General Data Protection Regulation (GDPR)

Confidentiality, Record Keeping and Data Protection

Version 1.0 April 2021

Review April 2023

This policy covers the following items:

1. Access to Employee Data
2. Caldicott Principles
3. Confidentiality of Service Users' Information
4. Document Tracking
5. Protecting Personal Data under the General Data Protection Regulation
6. Record Keeping
7. Sharing Information with Other Providers
8. Records Kept in Service Users' Homes

ACCESS TO EMPLOYEE DATA

Support to you aims to fulfil its obligations under the Data Protection Act 1998 to the fullest extent.

OUR PROCEDURE

1. Employees are allowed to have access to personal data about them held under the Data Protection Act 1998. This Act requires Support to You to respond to requests for access to personal data within 40 days.
2. Details of an employee's personal data are available upon request in accordance with the principles of the Data Protection Act 1998
3. Employees are required to read this information carefully and inform management at the earliest opportunity if they believe that any of their personal data are inaccurate or untrue, or if they are dissatisfied with the information in any way.

4. The Data Protection Act 1998 gives data subjects the right to have access to their personal data on request at reasonable intervals. Should employees wish to request access to their personal data, the request must be sent to info@supporttoyou.com The request will be judged in the light of the nature of the personal data and the frequency with which they are updated. The employee will then be informed whether or not the request is to be granted. If it is, the information will be provided within 40 days of the date of the request.
5. In the event of a disagreement between an employee and Support to You regarding personal data, the matter should be taken up under the Support to You's formal grievance procedure.

THE DATA PROTECTION ACT

Support to You recognises that it has a legal duty under the Data Protection Act 1998 to ensure the security and proper management of personal data and that this duty applies to its management, processing and storing of records and data, including information, data and notes about service users. Central to the Act is compliance with data protection principles which are designed to protect the rights of individuals about whom personal data is processed, whether this is via electronic or paper records.

The eight Data Protection principles state that we should make sure that personal information about people is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the UK without adequate protection.

Support to You's data protection policies and procedures are designed to comply fully with the Act and these principles. However, we also recognise that a further set of additional data protection principles apply to the NHS and social care, the Caldicott Principles.

The revised Caldicott Principles are as follows.

- Principle 1 — justify the purpose(s) for using confidential information.
- Principle 2 — only use confidential information when absolutely necessary.
- Principle 3 — use the minimum information that is required.
- Principle 4 — access to confidential information should be on a strict need-to-know basis.
- Principle 5 — everyone must understand their responsibilities.
- Principle 6 — understand and comply with the law.
- Principle 7 — the duty to share personal information can be as important as the duty to have regard for patient confidentiality.

Support to You understands that health and social care professionals should have the confidence to share information in the best interests of their patients and service users within the framework set out by these principles.

PERSON IDENTIFIABLE INFORMATION

With reference to both the Data Protection Act and the Caldicott guidelines, we recognise person-identifiable confidential information as including:

- a service user's name, address, full postcode and date of birth
- a service user's NHS number and any notes, records or information about their care or treatment
- any pictures, photographs, videos, audio recordings or other images of service users
- anything that may be used to identify a service user directly or indirectly, such as rare diseases, drug treatments or statistical analyses using small sample sizes that may allow individuals to be identified.

Importantly, we recognise that person identifiable information does not only relate to medical information and can take many forms. It can be stored on computers, transmitted across networks, printed or stored on paper, spoken or recorded.

We understand that overall, there should be a balance between the protection of information and the use and sharing of this information between agencies to improve care.

1. **POLICY**

   Support to You recognises that:

- We are required to have a data controller or manager who has overall responsibility for managing and effectively implementing all activities necessary to achieve compliance with the Data Protection Act 1998. The Data Controller for Support to You is Mrs. Susan Kemp
- NHS organisations and local authorities will have an allocated Caldicott Guardian who is responsible for agreeing and reviewing protocols for governing the transfer and disclosure of personal confidential data about patients and service users.
- A Caldicott Guardian is a senior health or social care person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.

- The Guardian plays a key role in ensuring that NHS, Councils with Social Services Responsibilities and partner organisations satisfy the highest practical standards for handling patient identifiable information.
- NHS and Social Care Caldicott Guardians are required to be registered and there is a UK Council of Caldicott Guardians made up of guardians from health and social care.

   Within Support to You:

- Managers and staff will comply fully not only with the eight principles of the Data Protection Act 1998, but also with the seven Caldicott Principles and with the common law duty of confidentiality. This means that any personal information given or received in confidence for one purpose may not be used for a different purpose or passed on to anyone else without the consent of the individual concerned. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.
- Service users will be told exactly what their personal information will be used for and how it will be stored and shared. This means fully describing how the data will be used and taking into consideration any language requirements or barriers to understanding, such as requirements under the Mental Capacity Act 2005.

- Support to You and its staff have a legal and ethical duty to safeguard the integrity, confidentiality, and availability of sensitive person identifiable information. Every use of person identifiable information must be lawful. Individual service users have a right to believe and expect that private and personal information given in confidence will be kept securely and used only for the purposes for which it was originally given and consented to.
- Staff and managers must be aware of the Caldicott Principles that will apply to any data exchange – they should be aware that NHS organisations and local authorities will have a Caldicott Guardian who will be required to agree to the exchange of person identifiable information.
- Staff and managers must ensure that, to comply with the Caldicott guidelines:
    - Every proposed use or transfer of person identifiable information within or from this organisation should be clearly defined and justified.
    - Personal identifiable information should not be used unless it is absolutely necessary and there is no alternative.
    - Where use of person identifiable information is considered to be essential, the minimum necessary personal identifiable information should be used and each individual item of personal information should be justified with the aim of reducing identity.
    - Where the use of personal confidential data is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.
    - Access to personal identifiable information should be on a strict “need to know” basis. Only those individuals who need access to person identifiable information should have access to it and they should only have access to the personal information items that they need to see. This may mean introducing access controls or splitting data flows where one information flow is used for several purposes.

- Managers should ensure that everyone is aware of their responsibilities and that a culture of care and due diligence for data security is in place. Actions should be taken to ensure that all staff who handle person identifiable information are aware of their responsibilities and obligations to respect confidentiality.
- Managers and staff should attend data protection and information governance training as required and to a level relative to the requirements of their role. All new staff should read this policy and Support to you GDRP policy and comply fully with them and with all related procedures.
- Any data breaches, including breaches of confidentiality, should be reported immediately on being discovered and should be fully investigated. A report should be submitted to Mrs. Susan Kemp.

CONFIDENTIALITY OF SERVICE USERS' INFORMATION POLICY STATEMENT

Support to You works on the principle that it has a duty of confidentiality to its service users. The service regards this as being of the utmost importance and a key part in building a trusting, caring environment where service users are safe in the knowledge that their confidences will be kept and where information about them will be protected safely. Our policy states that all the information we receive about or from service users is confidential and that only those people who need to know the information will have access to it. We will always seek their permission prior to sharing personal information about them with anyone else.

PROCEDURES

To comply with this policy Support to you staff must:

1. ensure that all files or written information of a confidential nature are stored in a secure manner in a locked filing cabinet and are only accessed by staff who have a need and a right to access them (see also the policy on Record Keeping)
2. wherever practical fill in all care records and service users' notes in the presence of and with the co-operation of the service user concerned
3. ensure that all care records and service users' notes, including care plans, are signed and dated.

Egress

Egress Web Access is an online service from Egress Software Technologies Ltd. that provides a secure way to share confidential information. We use this system when sending sensitive information about service users to another trusted organisation.

REQUESTS FOR INFORMATION

Support to you will not provide information to relatives, spouses, friends or advocates without the consent of the individual service user concerned. If the person is unable to give their consent a decision will be taken in line with "best interests" procedures set by the Mental Capacity Act 2005.

All enquiries for information, even if they are from close relatives, should be referred back to the service user or the service user's permission sought before disclosure. If the relative or person who seeks to have access to this information objects to the decision, they will be asked to make a formal written complaint, which will be addressed through the service's complaints procedure.

RECORD KEEPING

We keep information on all our service users but only keep minimal, relevant information to ensure that the care we offer as an organisation is of the highest quality. The files are only available to staff who need to use them. Information is kept on a secure cloud server which is password protected by 2 passwords.

Support to you makes sure that:

1. records required for the protection of service users and for the effective and efficient running of the service are maintained, are up to date and are accurate
2. service users have access to their records and information about them held by the service, as well as opportunities to help maintain their personal records
3. individual records and care service records are kept in a secure fashion, are up to date and in good order; and are constructed, maintained and used in accordance with the Data Protection Act 1998 and other statutory requirements.

We consider that access to information and security and privacy of data is a right of every service user and that service users are entitled to see a copy of all personal information held about them and to correct any error or omission in it.

Under the Data Protection Act 1998 the service should have a nominated data user/data controller.

The data user/data controller for this service is Mrs Susan Kemp

PROTECTING PERSONAL DATA UNDER THE GENERAL DATA PROTECTION REGULATION AIM AND SCOPE

This policy shows how we comply with the requirements of the data protection requirements found in Regulation 17: Good Governance of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, which expects service providers to have effective governance of their record keeping with records that are comprehensively fit for purpose and securely maintained.

The policy applies to all manual and electronic records kept by the service in relation to service users, including those involved with them, whose personal data might be found on their records, all staff, and any third parties (agencies and professionals), with whom anyone's personal data information held by the service might have to be disclosed or shared.

POLICY STATEMENT

Support to you recognises it must keep all records required for the protection and wellbeing of service users, and those for the effective and efficient running of the care service such as staff records to comply currently with the Data Protection Act 1998 and its successor Act, when passed by Parliament, and the EU General Data Protection Regulation (GDPR), which comes into force from May 2018 (and which is likely to apply post-Brexit).

In line with its registration under the Data Protection Act, and to comply with the GDPR, the service understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

This means that all personal data obtained and held by the care service to carry out its activities as a registered care provider must:

- have been obtained fairly and lawfully
- held for specified and lawful purposes as an organisation that is carrying out a public duty
- processed in recognition of persons' data protection rights, which are described in the GDPR in terms of the right:
    - – to be informed
    - – to have access
    - – for the information to be accurate and for any inaccuracies to be corrected
    - – to have information deleted (e.g. if inaccurate or inappropriately included)
    - – to restrict the processing of the data to keep it fit for its purpose only
    - – to have the information sent elsewhere as requested or consented to (e.g. in any transfer situation)
    - – to object to the inclusion of any information (e.g. if considered to be irrelevant)
    - – to regulate any automated decision-making and profiling of one's personal data.
- be adequate, relevant and not excessive in relation to the purpose for which it is being used
- be kept accurate and up to date, using whatever recording means are used or agreed (eg manual or electronic)

- not be kept for longer than is necessary for its given purpose (e.g. in line with agreed retention protocols for each type of record)
- have appropriate safeguards against unauthorised use, loss or damage with clear procedures for investigating any breaches of the data security
- comply with the relevant GDPR procedures for international transferring of personal data.

PROCEDURES

Support to you have therefore taken the following steps to protect everyone's personal data, which it holds or to which it has access so that it complies with current data protection laws and the GDPR.

It appoints or employs staff with specific responsibilities for:

1. the processing and controlling of data – Mrs Susan Kemp
2. the comprehensive reviewing and auditing of its data protection systems and procedures – Mrs Susan Kemp
3. overviewing the effectiveness and integrity of all the data that must be protected

RECORD KEEPING POLICY STATEMENT

Every care service is required to have systems and methods for keeping records that comply with its registration conditions as set out and specifically Regulation 16: Records of Personal Plans, Regulation 55: Records and Regulation 74: Duty to ensure there are systems in place for Keeping of Records and the General Data Protection Regulation (GDPR), which applies to all business and organisations that process personal data.

This policy is intended to set out the values, principles and policies underpinning Support to you's approach to record keeping, data protection and access to records.

The policy should be read and used in relation to policies on:

Support to You works to the following principles of good record keeping.

1. Records required for the protection of service users and for the effective and efficient running of the service are maintained, are up to date and are accurate.
2. Service users have access to their records and information about them held by the care service, as well as opportunities to help maintain their personal records.
3. Individuals' records and other records that contain private, confidential personal data are kept in a secure fashion, are up to date and in good order, and are constructed, maintained and used in line with the applicable regulations and related policies (see above).

DATA PROTECTION

ACCESS TO RECORDS

Support to You considers that access to information and security and privacy of data is an absolute right of every service user and that service users are entitled to see a copy of all personal information held about them and to correct any error or omission in it.

RECORD-KEEPING PROCEDURES

All Support to you staff must do the following.

1. Ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them. Where a service user keeps their own records at home the manner of safe storage is discussed with the person concerned and / or where appropriate, their relatives.
2. Be aware that the relatives of a service user do not have any automatic right of access to that service user's files and need to have the service user's permission to see any information on that person. If the service user lacks the mental capacity to give their permission a "best interests" procedure would then need to be followed in line with the Mental Capacity Act 2005.
3. Ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people.
4. Wherever practical or reasonable fill in all care records and service users' notes in the presence of and with the co-operation of the person concerned.
5. Ensure that all care records and service users' notes, including care plans, are signed and dated.
6. Check regularly on the accuracy of data being entered into computers.
7. Always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.
8. Use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data relating to service users or staff should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by the manager. Where personal data is recorded on any such device it should be protected by:

1. ensuring that data is recorded on such devices only where absolutely necessary
2. using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
3. ensuring that laptops or USB drives are not left lying around where they can be stolen.

RETENTION OF RECORDS

All records are kept in line with the requirements of the current legislation and guidance. Service users' personal records that have been kept independently by the service are always kept for a minimum of three years from the date of the last entry after they leave the service or after their death.

SHARING INFORMATION WITH OTHER PROVIDERS POLICY STATEMENT

Care in Hand accepts that to provide the highest standard of care for our service users it is vital to work in partnership with other professionals and services. A key aspect of partnership working is the sharing of relevant information, which in line with confidentiality and data protection rules, should always be on a "need to know" basis.

This policy is intended to set out the values, principles and procedures underpinning the service's approach to sharing information about service users with other providers.

POLICY ON SHARING INFORMATION WITH OTHER PROVIDERS

Support to You recognises that its services form one element in the range of care, treatment and support with which its service users need to be engaged, and that, to provide optimal care, it needs from time to time to share information with other health and social care providers. Subject to our obtaining the express consent of service users there is a particular responsibility for such information sharing:

- when a prospective service user is considering having further care input
- when a service user needs a specific health service
- when a service user is admitted to or discharged from hospital
- when a service user transfers to another care setting

Sharing information about a service user will only be undertaken with their express permission unless a best interests decision has been made by the appropriate health care professionals.

RECORDS KEPT IN SERVICE USERS' HOMES POLICY STATEMENT

This policy is intended to set out the values, principles and policies underpinning Support to You's approach to record keeping, data protection and access to records in respect of those records that are kept in service users' homes.

Support to You believes that all records required for the protection of service users and for the effective and efficient running of Support to you should be maintained accurately and should be up to date, that service users should have access to their records and information about them and that all individual records and agency records are kept in a confidential and secure fashion.

PROCEDURES

1. With the service user's consent, care workers should record, in records kept in the homes of service users, the time and date of every visit of to the home, the service provided and any significant occurrence.
2. Support to You staff should ensure that all written records are legible, factual, signed and dated by the person making the record, and kept in a safe place in the home, as agreed with the service user.
3. Support to You will ask any service user who refuses to have records kept in their home to confirm the refusal in writing, if this is not possible staff will document it and it will be kept at Support to You's office.
4. Individual records and Support to You records are always kept in a secure fashion, are up to date and in good order; and should be constructed, maintained and used in line with the Data Protection Act 1998 and other statutory requirements.
5. Support to You policy is to keep the ongoing records in the service user's home two months After the agreed time they are transferred with the permission of the service user, to the office for safe keeping and reviewing purposes.

Support to You staff should:

- wherever practical or reasonable, fill in all care records and service user notes in the presence of and with the co-operation of the service user concerned
- ensure that all care records and notes, including service users' plans, are signed and dated

- Ensure that all files or written information of a confidential nature are stored in as secure as possible within a service user's home – encouraging them to store out of plain sight.
- Inform the office where a file falls below the standards required (such as tattered or broken folder), where a replacement and updated file will be provided.