



MoCoCo

— HOUSE

**MH016 – DATA PROTECTION POLICY AND
PROCEDURE**

EMPOWERING YOUNG ADULTS FOR INDEPENDENT LIVING


www.mococo.org

PART OF MIDDLEWICH COMMUNITY CHURCH

Contents

1. Purpose of Policy.....	3
2. Service Records.....	3
3. Young People’s Records and Data	4
4. Registered Service Manager Responsibilities	5
5. Retention of Records	5
6. Confidentiality.....	6
7. Storing Electronic Data	7
8. Subject Access Requests	7
9. Information Sharing	8
10. Child Protection and Safeguarding Procedures	8
11. Data Accuracy	9
12. Staff Training.....	9
13. Associated Policies and Procedures.....	9

We are committed to review our Data Protection Policy and Procedure and when legislation changes.

Last Reviewed:	Kevin Pepper (Service Manager)		16/08/2023
Checked By:	Sylvia Brown (Service Consultant)		25/08/2023
Authorised By:			

1. Purpose of Policy

At MoCoCo House, we collect and process personal information about children and young people, as well as employed staff. We also keep records so we can operate our service.

On the 25th May 2018, the General Data Protection Regulation (GDPR) came into place across the European Union and also applies to the UK despite Brexit as the UK chose to also meet these regulations.

This policy provides MoCoCo House staff, students, and volunteers with an opportunity to familiarise themselves with the requirements in respect of processing personal data under GDPR regulations. Having this understanding is of vital importance to ensure we can demonstrate compliance with the terms of GDPR and avoid the risk of non-compliance and the consequences that can come from this. As a service we must gather and use young people’s personal information in order to provide services to them.

We recognise that the correct and lawful treatment of personal data will maintain confidence in the service. Protecting confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. The organisation can be exposed to potential fines of up to £17.5 million for failure to comply with the UK law relating to GDPR.

This policy explains what information we collect, how we maintain confidentiality and security and how long we keep information.

2. Service Records

Service records are regarded as confidential due to the sensitive nature of the information recorded, and include but are not limited to:

Service Record:	Type of Record:
Ofsted Registration Documents:	Paper/Electronic
Insurance and other contractual documentation	Paper/Electronic
Health and Safety Records: - Risk assessments	Paper/Electronic
Service Policy and Procedures:	Paper/Electronic
Employee Details: - Personal Information - Application forms, CV’s - DBS and employment references - Employment Contracts/ salaries - Monthly Supervision Records - Annual Appraisals (PDP) - Grievance and Disciplinary forms - Accident and incident forms. - Copies of qualification certificates - Photo of Staff Member	Paper/ Electronic
Company Documents (Middlewich Community Church)	Electronic (Breathe)
Financial Records regarding incomes and expenditures:	Electronic

3. Young People’s Records and Data

At MoCoCo House, we have a need to keep records about children and young people that we support, which include personal and development records. These records are regarded as highly confidential and contain highly sensitive information.

Personal records include, but are not limited to:

Personal Record:	Type of Record:
Referral information and young person’s ‘Pathway Care Plan’, provided by the Placing Authority.	Electronic
Incident/Information Sheets.	Electronic
Induction Paperwork: <ul style="list-style-type: none"> - Induction Form - Behaviour Contract - Consent Forms 	Paper
Care Plan Portal: <ul style="list-style-type: none"> - Personal details (name, age, DOB, family, social worker details etc). - Health Information - Risk Assessment - Information Sheet Log - Keyworking - Behaviour Management Plan - Work and Education (Timetables) - Missing from Home (MFH) - Warnings and Consequences Log - Authorised Visitors - Chronologies 	Electronic
Daily Sheet: A record kept daily by staff or the young person to detail their day.	Electronic
Keyworking forms: <ul style="list-style-type: none"> - Independence modules completed. - Development Sheets - Outreach sheets 	Electronic
Accident Report Forms:	Paper/ Electronic
Young Person contacts: <ul style="list-style-type: none"> - Social Worker and other professionals - Family Members - Friends and acquaintances - Support Agencies and Services 	Electronic
Young Person Correspondence:	Paper / Electronic
Young Person Identification:	Electronic
Picture of Young Person upon admission:	Electronic
Photos or Videos: Taken on house trips or activities with the consent of the young person.	Electronic

4. Registered Service Manager Responsibilities

All record keeping is the responsibility of the Registered Service Manager who is also the Data Protection Officer and Controller. The Registered Service Manager is responsible for the following:

- ✓ Ensuring electronic records are securely stored and encrypted where relevant.
- ✓ Ensuring all paper records are kept in an orderly way in files, and filing is kept up to date.
- ✓ Ensuring MoCoCo House staff are trained and understand how to securely store electronic and paper records appropriately.
- ✓ Ensuring all personal confidential details are locked away and are kept secure in the staff office, and the managers office.
- ✓ Ensuring the Placing Authority and anyone wanting to make a 'Subject Access Request' to information is given access within the bounds of the Data Protection Act 2018 and GDPR laws.
- ✓ Ensuring staff perform their duties in a professional and confidential way, in line with the Data Protection Act 2018 and GDPR Laws.
- ✓ Ensuring data protection policies and reviews take place.

5. Retention of Records

MoCoCo House is required to store young people's case records for 75 years from the date of birth of the child, or if the child dies before the age of 18, for 15 years from the date of his or her death (Department for Education, 2023).

When a young person is discharged from the service, their physical files are archived, and their electronic files are moved to a secure drive that can only be accessed by the Registered Service Manager.

Data in relation to employees will be kept for 6 years after the end of their employment.



6. Confidentiality

The definition of 'Confidentiality' is:

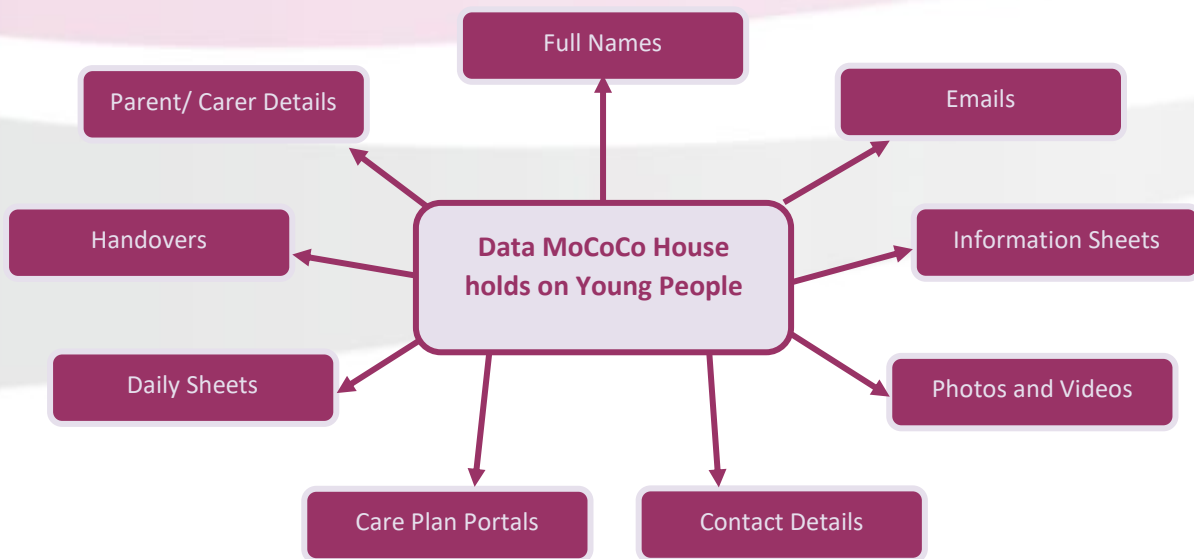
“Confidential information is information of some sensitivity, which is not already lawfully in the public domain or readily available from another public source, and which has been shared in a relationship where the person giving the information understood it would not be shared with others”.

(Information Sharing: Practitioners Guide).

At MoCoCo House, staff, students and volunteers must maintain a confidential relationship with the young people we support. It is our intention to respect the privacy of young people, while ensuring that they access a high-quality service.

In doing so staff should:

- ✓ Ensure all confidential data is stored securely.
- ✓ Ensure notebooks and other notes are kept in the staff office, away from service users, and any confidential information recorded is shredded and disposed of regularly. Staff notes should only be used in the short-term for recording information before processing the information on the computer system.
- ✓ Ensure workspaces are cleared at the end of shifts, leaving no confidential information behind.
- ✓ Ensure USB memory sticks are used solely for the purpose of transferring documents, and the data is deleted from the memory stick after use.
- ✓ Ensure computers, laptops and other devices are password protected when not in use in communal spaces.
- ✓ Check who they are talking to over the phone before disclosing confidential information.
- ✓ Only disclose confidential information to professionals on a 'need to know' basis.
- ✓ Remain careful not to disclose information about other young people or staff to other young people. Staff need to be cautious when working with young people in a group environment to ensure confidential information is not shared with the wider group.



7. Storing Electronic Data

At MoCoCo House, staff are expected to record information electronically on our Google Drive System. Few documents are handwritten, and therefore, most of the confidential information that we hold is computerised.

When confidential data is stored electronically staff must:

- ✓ Protect information from unauthorised access. This is done by storing all electronic data on the Google Drive system.
- ✓ Keep computer passwords secure, which should be changed regularly. Staff must not share passwords with anyone outside of the organisation.
- ✓ All data should be stored on the Google Drive System including, calendars, contacts, and emails.
- ✓ Ensure confidential data is not saved directly to computers, laptops, and mobile devices, and should only be used to access data from the Google Drive System.
- ✓ All devices used to connect to the Google Drive System should be protected by approved security and firewall software's.

8. Subject Access Requests

The Local Authority who has 'Parental Responsibility' or parents who share 'Parental Responsibility' with the Local Authority, have a right to access the personal data we hold on the young people we support. Equally, young people over the age of 16, also have the right to access their personal data, unless it is deemed harmful by the Local Authority.

Procedure for 'Subject Access Requests:

1. Any request to see a young person's file by the young person themselves, or their parent (with parental responsibility) may be made verbally or in writing to the Registered Service Manager.
2. The Registered Service Manager will acknowledge the request in writing and will prepare the file for viewing.
3. The Registered Service Manager will contact the Placing Authority and other agencies who have provided information, stating that a request for disclosure has been received and will ask for their permission to disclose to the person requesting it. (Often agencies will ask that information is sought from them directly and will refuse to disclose in this instance).
4. The Registered Service Manager will keep copies of any correspondence and their replies.
5. The young person's file is scanned, taking a copy of its full contents.
6. Any information which has been denied will be redacted, using a redacting marker, and every reference to the third party and information they have added is removed.
7. What remains is the information recorded by MoCoCo House and that of any third parties who have agreed to their information being disclosed. This is referred to as the 'clean copy'.
8. The 'Clean Copy' should be photocopied ready to show the individual requesting the information. The Registered Service Manager must go through the file with the requester, so that it can be explained.



9. Information Sharing

We can provide information more freely to the young people's Placing Authority and Social Worker upon request. Other professionals in a young person's support network may be given certain information if this is on a 'need to know' basis, however, staff need to be careful to only share relevant information.

Poor or non-existent information sharing is a factor that has been repeatedly identified as an issue in Serious Case Reviews (SCRs) carried out, following the death or serious injury to a child or young person. In some cases, sharing information can be the difference between life and death, so staff must understand in what circumstances they can share information.

Fears of sharing information should not be a reason for not sharing information with the intention of safeguarding and promoting the welfare of young people at MoCoCo House. Staff must take responsibility for sharing any safeguarding concerns they have, or sharing any information that they have to the Registered Service Manager within a timely manner, so an action plan can be put into place to share the information with relevant third parties.

If staff are unsure when they can share information to a third party, they must always liaise with the Registered Service Manager or a Senior staff member for support. The three critical criteria for information sharing are:

1. Where there is evidence that the child is suffering, or is at risk of suffering, significant harm.
2. Where there is reasonable cause to believe that a child may be suffering or at risk of suffering significant harm.
3. To prevent significant harm arising to children and young people or serious harm to adults including the prevention, detection, and prosecution of serious crime.

Our sharing procedures are based on the 'Seven Golden Rules for Sharing Information' as set out in '**Information Sharing: Practitioners Guide**' (HMG 2018). Please see **Appendix A** for more information.

10. Child Protection and Safeguarding Procedures

Where there is a child protection or safeguarding concern about a child or young person living at MoCoCo House, all staff must follow the necessary child protection procedures when an incident occurs:

1. Report the concern to the Registered Service Manager immediately, or in their absence, to a senior member of staff, and follow their instructions.
2. Produce a full written account of the concern or incident on an 'Information recording Sheet' and send to the Registered Service Manager via email.
3. Report the concern to the allocated social worker by sending the 'Information recording sheet' by secure email. If the concern is more urgent, staff should contact the social worker by telephone, as well as sending the concern via email. In the absence of the allocated social worker, staff should report the concern to the Local Safeguarding Board and ask for a duty social worker.
4. Should staff have a concern regarding a young person out of working hours, staff should contact the Emergency Duty Team (EDT), to report their concern.
5. Staff should follow the advice of the local authority, which may include reporting the concern to the police.
6. The Registered Service Manager should always be kept informed throughout the process.

11. Data Accuracy

The law requires MoCoCo House staff to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all staff who work with young people's data, to take reasonable steps to ensure that it is kept as accurate as possible.

Data relating to young people is held in a few places as necessary (Care Plan Portals, Young People's Files, Contacts, and Calendar). The service is confident that the computer systems in place cover all aspects of recording relevant data in relation to young people, and staff must not create alternative systems without authorisation from the Registered Service Manager.

Staff will take every opportunity to ensure data is updated when new information has been received. Young People's Keyworkers are responsible for ensuring 'Care Plan Portals' are updated routinely, however, it is the responsibility of all staff to update records when they are on shift, as and when they receive new information.

12. Staff Training

All MoCoCo House staff complete a formal induction which covers how we handle data within the service, as well as how to operate the computer systems we have in place to protect young people's data. This includes:

- ✓ What to do when data is requested by a third party.
- ✓ What 'Parental Responsibility' is and who we can share information with.
- ✓ In what circumstances can we share information without consent.
- ✓ What to do if a young person asks to see their own file.

Staff also complete training on Data Protection and GDPR, as part of their ongoing professional development.

13. Associated Policies and Procedures

The service also has the following related Policies in place that staff need to read and understand:

- **MH01** - Safeguarding and Child Protection Policy and Procedure.
- **MH05** - Behaviour Management Policy and Procedure.
- **MH017** – Surveillance and Monitoring Policy and Procedure.
- Staff Code of Conduct.



Appendix A: Data Protection Golden Rules when Sharing Information

1. Remember that the General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law are not barriers to justified information sharing but provide a framework to ensure that personal information about living individuals is shared appropriately.
2. Be open and honest with the individual (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 from other practitioners, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.
5. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.
6. Necessary, proportionate, relevant, adequate, 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 individuals 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.

For more information please visit:

HM Government – Information Sharing. Advice for practitioners providing safeguarding services to children, young people, parents, and carers.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1062969/Information_sharing_advice_practitioners_safeguarding_services.pdf

Policy & Procedure Amendments

Date:	Section within Policy:	Change(s) made to Policy/Procedure:	By whom:

Declaration:

I have read and understood the MoCoCo House Data Protection Policy and Procedure and accepted the principles within to safeguard children and young people at MoCoCo House.

All staff please sign Below:

Staff Member:	Position:	Date:	Signature: