during the performance of such contracts or work agreed with them.

Signed: _____

Name of Individual: _____

Position in organisation: _____

Date: _____

* delete as appropriate

APPENDIX 4
MEETING
TYPE/TITLE.....DATE.....LOCATION.....

	Name (pls print)	Job title, Agency representing /Dept if Trafford or Trust employee	Signature to agree to comply with content of Confidentiality Agreement
<p><u>Confidentiality Information Agreement for Multi Agency Meetings</u></p> <p>This document forms part of the 'Trafford Information Sharing and Confidentiality Policy for Staff Working with Children, Young People & Their Families'.</p> <p>This agreement must be signed by all meeting attendees whether agency representatives or employees. It must be completed as part of any meeting held by Trafford CYPS/Trust where information sharing of a sensitive or confidential nature about clients or the organisation will occur.</p> <p>Confidential and sensitive information shall include all confidential records, reports, documents and other information that is collated, acquired and/or presented.</p>			
<p>Your Responsibilities at this Meeting</p> <ul style="list-style-type: none"> • Information Sharing is only permitted where specific consent is obtained from the service user or where an information 			

<p>sharing protocol and/or matrix is in place. Information sharing can occur without consent in certain circumstances i.e. Child Protection Matters (See Trafford CYPS/HCT/PCT Policy on Information Sharing & Confidentiality for clarification).</p>			
<ul style="list-style-type: none"> • When your employment or association with Trafford CYPS/Trust ends, you will not access or disclose any Trafford CYPS/Trust information that you had access to; legal action may result if you do. 			
<ul style="list-style-type: none"> • You will not divulge to any third party any confidential information shared at this meeting. <p>You must ask the chair of the meeting for clarification if there are any items you do not understand before signing this agreement. Your signature acknowledges that you have read and understood this agreement and realize it is a condition of your attendance at this meeting. A copy of this signed agreement will be made available to you at your request.</p>			

Copy as required for the same meeting if more attendees present, ensuring the meeting details are completed and the same for all sheet