# Data Protection and Disclosure of Information

## Policy Statement

At Culmside Support LLP we believe

- Records that are kept should be relevant, accurate and up to date
- People should have access to their records and an opportunity to be involved in maintaining them
- Individual and service records should be kept in a secure way, kept up to date, in good order and are written, maintained and used in accordance with Data Protection Act 2018 which implements the EU's General Data Protection Regulation (GDPR) and other statutory requirements.

## Aim of the Policy

This policy is intended to set out the values, principles and policies underpinning this service's approach to record keeping, data protection and access to records. The policy sets out the actions the management of the service and the staff employed by the service will undertake to meet the regulations and standards affecting care home management and safeguarding of information.

## Data Protection

This policy has been written to ensure that the processing of Personal Data in connection with employees and people who are supported by Culmside Support LLP will comply with the UK Data Protection Act 2018, which implements within the UK the requirements of the EC Data Protection Directive (EC/95/46) and GDPR.

The basic requirement is that the processing, both automated and manual, will comply with the following data protection principles which require that personal data shall:

- Be processed fairly and lawfully
- Be obtained only for specified and lawful purposes, and not be processed in any incompatible manner
- Be adequate, relevant and not excessive
- Be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- Not be kept longer than necessary
- Shall be processed in accordance with the rights of Data Subjects
- Be protected by appropriate security measures
- Not be transferred outside the EEA unless adequate level of data protection exist

The data user/controller for this policy is: **Claire Lewis**
Claire Lewis is responsible for overseeing compliance with this policy and should be notified in the event that a Data Protection breach is suspected

## Rights of Access to information

Culmside Support LLP believes that access to information and security and privacy of data is an absolute right of every person who is supported by or works at Culmside Support LLP. We believe each person is entitled to see a copy of all personal information held about them and raise queries about the information if it is not factual or accurate. We believe people have the right to correct any omission or error within that information, where it is not accurate.

All requests for a copy of personal data should be made to Claire Lewis who is the Data Controller and Guardian for the organisation. In her absence Matt Lewis is to be contacted.

An authorised representative may be allowed to view the data provided the data controller is satisfied that permission has been given i.e. signature on FORM CSLLPSAR14 and proof of identity seen.

The data controller will arrange access and support to go through the information if needed. Viewing of some documents will be in the presence of the management. This is for security reasons so that no material can be removed or destroyed
Where people request a copy of information the organisation will respond to the request within twelve working days. If a request for a copy of data is made a fee may be charged to cover administration costs. Where people want a copy of data they should complete Form CSLLPSAR14 (See Appendix A)

**Data Accuracy Procedure**

We commit to ensuring that we comply with the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17 that we will "maintain securely an accurate, complete and contemporaneous record in respect of each service user, including a record of the care and treatment provided to the service user and of decisions taken in relation to the care and treatment provided"

We ensure accuracy in our data in both hardcopy and digital records by making sure all data has the following characteristics:

- Authentic – i.e. the data is what is claims to be, has been created or sent by the person who said that they created or sent it, and that this was done at the time claimed
- Reliable – i.e. the data is complete, accurate, has been created close to the time of the activity it records, and has been created by individuals with direct knowledge of the event it records
- Integrity – i.e. the data is complete and unaltered, it is also protected from being changed or altered by unauthorised persons, any alterations are clearly marked and the person who made them can be identified
- Useable – i.e. the data can be located when it is required for use and its context is clear in a contemporaneous record

*Dispute over accuracy of record*

When a person is not happy with the information or data that has been collected we will try to resolve any disagreement between the home and the person. If the matter cannot be resolved, the following procedures are to be followed:

- People who are supported by Culmside Support LLP, or someone acting on their behalf are requested to use the organisations formal complaints procedure.
- Employees are requested to use the organisations formal grievance procedure.

In all cases we will respond to a request for rectification within one month. Should the request be complex this may be extended to two months, however, we will inform the individual in writing of the extension and the reasons why it is required within one month.

To request for their records to be rectified service users or staff should contact us with the request for rectification either verbally or in writing. If the rectification is due to the record being incomplete, then the individual should also provide the supplementary information to update the record.

While we are assessing the request to rectify records we will restrict processing of the data in question. This will be done in line with our Right to Restrict Processing Procedure as outlined in our Record Keeping Policy.

In the instance where the rectification request is refused, the reason will be explained in full and in writing within one month of the original request having been received.

All individuals who have their rectification request refused will be informed of their legal rights to complain to the ICO and to seek a judicial remedy

All staff will be informed of this policy in the staff handbook.

All service users, or their legal representative, will be informed of this policy, as well as their other rights as regards their personal data, when they sign initial contracts with us.

In order to process your request for rectification, you might be asked to provide identifying documents so that we can authenticate that it is appropriate for you to update your data.

**Retention of Records**

*Employment Records*

Employment records covered by this policy shall be retained, after the actual date of employee leaving for 7 years, after that period the records will be destroyed. Employment records contain any information legitimately required for the purposes of:

- Statutory employment records
- Operational management and administration

This might include information found on the list below (the list is not exhaustive)

- Applications for vacancies and CV's
- Interview records
- References
- Medical reports
- Offers of employment
- Statutory statements of terms and conditions
- Disciplinary and grievance records
- Performance appraisals and similar reviews
- Notes of informal meetings and interviews
- Allowances and expenses
- Training details
- Salary, additional payments and bonuses etc
- Work permits
- Related correspondence
- Attendance record

What may not be included is information, data or other material that cannot legitimately be shown to be related directly or indirectly to your employment.

*People who are supported by Culmside Support LLP*
Records covered by this policy shall be retained for 20 years after the actual date of the person leaving Culmside Support LLP, after that period the records will be destroyed. The records we keep will contain any information legitimately required for the purposes of:

- Statutory records required by legislation, regulations or at the request of the registration authority
- Operational management and administration that will enable the home to give high quality care

This might include the following:

- Culmside Support LLP Agreement
- Admission Record
- Assessment Details
- Support Plans
- Property Register
- Financial Accounts
- Medical Records (depending on circumstances)
- Risk assessment forms associated with the Person
- Self Medication Assessment

These are examples only and there will be other legitimate entries that may be included.

What will not be included is information, data or other material that cannot legitimately be shown to be related directly or indirectly to affording the person high quality and dignified care.

*Other records*
All other records are kept in line with CQC requirements, other legislation or policy requirements.

The information is kept in a locked fire proof cabinet that only the management of Culmside Support LLP can access. Where the organisation no longer operates the appropriate people or people acting on their behalf will be informed of the storage point of the information and rights of access.

**Record Retention Schedule**
A retention schedule of all records is kept on file electronically and reviewed every 12 months.

**Record Review**
To ensure accuracy of personal data all records will be reviewed every 12 months. Claire Lewis is responsible for carrying out the review. A note will be put on the file of the individual that an annual review of the information has taken place.

Employees and people who live or are supported by Culmside Support LLP are asked to inform Claire Lewis of any changes in their circumstances that could affect the accuracy of the information.

**Security and storage of confidential information**
*Computer/Tablets/Mobile phones*
Information held on any electronic device is password controlled. Any information transferred off the computer is stored on an encrypted/password protected device.

All information held on computer relating to people who are supported by Culmside Support LLP or employee's is backed-up every month. This information is password protected and stored in a secure location away from the office. This is done in case of disaster.

No new computer or computer software can by used without the permission of the Manager (data protection controller).

All electronic devices are set to automatically update.

*Written*
Any confidential written records that are kept involving staff or people who are supported by Culmside Support LLP will be kept in locked cabinet in the office. The Manager and Senior Support Officer are the only staff allowed access to this information they must ensure the documents will not be taken out of the main office or left open for other members of staff or visitors to view.

Working documents used for the care and support of an individual will be kept discreetly and wherever possible the person will be encouraged to manage the storage and sharing of information about themselves. Qualified staff will have access and trainees will only have access under supervision of a qualified staff member.

**Portable devices**
We recognise that information held on portable devices is at increased risk. Portable devices include memory sticks, CDs, DVDs, mobile phones etc. All portable devices have been documented on the IAR, and all relevant staff have received guidelines on safe usage and have signed a Portable Device Assignment Form. Due to the increased risk of viruses and the risk of losing data, the following procedures are followed:

- Only portable devices issued by us may be used
- Portable devices such as memory sticks, CDs, etc. must not be used on personal computers
- All portable devices are security marked with a company stick
- Password protected screensavers are installed on laptops
- Anti-virus software is in use and is regularly updated.
- Regular backups are taken of the data stored on portable devices;
- All portable devices are protected by either a PIN and/or biometrics (finger print)

**Induction/ Probation**
Staff will be given restricted access to sensitive information about the people who live at Culmside Support LLP for the first 3 months. Following a successful trial period essential access shall be given unless there are any justified restrictions applied by the person, their family or Care Manager. Any restrictions will be agreed with the Manager of Culmside Support LLP.

**Removal of data from the premises**
***Under no circumstance must any record of a person using the service or employee be taken off the premises without the permission of the Manager, or in his/her absence one of the partners.***
If a member of staff breaches the policy it will be dealt with under the disciplinary procedure. With the exception of data held on individual business mobile phones which should be locked using biometrics and PIN and remain in the possession of the individual the phone has been assigned to.

**Consent**

If Culmside Support LLP are required to obtain consent, we will ensure that the following requirements are met;

- The consent is freely given
- The person giving consent understands fully to the best of their ability, what they are consenting to
- There must be a positive indication of consent (opt-in as opposed to opt-out)
- The person giving consent must be able to withdraw their consent at any time
- Consent should be documented so that it may be referred to in the future, if necessary

**Sharing Information**
Where we have a legal duty to do so Culmside Support LLP will share information with partner agencies, for example health professionals, the police, care manager, the commissioner or CQC officer. This will occur in regard of staff and people who are supported by Culmside Support LLP. The data controller (Claire Lewis) will ensure the organisation the information is being shared with, has a protocol for secure information storage prior to sharing the information. If she is not satisfied this is adequate the information will not be shared.

All information verbal and written will only be shared using a password protection system, in order to validate the authorisation of the person to receive the information.

**Disposal of Information**
When documents are no longer required, they will be shredded and disposed of securely and appropriately. People may be required to witness and sign to say the information was cross shredded and disposed of suitably.

Where a computer hard drive is disposed of, all items on the hard drive will be deleted and the hard drive wiped by an approved data service and the hard drive disposed of securely and appropriately.

**Responsibilities**
*Staff* are responsible for the following aspects of this Policy

- Ensure that all written information of a confidential nature are stored in a secure manner in a locked filing cabinet and only accessed by staff who need and have a right to access them.
- Ensure that all files or written information of a personal nature are not left out where they can be read by unauthorised staff or others.
- Wherever practical or reasonable fill in all records and notes in the presence of, and with the co-operation of, the individual concerned.
- Ensure that all care records and notes, including support plans & daily records, are signed and dated.
- Ensure all information is factual, descriptive, accurate and respectful.
- Check regularly on the accuracy of data being entered into computers.
- Always use secure passwords to access the computer system and not abuse them by passing them on to third parties.
- Always check the identity of any person requesting information about an individual and seek guidance if in doubt of their identity or reason for needing the information.
- Inform the manager of any changes that may affect the accuracy of the information stored about you.
- Use logout facilities to ensure that personal data is not left on screen when not in use.
- Only share information on a NEED TO KNOW basis.

- Participate in training relating to this policy to ensure an up to date knowledge of legislation and current practice
- If it is necessary to transfer personal data to or from a person's home staff must ensure that the computer/ device/information is locked in the boot of their car
- All staff are required to abide by Data Protection training at all times [when handling Devon County Council data]
- Staff are prohibited from processing personal data outside the strict requirements of their job roles
- Any deliberate or reckless breach of the Data Protection policy by an employee may result in disciplinary action which could lead to dismissal
- All staff are required to report any suspected Data Protection breaches to Claire Lewis
- If you suspect that a Data Protection breach involving Devon County Council data has occurred, you must notify the Council immediately, by emailing keepdevondatasafe@devon.gov.uk or by phoning 01392 383000 and asking for the "Information Governance Team."
- Staff should report any breach of data to the manager using the Data Security Breach incident Report Form
- Staff are aware that data accuracy and security is a contractual and legislative requirement and that breach of this policy might result in disciplinary action

*People* who are supported by Culmside Support LLP (and people acting on their behalf) can help

- Ensure that all written information of a confidential nature are stored in a secure manner for example in a locked filing cabinet
- Ensure that all files or written information of a personal nature are not left out where they can be read by unauthorised staff or others.
- Staff fill in records and notes about you, join in with recording your information
- Make sure that all records and notes about you, including support plans, are signed and dated.
- Always use secure passwords when using a computer system and not tell people what your password is
- Always check the identity of any person requesting information about you and ask for help if you do not know who they are or why they need the information.
- Inform the manager of any changes that may affect the accuracy of the information stored about you.
- Only share information about yourself on a NEED TO KNOW basis.

END

**Applicable Publications and Legislation**

- Data Protection Act 1998
- Human Rights Act 1998
- Confidentiality: Code of Practice (DoH, 2003)
- Information Security Management (DoH 2007)
- Health and Social Care Act 2008
- Various Employment Legislation
- Records Management (DoH 2006)
- Codes of Practice:Information Commissioner (ICO)
- Professional Guidance and Codes of Conduct: GSCC
- Mental Capacity Act (2005)
- Health & social Care Act (2008) Regulations 2014
- GDPR Regulations 2018

Document Information

| | | | |
|---|---|---|---|
| Date of Issue: | July 2011 | Version | 1.0 |
| Author: | C.Lewis | | |
| Approved By: | | Date Approved: | |
| Matt Lewis – Partner | | July 2011 | |
| Beryl Lewis - Partner | | July 2011 | |
| | | | |
| Links or overlaps with other strategies/policies/documents: | | | |
| Confidentiality | | | |
| Record Keeping | | | |
| CRB Handling and Safekeeping Policy | | | |
| Information Asset Register | | | |
| Record of Processing Data | | | |
| Privacy Notice | | | |

Amendment History

| Issue | Status | Date | Reason for Change | Authorised |
|---|---|---|---|---|
| 1.0 | Review | Sept 12 | Review complete no change necessary | Matt Lewis |
| 2.0 | Update | Mar14 | New form for Subject Access Request | Claire Lewis |
| 3.0 | Update | Dec 18 | Addition of GDPR regulations | Claire Lewis |
| 4.0 | Update | Sept 2020 | Additional information included pertaining to mobile devices and data quality | Claire Lewis |