Confidentiality & Information Sharing Policy

Arrangements for Review:

Ian Townsend-Blazier is responsible for the implementation of this policy and conducting regular reviews. This policy was adopted in January 2013 and reviewed in:

January 2014
January 2015
January 2016
January 2017
January 2018

Next review date: January 2019
Introduction
This policy relates to provisions under the following Acts:

Human Rights Act 1998: Gives everyone the right to “respect for his private and family life, his home and his correspondence”, unless this is overridden by the ‘public interest’, e.g. for reasons of Child Protection, for the protection of public safety, public order, health or morals or for the rights and freedoms of others.

Data Protection Act 1998: Applies to personal data of living, identifiable individuals, not anonymised data; manual and electronic records. (see our Data Protection Policy)


Rationale
At Children & Families Ltd (C&F) we believe that:

- The safety, wellbeing and protection of children are the paramount considerations in all decisions made about confidentiality and information sharing. The appropriate sharing of information between staff is an essential element in ensuring our service users wellbeing and safety.
- We fulfil our legal duties under the Data Protection Act (see Data Protection policy) and common law duty of confidentiality.
- It is an essential part of our ethos that trust is established between children, staff, and parents/carers.
- Service users and staff need to know the boundaries of confidentiality and information sharing in order to feel safe and comfortable in discussing personal issues and concerns.
- Our attitude to confidentiality and information sharing is open and easily understood and everyone should be able to trust the boundaries that we operate.
- Service users need to know that no one can offer absolute confidentiality e.g. if there are child protection concerns that must be reported.

Definition of Confidentiality
Confidential information can be defined as information of some sensitivity not already in the public domain or not readily available from another public source, and which has been shared in a relationship where the person giving it understood that it would not be shared with others without their express consent.

When speaking confidentially to someone the confider has the belief that the confidant will not discuss the content of the conversation with another. The confider is asking for the content of the conversation to be kept secret. Anyone offering absolute confidentiality to someone else would be offering to keep the content of his or her conversation completely secret and discuss it with no one.

In practice it is not usually possible to offer absolute confidentiality. A balance needs to be struck between ensuring the safety, wellbeing and protection of our service users and staff and ensuring that when it is essential to share personal information, good practice is followed.
This means that in most cases what is on offer is limited confidentiality. Disclosure of the content of a conversation could be discussed with professional colleagues but the confider would not be identified except in certain circumstances.

The general rule is that staff should make clear to service users that there are limits to confidentiality. These limits relate to ensuring the protection of children and sometimes adults. The service user will be informed when a confidence has to be broken for this reason and will be encouraged to do this for themselves whenever this is possible.

Disclosures to staff and volunteers
Staff and volunteers should not promise confidentiality. The safety, wellbeing and protection of the child is the paramount consideration in all decisions made about confidentiality.

Staff are not obliged to break confidentiality except where child protection is or may be an issue, however we believe it is important staff are able to share information about service users with colleagues in a professional and supportive way, on a need to know basis. Staff should discuss any child protection concerns with their line manager or their DCPC (Designated Child Protection Coordinators are listed in the Child Protection Policy). All staff receive basic child protection awareness training and are expected to follow C&F’s Child Protection policy and procedures.

When confidentiality should be broken and procedure for doing this
See the Child Protection Policy and Procedure. Where this does not apply and you are still concerned and unsure of whether the information should be passed on or other action taken you should speak to your line manager.

When a disclosure is being made we must:
- Tell the service user that we cannot guarantee confidentiality if we think that they or someone else may be at risk of harm
- Not interrogate or ask leading questions
- Accurately record what is said using the words of the speaker

The Child Protection Policy and Procedure should be followed at all times.

Keeping confidence
Where confidential information received is clearly not of a child protection nature, there are no valid legal reasons to break confidentiality and no consent to share the information, confidentiality must be maintained. Inappropriate and unjustified sharing of confidential information will be considered a disciplinary matter.

Good practice in information sharing
When in doubt about whether or not to share information, all staff and volunteers should refer to the ‘Seven Golden Rules for Information Sharing’ below and flow chart available at: https://www.education.gov.uk/publications/eOrderingDownload/Info-sharing_poster.pdf

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.

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, that 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.

**Kent & Medway Information Sharing Agreement (KMISA)**
Children & Families Ltd is a signatory to KMISA and its terms are incorporated into this policy under Appendix A. The Designated Officer for information governance under this agreement is the Company Secretary.
# Kent and Medway Information Sharing Agreement v4

## 2014/15

<table>
<thead>
<tr>
<th>Programme</th>
<th>IG Partnership Board</th>
<th>Project</th>
<th>KMISA Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Reference</td>
<td></td>
<td>Status</td>
<td>Approved</td>
</tr>
<tr>
<td>Programme Manager</td>
<td>Charlie Beaumont</td>
<td>Version</td>
<td>4.0</td>
</tr>
<tr>
<td>Author</td>
<td>Day, Alan - ST ICT</td>
<td>Version issue date</td>
<td>18/09/2014</td>
</tr>
</tbody>
</table>
Contents

1. Introduction
2. What is Information Sharing?
3. Terms of Agreement
4. Information Sharing Principles
5. Governance and Administration
   5.1 Kent and Medway IG Partnership Board
   5.2 Designated Officers
   5.3 Standard Operating Procedures
   5.4 Information Security
   5.5 Incident Reporting
   5.6 Concerns and Complaints
   5.7 Government Security Classifications
   5.8 Indemnity
   5.9 Signatories
6. Advice & Guidance
1. **Introduction**

This agreement seeks to improve the way personal information is shared by local public services in Kent and Medway in order to maximise service delivery. Signatories to this agreement enter a supportive community founded on mutual trust.

2. **What is Information Sharing?**

‘Information Sharing’ is the disclosure, exchange or pooling of personal information between organisations acting as Data Controllers in their own right and for their own purposes. This may include routine sharing of datasets used to plan and improve services or ad-hoc disclosures that support or protect individuals. Information may be shared for more than one purpose.

The terms ‘Information Sharing’ and ‘Data Sharing’ refer only to mutual arrangements between Data Controllers where each is using the information for their own purpose(s). These terms do not apply to Data Processing arrangements where a party is acting only under instruction from a Data Controller.

People expect organisations to share their personal information where it helps to provide or improve the services they want. It is part of the way local public services work and should be approached with confidence.

This agreement sets out principles for respecting the privacy and confidentiality of individuals and protecting their personal information whilst ensuring they receive effective and efficient services.

3. **Terms of Agreement**

This agreement may be used by public authorities and public service organisations operating within Kent and Medway, including services in the voluntary and private sector. In doing so, such organisations agree to be bound by its terms and principles.

3.1 In signing this agreement you are confirming that you are authorised to enter into agreements on behalf of your organisation and that your organisation is registered with the Information Commissioner’s Office (ICO) as a Data Controller.

3.2 Parties to this agreement are responsible for the ongoing protection and lifecycle management of personal information received unless otherwise agreed in writing.

3.3 This agreement should not be used to govern disclosure of personal information to a service provider acting solely under the instruction of a Data Controller. The Data Protection Act 1998 defines these as Data Processors. Such arrangements are accountable through contracts or service agreements that include appropriate data protection clauses.

3.4 Only signatories to this agreement are bound by its terms. There is an expectation that parties with whom information is shared should be encouraged to sign in their own right. Information shared with non-signatories is outside of the terms of this agreement.

3.5 Joint Data Controller arrangements may be agreed between signatories on the condition that the parties enter into a separate written agreement that specifies terms and conditions and apportions liabilities.

3.6 Disclosures made under this agreement do not transfer copyright ownership or intellectual property rights unless expressly stated otherwise or appropriately licensed.

---

1. A current list of signatories is available to members on the Kent Connects portal.
3.7 Parties to this agreement must each nominate at least one Designated Officer (DO) to act as that organisation’s point of contact.

3.8 A sending (disclosing) party is responsible for ensuring that outbound personal information is appropriately protected in transit. Responsibility for protection transfers to the recipient organisation once accessed or opened by that organisation or one of its employees, contractors or agents.

4. Information Sharing Principles
Parties to this agreement agree to apply the following principles:

4.1 A person’s health, safety and wellbeing is more important than data protection.

4.2 Information sharing is legitimate where it is used to improve services or positively benefit customers or service users, or where it assists in detection of crime and fraud.

4.3 The way personal information is used and with whom it may be shared should be transparent (e.g. privacy notices or verbal scripts).

4.4 Disclosure of sensitive or confidential information requires a person’s explicit consent unless for a statutory purpose.

4.5 The potential consequences of an individual declining consent should be explained to them (e.g. limitations in the provision or quality of service).

4.6 Registered professionals or practitioners involved in an individual’s direct care and support are encouraged to share information in accordance with their respective professional codes of practice. Such sharing may be subject to the common law duty of confidence.

4.7 Decisions to disclose personal confidential information without a person’s knowledge or consent are considered a matter of professional judgement. Such decisions must be judged at an appropriately senior level and are expected to consider the sensitivity and potential impact on a person’s security and safety.

4.8 Disclosure and sharing of information for research, statistical or business intelligence purposes is expected to comply with the ICO Anonymisation Code of Practice (2012)²

4.9 Disclosure of patient information must be approved by an organisation’s Caldicott Guardian or an appropriate responsible officer.

² Anonymisation: managing data protection risk code of practice (ICO 2012)
5. Governance and administration
This is an agreement between co-signatories. Content is reviewed and co-ordinated by the Information Governance Partnership Board (IGPB) which reports to the Joint Chief Executives Board. The terms of reference for IGPB can be found on the Kent Connects portal.

5.1 The IG Partnership Board (IGPB)
The IGPB is responsible for revisions to this agreement and meets at least quarterly. Agenda and minutes are published on the Kent Connects portal to which all signatories have access.

Representatives of signatory organisations are invited to attend meetings and encouraged to participate in discussions.

5.2 Designated Officers (DOs)
Each organisation must nominate at least one Designated Officer (DO). Designated Officers must be of sufficient standing to perform the following roles within their organisation:

(a) Acting as the main point of contact for:
   (i) Additions to, and amendment of Standard Operating Procedures;
   (ii) Changes to this agreement;
   (iii) Communications related to information sharing issues; and
   (iv) Information Assurance and audit requests.
(b) Co-ordinating, approving and maintaining records of Standard Operating Procedures for individual information sharing arrangements.
(c) Reviewing Standard Operating Procedures.
(d) Where applicable, consulting their Caldicott Guardian before sharing patient information.
(e) Appointing a deputy during periods of absence and delegating responsibilities
(f) Assisting co-signatories in complying with Subject Access and Freedom of Information requests and in the handling of complaints.
(g) Handling adverse events and incidents relating to information sharing arrangements.

5.3 Standard Operating Procedures
Standard Operating Procedures (SOPs) articulate specific information sharing arrangements made between signatories to this agreement. These may use or customise standard templates where available or be individually drafted as a custom document. Wherever possible these should use standardised formats.

SOPs must be recorded and published to partners through the Kent Connects IG portal, and must include at least the following information.
• Statement confirming that participating parties are signatories to this agreement and bound by its terms.

• Commencement date

• Parties and their contact details

• Purpose / Reason

• Description of information to be shared

• Means of transferring the personal information

• Approvals (where applicable, e.g. Caldicott)

• Retention periods and secure disposal arrangements

• SOP review date

5.4 Information Security

Parties are responsible for satisfying themselves that organisations to whom they disclose information have in place appropriate technical and organisational information security measures in place, including:

(a) Data protection policies and management processes.

(b) Retention, archive, storage and disposal policies and processes.

(c) Incident reporting procedures.

(d) Controls to minimise the risk of loss or breach.

Parties may wish to consider the following standards when assessing risk:

• Current PSN Code of Compliance Certificate

• ISO27001 (Information Security) certification or audited ‘Statement of Applicability’.

• NHS IG Toolkit rated as satisfactory (Health related).

5.5 Incident reporting

In the event of breach or loss of personal information received under this agreement, the organisation that provided it should be informed as soon as possible.

5.6 Concerns and complaints

Concerns or complaints relating to information sharing arrangements made under agreement should be raised with the relevant DO who may escalate as appropriate within their organisation.

Where an issue cannot be resolved between the relevant parties, the IGPB may be consulted for guidance.
5.7 **Government Security Classifications**
Organisations complying with Public Service Network (PSN) Agency terms and conditions should classify and where appropriate mark documents and files in accordance with HMG Government Security Classifications April 2014\(^3\) (as amended from time to time).

5.8 **Indemnity**

If an individual (Data Subject) suffers loss or damage as a result of the misuse, inaccuracy or misinterpretation of information disclosed under this agreement and brings a consequential action or demand, the parties to that disclosure indemnify each other against legal liabilities so arising.

Provided that this indemnity shall not apply:

- Where the liability arises from the supply of incomplete or incorrect information, unless the person or authority claiming the benefit of this indemnity establishes that the error did not result from any wilful wrongdoing or negligence on its part;

- Unless the party claiming the benefit of the indemnity has notified the party against whom it intends to invoke the indemnity within 56 days of any third party action claim or demand and thereafter the parties shall consult as to how the party against whom the claim has been made should proceed in respect of such claim;

- To the party seeking to invoke the indemnity if it has made or makes any admission, which may be prejudicial to the defence of the action, claim or demand.

5.9 **Signatories**

The statement at the end of this agreement must be signed by an appropriately senior officer or manager on behalf of their organisation. This confirms their organisation's compliance with relevant legislation and acceptance of the terms and conditions of this agreement.

(a) Following changes to this agreement, each organisation will be asked to sign a fresh declaration.

The IGPB will store completed statements and co-ordinate proposed changes to this agreement for Joint Kent Chief Executives' approval.

6. **Advice and Guidance**

Parties to this agreement have access to IGPB pages of the Kent Connects portal. The portal can be found at the following link.

http://www.kentconnects.gov.uk/infosharing

The portal provides useful resources, advice and guidance on using this agree

\(^3\) Government Security Classifications April 2014