

Derbyshire County Council

Adult Care Department

INFORMATION SHARING AND SECURITY AGREEMENT

|  |
| --- |
| **Glossary of Terms** |
| Adult Care | The department within Derbyshire County Council with management responsibility for adult social care |
| Agreement  | This Information and Security Agreement |
| Candour | Any person harmed by the provision of a health or social care, service is informed of the fact and an appropriate remedy offered, regardless of whether a complaint has been made or a question asked about it. |
| Client | A person receiving a health and/or social care service who is the subject of shared information. |
| Confidential information | Any information which has been designated as confidential by either Party in writing or that ought to be considered as confidential (however it is conveyed or on whatever media it is stored) including information which relates to the business, affairs, properties, assets, trading practices, goods or services, developments, trade secrets, Intellectual Property Rights, know-how, personnel, customers and suppliers of either Party, all personal information and sensitive personal information and the commercially sensitive information. |
| Data  | Information which (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,(b) is recorded with the intention that it should be processed by means of such equipment,(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d). |
| Data Controller  | The party who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. |
| Data Processor | In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. |
| DPA | the Data Protection Act 1998 and all applicable laws and regulations relating to processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner |
| Data Protection Officer | The named person who is responsible for Data protection for the organisation. |
| FOIA | The Freedom of Information Act 2000 and any subordinate legislation made under this Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government Department in relation to such legislation |
| Health and Social Care Act 2008 | Legislation, including requirements for registration and inspection by a regulator, of health and adult social care services with the aim of ensuring safety and quality of care for clients. |
| MCA | The Mental Capacity Act 2005 came into force in England and Wales in 2007 and aims to empower and protect people who may not be able to make some decisions for themselves; enables people to plan ahead in case they are unable to make important decisions in the future; provides a framework for assessment and decision making for specific decisions if it appears that a person may not have the capacity to do this. |
| Personal Data/Information  | Data that relates to a living person who can be identified:(a) from those data, or(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the person and any indication of the intentions of the data controller or any other person in respect of the person. |
| Privacy Notice | The oral or written statement that people are given when information about them is collected. Also referred to as a Fair Processing notice |
| SAB | Safeguarding Adults Board is a multi-agency forum to provide strategic leadership in preventing, detecting and safeguarding adults from abusive behaviour. SABs are a requirement of the Care Act 2014. |
| SAR | Under the Data Protection Act 1998, people can make a Subject Access Request to see the information about themselves that is held on computer and in some paper records by writing to the person or organisation they believes holds it, accompanied by the appropriate fee. |
| Safeguarding of Vulnerable Adults | The process of protecting adults with care and support needs who may be in vulnerable circumstances and at risk of abuse or neglect by others. |
| Sensitive Personal Data/Information | Personal Data consisting of information as to (a) the racial or ethnic origin of the data subject,(b) his political opinions,(c ) his religious beliefs or other beliefs of a similar nature,(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),(e) his physical or mental health or condition,(f) his sexual life,(g) the commission or alleged commission by him of any offence, or(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings. |
| Service | The care and / or support provision contracted by the Council and provided by the Provider |
| Third Party | in relation to personal data, means any person other than –(a) the data subject,(b) the data controller, or(c) any data processor or other person authorised to process data for the data controller or processor. |

Parties

A) DERBYSHIRE COUNTY COUNCIL (Council) and

B) [Provider] (Provider)

**1 Introduction**

1.1 Local organisations are increasingly working together. To work together effectively, organisations need to be able to share information about the services they provide and the people they provide these services to. The motto for better care services should be: “To care appropriately, you must share appropriately”. Organisations involved in providing services to the public have a legal responsibility to ensure that their use of personal information is lawful, properly controlled and that a person’s rights are respected.

1.2 This document is an Information Sharing Agreement established to secure the transfer of personal information between the Adult Care department and private, independent and voluntary sectors so that people receive the highest quality joined-up care possible. This agreement does not give carte blanche licence for the wholesale sharing of information. Information sharing must take place for justifiable legal purposes within the constraints of the law, relevant guidance, and service specific requirements and should be underpinned by an ethos of informed consent and client confidentiality.

1.3 The principal legislation concerning the protection and use of personal information is listed below and further explained in:

• [Human Rights Act 1998 (article 8)](http://www.legislation.gov.uk/ukpga/1998/42/schedule/1/part/I/chapter/7)

• [The Freedom of Information Act 2000](https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/)

• [Data Protection Act 1998](https://ico.org.uk/for-organisations/guide-to-data-protection/)

• [The Common Law Duty of Confidence](http://webarchive.nationalarchives.gov.uk/%2B/www.dh.gov.uk/en/publicationsandstatistics/publications/publicationspolicyandguidance/browsable/DH_5803173)

• [Computer Misuse Act](http://www.legislation.gov.uk/ukpga/1990/18/contents) 1990

• [Civil Contingencies Act 2004](http://www.legislation.gov.uk/ukpga/2004/36/contents)

• [The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014](http://www.legislation.gov.uk/ukdsi/2014/9780111117613/contents)

• [Care Act 2014](https://www.gov.uk/government/publications/care-act-2014-part-1-factsheets)

Other legislation may be relevant when sharing specific information.

 Guidance to be followed as listed:

• [Information: To share or not to share? The Information Governance Review March 2013](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf)

• [Caldicott Principles](https://www.wcppe.org.uk/sites/default/files/file/NES/CaldicottPrinciples-DataProtectionAct.pdf) as defined within the above guidance

* [ICO Data Sharing Code of Practice May 2011](https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf)

**2 Application**

This agreement applies to all providers who hold one of the Adult Care contracts listed below:

* Terms and Conditions of Accommodation in the Independent Sector with effect from 10th April 2006 Care Homes which provide personal care and nursing care
* Terms and Conditions, Home Care Spot Contract Arrangements v2 (Final with correction 25 February 2015)
* Terms and Conditions of Accommodation in the Independent Sector with effect from 1st April 2013 Care Homes which provide specialist residential support and Care Homes which provide specialist nursing support
* Terms and Conditions For Respite Day Care for Older People in the Independent Sector with effect from 1 April 2000
* Terms and Conditions for Spot Purchased Day Services with effect from 1st April 2012
* Terms and Conditions for Spot Purchased Day Services with effect from 1st April 2016
* Adult Care Contract Template Agreement Updated October 2015
* Adult Care Contract Template Agreement Final 310112

**3 Scope and limitations**

This agreement covers all information as defined in the Data Protection Act 1998 (DPA), including personal information and sensitive personal information, but does not include non-personal information and anonymised information.

Information may be held as either manual or electronic records, or records held by means of audio and/or visual technology.

**3.1 Confidential information**

“Confidential Information” means any information which has been designated as confidential by either Party in writing or that ought to be considered as confidential (however it is conveyed or on whatever media it is stored) including information which relates to the business, affairs, properties, assets, trading practices, goods or services, developments, trade secrets, Intellectual Property Rights, know-how, personnel, customers and suppliers of either Party, all personal information and sensitive personal information and the commercially sensitive information.

**3.2** **Information given in confidence**

Health and social care staff may receive important information about a client from a third party, such as a partner, family member, friend or carer. This information can often be relevant to a client’s care, but may also be highly sensitive and may have been given in confidence. In terms of data from a third party, there is a need to consider what information can be disclosed to the client, without breaching any obligation of confidentiality owed to the third party. In some instances, it may be possible to separate the identity of the third party giving evidence from the information they give. However, it is possible that, the client can identify the source even with the identity withheld. It is therefore important that information from a third party is not put on record unless the provider of the information understands that the client may become aware of this information and its source. Information can be withheld if a professional believes there is a risk of harm to the third party if the information is shared.

It should be explained to the third party that either at the time or sometime in the future the client may be able to identify the source of the information even if their identity is withheld. This should be undertaken BEFORE the third party has disclosed the information they wish to share. This means the third party has the following options:

• The third party consents to the person finding out their identity.

• The third party wants the information recorded and understands there is a

risk of them being identified as the source of the information even if it is not readily identified to the client.

• The third party decides not to share the information

• The third party may not be able to withdraw information about the client if a court order has been issued or on public interest grounds such as if the client poses a significant risk to others or is at significant risk of harm.

**3.3 Personal Data**

The term ‘personal data’ refers to any information about a person who can be personally identified from that information. The term is further defined in the DPA as:

• Data relating to a living person who can be identified from those data;

or

• Any other information which is in the possession of, or is likely to come into the possession of the data controller (person or organisation collecting that information).

Personal information may include:

• Name

• Address, Postcode, Telephone number, Mobile phone number

• Age

• Gender

• Nationality

• Primary language

• Registered disability / mobility

• Support required / current known vulnerability

• Medical needs

• GP name and practice contact details

• Care or service providers

• Contact details of family members or significant others

• Information stored on Person Held Records

A person may consider certain information about themselves to be particularly private and may request other information be kept especially confidential e.g. any use of a pseudonym where their true identity needs to be withheld to protect them.

**3.4 Sensitive Personal Data**

The DPA also defines certain classes of personal information as ‘sensitive data' where additional conditions must be met for that information to be used and disclosed lawfully. This includes:

* the racial or ethnic origin of the data subject,
* political opinions,
* religious beliefs or other beliefs of a similar nature,
* whether the data subject is a member of a trade union (within the meaning of

the Trade Union and Labour Relations (Consolidation) Act 1992),

* physical or mental health or condition,
* sexual life,
* the commission or alleged commission by the data subject of any offence, or

any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

**3.5 Non-Personal information**

From the definition above, it follows that information or a combination of information, that does not relate to and identify a person, is not personal information and therefore not subject to the DPA. Whilst not the focus of this Agreement, parties should not assume the non-personal information is not sensitive and can be freely shared. This may not be the case and the Party from whom the information originated from should be contacted before any further sharing takes place.

**3.6 Anonymised Information**

This is information which may include some personal information but from which no specific person can be identified. Data protection law does not apply to information rendered anonymous in such a way that the person is no longer identifiable and cannot be re-identified. This does not cover information that is transferred in an anonymous fashion but the receiving organisation is made of aware of the identity of the client or places the information on a personal record. This is not anonymous, and the DPA would apply as the information would be classed as personal.

**4 Conditions**

Information should be treated as confidential unless the exceptions below are met, the requirements of the DPA are met, or consent has been given.

**4.1 Confidentiality**

 Confidentiality is an important principle that enables people to feel safe in sharing their concerns and to ask for help. Each party shall treat all information as confidential and will safeguard it accordingly and shall not disclose it to any other person except:

• where disclosure is otherwise expressly permitted by the provisions of the Agreement;

• in respect of Safeguarding issues. It is inappropriate for parties to give assurances of absolute confidentiality in cases where there are concerns about abuse, particularly in those situations when other adults may be at risk.

• which must be disclosed pursuant to a statutory, legal or parliamentary obligation placed upon the Party making the disclosure, including any requirements for disclosure under the FOIA regulations or pursuant to any other Law;

* 1. **Disclosure**

In order to disclose personal information at least one condition in schedule two of the DPA must be met. In order to disclose sensitive personal information at least one condition in both schedules two and three of the DPA must be met.

* 1. **When consent is given:**

• Informed explicit consent should be obtained from clients wherever possible. When using sensitive information, explicit consent must be obtained subject to any existing exemptions. In such cases the client’s consent must be clear and cover items such as the specific details of processing, the information to be processed and the purpose for processing.

* Where consent cannot be obtained from the client due to a lack of capacity according to sections 2 and 3 of the MCA, consent should be obtained from a person lawfully acting on their behalf. Where there is no legally appointed person, an assessment, and if necessary following this, a best interest decision should be taken in relation to the information that is proposed to be shared.
* Implied consent - For clients who reside in care homes, relevant clinical and social care information can be shared with a registered and regulated professional at the care home, unless the person objects. This can be done on the basis of implied consent. For clients who reside in their own home with a package of care, relevant clinical and social care information can be shared with the registered and regulated professionals providing that care, unless the client objects. This can also be done on the basis of implied consent.
* However, in residential care homes and for clients living at home, a considerable proportion of care is provided by staff that are not regulated by statute. It cannot be assumed that implied consent has been given for confidential personal information to be passed to these unregistered and unregulated staff. As such it is essential that informed explicit consent is obtained.

**4.4 Privacy Notices**

 Parties should ensure they have appropriate privacy notices, sometimes known as fair processing notices, in place to ensure that clients know which organisations are sharing their personal information and what it is being used for, and that this notice is being appropriately communicated.

**4.5 Before agreeing to share information parties should consider:**

What is the sharing meant to achieve?

* What information needs to be shared?
* Who requires access to the shared personal information?
* When should it be shared?
* How should it be shared?
* How can we check if sharing is achieving its objectives?
* What risk does the information sharing pose?
* Could the objectives be achieved without sharing the information or by anonymising it?

**4.6 Routine sharing**

This will generally involve routine sharing of information between parties for an agreed purpose. It could also involve a group of organisations making an agreement to ‘pool’ their data for specific purposes. A Data Sharing Checklist can be found in the Appendices along with a sample request and decision recording template.

**4.7 One-off sharing**

Parties may also decide, or be asked, to share information in situations which are not covered by any routine agreement. In some cases this may involve a decision about sharing being made in conditions of real urgency, for example in an emergency situation. A Data Sharing Checklist can be found in the Appendices along with a sample request and decision recording template.

**4.8 Safeguarding Board requests**

A Safeguarding Adults Board (SAB) may request the parties to supply information to it or to another person. In accordance with the Care Act 2014 the information must be provided to the SAB if:

• the request is made in order to enable or assist the SAB to do its job;

• the information requested relates to the person to whom the request is made and their functions or activities;

• the information requested has already been supplied to another organisation subject to an SAB request for information.

**4.9 FOIA/DPA requests**

The DPA gives people certain rights over their personal information including the right to access information held about them, know how their information is being used, and object to the way their information is being used. Therefore, parties should make it expressly clear how client information may be shared, with whom, and for what purpose.

People can request access to their information in the form of a Subject Access Request. This should be dealt with in line with organisational policy and procedures. If a request is made and third party information is held, a decision should be made about whether to include the information and its source. In some instances the source should be asked about whether the information should be included.

In addition, public bodies involved in information sharing are subject to freedom of information law. People should be made aware that information they provide may be shared with and held by an organisation subject to FOIA. Whilst there is an exemption with the FOIA for the personal data of third parties, people should be advised that their information could fall within the scope of a request.

**4.10 Duty of Candour**

The aim of Regulation 20 of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 Duty of Candour is to ensure that providers are open and transparent with people who use services and other ‘relevant persons’ (people acting lawfully on their behalf) in relation to care and treatment.

It also sets out some specific requirements that providers must follow when things go wrong with care and treatment, including informing people about the incident, providing reasonable support, providing truthful information and an apology.

Parties should therefore be aware of the possibility that information provided by them to another party could be shared under this requirement.

**5 Process considerations**

**5.1 Consent and transparency**

*•* Where parties have a statutory obligation to disclose personal information then the consent of the client is not required; but the client should be informed that such an obligation exists.

• If a Party decides not to disclose some or all of the personal information, the requesting organisation must be informed. For example a Party relying on a lawful exemption from disclosure or on the inability to obtain consent from the client.

• Consent has to be signified by some communication between the Party and the client. If the client does not respond this cannot be assumed as implied consent.

• If consent is used as a form of justification for disclosure, the client must have the right to withdraw consent at any time.

• Parties must be aware that a client may withdraw consent to processing (i.e. Section 10 DPA) of their personal information. In this case processing can only continue where an applicable Data Protection Act Schedule 2, and if relevant Schedule 3, purpose applies.

• Where parties rely on consent as the condition for processing personal information then withdrawal means that the condition for processing will no longer apply. Withdrawal of consent should be communicated to the other Party and processing cease as soon as possible.

* In certain limited circumstances the DPA provides for personal information, even sensitive information, to be shared without the person’s knowledge for:
1. The prevention or detection of crime
2. The apprehension or prosecution of off enders
3. The assessment or collection of tax or duty.

**5.3 Storage and Security**

• Each Party is responsible for ensuring that their organisational and security measures protect the lawful use of information shared under this Agreement.

• Each Party will ensure a reasonable level of security for supplied information, personal or non-personal, and process the information accordingly.

* To determine what security measures are appropriate in any given case, parties must consider the type of information and the harm that would arise from a breach of security.
* In particular, each party must make sure they have procedures in place to do everything reasonable to:
1. prevent unauthorised or unlawful processing of personal information
2. make accidental compromise, loss, destruction or damage unlikely during storage, handling, use, processing transmission or transport;
3. deter deliberate compromise or opportunist attack;
4. dispose of or destroy the information in a way that makes reconstruction unlikely;
5. promote discretion to avoid unauthorised access;
6. provide clear guidance regarding confidentiality including use of social and media and electronic communication;
* In particular, they must consider:
1. physical and electronic security measures available – see checklists in the Appendices
2. the reliability of employees having access to the information
* Minimum security precautions include that clients should be referred to by the Personal Identification Number (PIN) used by the Council Adult Care department in correspondence and password protection used for attachments where information is sent electronically.
* It is assumed that each Party has achieved or will be working towards ISO 27001, the International Standard for Information Security Management, compliance or a similar level of compatible security. It is accepted that not all Parties will have security classification in place.

**5.4 Quality and compatibility**

* Information needs to be of a standard fit for the purpose for which it is being used and/or shared. Without this any decision made on the information may be flawed and inappropriate actions may result.
* Parties are expected to ensure that the personal information and sensitive personal information that is held is processed in accordance with DPA principles: this includes ensuring that the information is accurate, complete and up-to-date and is not kept any longer than is necessary.
* Where parties share information under this Agreement it is expected that they will either have an Information Quality Strategy and the supporting processes and procedures in place or be formally working towards this.
* Information identified as inaccurate, out of date or inadequate for the purpose should be notified to the Data Controller of the originating party, who will be responsible for correcting the information and notifying all other recipients who must make sure their own records are corrected.

**5.7 Proportionality**

* Information shared under this Agreement will be adequate to enable the effective discharge of service objectives.
* Where information received by any party is insufficient to achieve the agreed purpose, clarification will be sought before the information is acted upon. Parties receiving such queries will act promptly to resolve them.
* Information received which is excessive in relation to the purpose of the Service will not be retained by the receiving Party.

**5.8 Need to know**

This agreement does not give licence for unrestricted access to information the other Party may hold. Staff should only be given access to personal information for a justifiable need to know purpose where there is a legal right, in order for them to perform their duties in connection with the services they are there to deliver.

**5.9 Usage**

* All shared information, personal or otherwise, must only be used for the purpose(s) specified at the time of disclosure(s) unless obliged under statute or regulation, or under the instructions of a court or as agreed elsewhere.
* Restrictions may also apply to any further use of non-personal information, such as commercial sensitivity and this should be considered when considering secondary use for non-personal information. If in doubt the information’s original owner should be consulted.
* Additional statutory restrictions apply to the disclosure of certain information for example Criminal Records, HIV and AIDS, Assisted Conception and Abortion, Child Protection
* Each Party should ensure that their contracts with external service providers include a condition that they abide by their rules and policies in relation to the protection and use of confidential information.

**5.10 Complaints/breaches**

* If there is a security breach or incident involving a risk or breach in which information received from the other party under this Agreement is or could be compromised, the originator will be notified at the earliest opportunity who must follow organisational policy and procedures relating to such a matter.
* All complaints or data breaches relative to this Agreement will be notified to the designated Data Protection Officer of the relevant party in accordance with their respective policy and procedures.
* Both parties are responsible for having in place effective procedures to address complaints relating to the disclosure of information and breaches in security or confidentiality, and information about these procedures should be made available to service users.

**5.11 Retention and destruction**

* Parties should have a written policy for retention and disposal of information that meets their legal obligations. Details of the Councils Records Retention Policy and Schedules can be found [here](http://www.derbyshire.gov.uk/working_for_us/data/how_to_dispose_of_confidential_information_safely/default.asp).
* Records will be retained for the periods of time required by Law and securely destroy them thereafter.
* Information no longer required for the agreed purpose will be disposed of in a manner consistent with the Parties’ security obligations.
* Where a Party is unable to retain records, for example in case of a business failure, the Council Data Protection Officer will be notified and make arrangements for appropriate storage and/ or destruction.

**5.12 Indemnity and liability**

* Each Party will keep the other party fully indemnified against any and all costs, expenses and claims arising out of any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending party or its sub-contractors, employees, agents or any other person within the control of the offending party of any personal information obtained in connection with this agreement.
* Parties or any third party processor to the applicable party will accept total liability for the breach if legal proceedings are served in relation to the breach.

**5.13 Monitoring and audit**

* Parties accept responsibility for undertaking periodic internal audits to check compliance with this agreement and to act upon any findings or areas for improvement.
* As part of its contract management and monitoring processes, Derbyshire County Council Adult Care will make checks to confirm compliance with this agreement.

**5.14 Staffing**

* Both parties are responsible for ensuring that organisational measures are in place to protect the security and integrity of personal information and that their staff are properly trained to understand their responsibilities and comply with the law when using and sharing personal information.
* Each Party to the Agreement is responsible for ensuring every member of its staff is aware and complies with the obligation to protect confidentiality and a duty to disclose information only to those who have a right to see it.
* All staff will be made aware that disclosure of personal information, which cannot be justified on legal or statutory grounds, whether inadvertently or intentionally, could be subject to disciplinary action.

**6 Review of Agreement**

* The Agreement will last for the duration of any contract held between the Council and the other Party.
* It will be reviewed in line with any review timescales for the overall contract documentation, or as changes in legislation dictate.
* Either party can request a review where a joint discussion or decision in relation to this agreement is necessary to address local service needs or problems.

**7 Signatures**

I have read, understood, and agree that the agency I represent will abide by the terms and conditions of this Agreement.

**For the Council:**

Signature:

Name:

Job Title:

Date:

**For the Provider:**

Signature:

Name:

Job Title:

Date:

**7 Appendices**

**Data Protection Act Flowchart**



**Checklists**









