

Connections in Mind Data Protection Policy

Last updated: November 2021

1. Introduction

Connections in Mind needs to collect and use certain types of information about the Individuals or Service Users who come into contact with **Connections in Mind** in order to carry on our work. This personal information must be collected and dealt with appropriately whether it is collected on paper, stored in a computer database, or recorded on other material, and there are safeguards to ensure this under the GDPR 2018.

2. Data Controller

Connections in Mind is the Data Controller under the Act, which means that it determines what purposes personal information held, will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

3. Disclosure

Connections in Mind may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

This data protection policy ensures **Connections in Mind** :

- Complies with data protection law and follow good practice
- Protects the rights of staff,, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

4. Data protection law

The General Data Protection Regulation describes how organisations — including Connections in Mind must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The General Data Protection Regulation is underpinned by **eight important principles**. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEEA),, unless that country or territory also ensures an adequate level of protection

The Individual/Service User will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows **Connections in Mind** to disclose data (including sensitive data) without the data subject's consent.

These are:

- a) Carrying out a legal duty or as authorised by the Secretary of State
- b) Protecting vital interests of a Individual/Service User or other person
- c) The Individual/Service User has already made the information public
- d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- e) Monitoring for equal opportunities purposes – i.e. race, disability or religion
- f) Providing a confidential service where the Individual/Service User's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Individuals/Service Users to provide consent signatures.

Connections in Mind regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

Connections in Mind intends to ensure that personal information is treated lawfully and correctly.

To this end, **Connections in Mind** will adhere to the Principles of the GDPR, 2018.

Specifically, the Principles require that personal information:

- a) Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
- b) Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
- c) Shall be adequate, relevant and not excessive in relation to those purpose(s)
- d) Shall be accurate and, where necessary, kept up to date,
- e) Shall not be kept for longer than is necessary
- f) Shall be processed in accordance with the rights of data subjects under the Act,
- g) Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
- h) Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Individuals/Service Users in relation to the processing of personal information.

Connections in Mind will, through appropriate management and strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information
- Meet its legal obligations to specify the purposes for which information is used

- Collect and process appropriate information, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements
- Ensure the quality of information use
- Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
 - The right to be informed that processing is being undertaken,
 - The right of access to one's personal information
 - The right to prevent processing in certain circumstances and
 - The right to correct, rectify, block or erase information which is regarded as wrong information)
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred abroad without suitable safeguards
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- Set out clear procedures for responding to requests for information

4. Data collection

Informed consent is when

- An Individual/Service User clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- And then gives their consent.

Connections in Mind will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

DATA PROTECTION POLICY

When collecting data, **Connections in Mind** will ensure that the Individual/Service User:

- a) Clearly understands why the information is needed
- b) Understands what it will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing
- c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- e) Has received sufficient information on why their data is needed and how it will be used

5. Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is **Connections in Mind** responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

6. Data access and accuracy

All Individuals/Service Users have the right to access the information **Connections in Mind** holds about them. **Connections in Mind** will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition, **Connections in Mind** will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Everyone processing personal information is appropriately trained to do so
- Everyone processing personal information is appropriately supervised

DATA PROTECTION POLICY

- Anybody wanting to make enquiries about handling personal information knows what to do
- It deals promptly and courteously with any enquiries about handling personal information
- It describes clearly how it handles personal information
- It will regularly review and audit the ways it hold, manage and use personal information
- It regularly assesses and evaluates its methods and performance in relation to handling personal information
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

Compliance with GDPR

GDPR stands for General Data Protection Regulation and replaces the previous Data Protection Directives that were in place. It was approved by the EU Parliament in 2016 and came into effect on 25th May 2018.

GDPR states that personal data should be 'processed fairly and lawfully' and 'collected for specified, explicit and legitimate purposes' and that individuals data is not processed without their knowledge and is only processed with their 'explicit consent'. GDPR covers personal data relating to individuals. Connections in Mind is committed to protecting the rights and freedoms of individuals with respect to the processing of children's, parents, staff and freelance personal data.

The Data Protection Act gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

GDPR includes 7 rights for individuals

1) The right to be informed

To deliver our services we collect parent's names, addresses, telephone numbers, email addresses, children's full names, addresses, date of birth and we keep notes about relevant information given by you, your child's school and professional notes from our coaches about your child. If you wish to

share reports with us from other professionals regarding your child, we will only be able to access these with your specific permission.

As an employer Connections in Mind is required to hold data on its employees; names, addresses, email addresses, telephone numbers, date of birth, photographic ID such as passport and driver's license, bank details. This information is also required for Disclosure and Barring Service checks (DBS) and proof of eligibility to work in the UK. This information is sent via a secure file transfer system to UKCRBs for the processing of DBS checks.

Connections in Mind uses Cookies on its website to collect data for Google Analytics, this data is anonymous.

2) The right of access

Connections in Mind is a company registered in England & Wales. Registration No: 10302221. Registered Office: Palladium House, 1-4 Argyll Street, London W1F 7LD

Telephone: 020 8050 1605

At any point an individual can make a request relating to their data and Connections in Mind will need to provide a response (within 1 month). Connections in Mind can refuse a request, if we have a lawful obligation to retain data but we will inform the individual of the reasons for the rejection. The individual will have the right to complain to the ICO if they are not happy with the decision.

3) The right to erasure

You have the right to request the deletion of your data where there is no compelling reason for its continued use. However Connections in Mind has a legal duty to keep children's and parent's details for a reasonable time.

Staff records must be kept for 6 years after the member of staff leaves employment, before they can be erased. This data is archived on secure servers and removed after the legal retention period.

4) The right to restrict processing

Parents, staff and freelance contractors can object to Connections in Mind processing their data. This means that records can be stored but must not be used in any way, for example reports or for communications.

5) The right to data portability

Connections in Mind requires data to be transferred from one IT system to another. These recipients use secure file transfer systems and have their own policies and procedures in place in relation to GDPR.

6) The right to object

Parents, staff and freelance contractors can object to their data being used for certain activities like marketing or research.

7) The right not to be subject to automated decision-making including profiling.

Automated decisions and profiling are used for marketing based organisations. Connections in Mind does not use personal data for such purposes.

Storage and use of personal information

All parent, children, staff and freelance contractor records are kept online on our CRM. Members of staff can have access to these files but information taken from the files about individual children is confidential and apart from archiving, these records remain on the CRM at all times. These records are deleted after the retention period.

Information about individual children is used in certain documents, such as referrals to external agencies and disclosure forms. These documents include data such as children's names, date of birth and sometimes address. These records are shredded after the relevant retention period.

Connections in Mind collects a large amount of personal data every year including; names and addresses of those enquiring about our services. These records are deleted after the relevant retention period. Information regarding families' involvement with other agencies is stored electronically on our CRM deleted after the relevant retention period.

GDPR means that Connections in Mind must;

- * Manage and process personal data properly
- * Protect the individual's rights to privacy
- * Provide an individual with access to all personal information held on them

| Children's Records | Retention Period | Status | Authority |
|-------------------------------------|--|-------------|-----------|
| Children's records - personal data, | A reasonable period of time after children | Requirement | GDPR |

DATA PROTECTION POLICY

| | | | |
|--|---------------------------------|----------------|---|
| reports, supervision notes and other correspondence | stopped using our services | | |
| Personnel Records | Retention Period | Status | Authority |
| Personnel files and training records (including disciplinary records and working time records) | 6 years after employment ceases | Recommendation | Chartered Institute of Personnel and Development |
| DBS check | 6 months | Recommendation | DBS Code of Practice The following basic information should be retained after the certificate is destroyed: the date of issue; the name of the subject; the type of disclosure; the position for which the disclosure was requested; the unique reference number; and the details of the recruitment decision taken |

DATA PROTECTION POLICY

| | | | |
|---|---|----------------|--|
| Wage/salary records (including overtime, bonuses and expenses) | 6 years | Requirement | Taxes Management Act 1970 |
| Statutory Maternity Pay (SMP) records | 3 years after the end of the tax year to which they relate | Requirement | The Statutory Maternity Pay (General) Regulations 1986 |
| Statutory Sick Pay (SSP) records | 3 years after the end of the tax year to which they relate | Requirement | The Statutory Sick Pay (General) Regulations 1982 |
| Income tax and National Insurance returns/records | At least 3 years after the end of the tax year to which they relate | Requirement | The Income Tax (Employments) Regulations 1993 (as amended) |
| Redundancy details, calculations of payments, refunds, notification to the Secretary of State | 6 years after employment ends | Recommendation | Chartered Institute of Personnel and Development |
| Records of any reportable death, injury, disease or dangerous occurrence | 3 years after the date the record was made | Requirement | The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (as amended) |

DATA PROTECTION POLICY

| | | | |
|--|--|----------------|--|
| Accident/medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH) | 40 years from the date of the last entry | Requirement | The Control of Substances Hazardous to Health Regulations 2002 (COSHH) |
| Assessments under Health and Safety Regulations and records of consultations with safety representatives and committee | Permanently | Recommendation | Chartered Institute of Personnel and Development |
| Financial Records | Retention Period | Status | Authority |
| Accounting Records | 3 years from the end of the financial year for private companies, 6 years for public limited companies | Requirement | Companies Act 2006 |
| | 6 years for charities | Requirement | Charities Act 2011 |
| Administration Records | Retention Period | Status | Authority |
| Employers' liability insurance records | For as long as possible | Recommendation | Health and Safety Executive |

DATA PROTECTION POLICY



In case of any queries or questions in relation to this policy please contact the **Connections in Mind** Data Protection Officer:

Mrs. Victoria Bagnall

Signed:

A handwritten signature in blue ink that reads 'V Bagnall.' The signature is written on a light blue rectangular background.

Position: Director

Date: 30/11/20

Last Reviewed Date: 15/11/21

Next Review: 15/11/22

Glossary of Terms

Data Controller – The person who (either alone or with others) decides what personal information **Connections in Mind** will hold and how it will be held or used.

Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person(s) responsible for ensuring that **Connections in Mind** follows its data protection policy and complies with the Data Protection Act 1998.

Individual/Service User – The person whose personal information is being held or processed by **Connections in Mind** for example: a client, an employee, or supporter.

Explicit consent – is a freely given, specific and informed agreement by an Individual/Service User in the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.

Notification – Notifying the Information Commissioner about the data processing activities of **Connections in Mind**, as certain activities may be exempt from notification.

The link below will take to the ICO website where a self assessment guide will help you to decide if you are exempt from notification:
http://www.ico.gov.uk/for_organisations/data_protection/the_guide/exemptions.aspx

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within (GROUP).

Sensitive data – refers to data about:

- Racial or ethnic origin
- Political affiliations
- Religion or similar beliefs
- Trade union membership
- Physical or mental health

DATA PROTECTION POLICY



- Sexuality
- Criminal record or proceedings

This pack has been adapted with permission from Voluntary Action Leicester Model Data Protection Policy.