Home Link Family Support

General Data Protection Regulation Policy

Home Link Family Support is committed to a policy of protecting the rights and privacy of individuals, including Service Users, Staff, Volunteers and the Board, in accordance with the General Data Protection Regulation (GDPR) May 2018.

The GDPR demands higher transparency and accountability in how we manage and use personal data. It also gives individuals stronger rights to understand and control how their data is used.

Home Link Family Support needs to process some personal information about its Service Users, Staff, Volunteers and Board for various purposes such as, but not limited to:

1. Providing a range of support to Service Users
2. The recruitment and payment of Staff
3. The recruitment of Volunteers
4. The recruitment of the Board
5. Complying with legal obligations to funding bodies and the organisations we work with to provide our services

Scope

This policy applies to Staff, Volunteers and Board members. Any breach of this policy or of the General Data Protection Regulation itself may be considered an offence and Home Link Family Support's disciplinary procedures may be applied.

Other agencies and individuals working with Home Link Family Support, who have access or require access to personal information, will be expected to comply with the GDPR.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

Further details of good practice can be found in the Home Link Family Support *Data Protection Principles, Guidelines and Best Practice* document.

Responsibilities under GDPR

Home Link Family Support is a "Data Controller"; this means we determine the purposes and means of processing data. We are responsible for ensuring any personal data we hold is processed in compliance with GDPR.

Compliance with the legislation is the personal responsibility of all members of Staff who process personal information.

"Personal data" refers to any information relating to an identifiable person who can be directly or indirectly identified using particular personal identifiers. The personal identifiers, which constitute personal data, include:

- names
- addresses
- telephone numbers
- job titles
- date of birth
- salary
- ID numbers
- location data
- online identifiers
- genetic data or biometric data

The GDPR lists "**special categories of personal data**" which include:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership
- genetic and biometric data
- data concerning health, sex life or sexual orientation

The GDPR applies to personal data held in automated systems and in manual filing systems.

Data Protection Principles

Under the GDPR, the data principles set out the main responsibilities we must meet to comply with the legislation.

The GDPR requires that the data controller shall be responsible for, and be able to demonstrate, compliance with the following principles:

1. Data will be processed lawfully, fairly and in a transparent manner in relation to individuals.

We have created *Privacy Notices* that sets out our legal basis for:

- collecting and processing personal data
- how we use the data
- how the data is securely stored and destroyed

We have ensured our *Privacy Notices* are clearly written and easy for Service Users, Volunteers and Board members to understand.

2. Data will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

We will ensure that all data collected will only be used for the purposes stated in our *Privacy Notices*.

3. Data will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

We will only collect data we need to enable us to provide suitable support to our Service Users.

4. Data will be accurate and kept up to date.

We will ensure that any inaccurate data or any changes to circumstances are noted and amended. We will regularly check with our Services Users to make sure we have accurate information.

5. Data will not be kept for longer than is necessary for the purposes for which the personal data is processed.

We archive our closed files by year of deletion. We annually delete files that are no longer required; this includes deletion of manual and electronic files. Files are disposed of securely. Our Records Management policy states our retention periods.

6. Data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

We will ensure that all personal data is accessible only to those who have a valid reason for using it. We have appropriate security measures in place which include:

- keeping hard copy personal data in locked cabinets with controlled key access
- archived data is stored in locked cabinets with controlled key access
- using lock bags to transport any personal data out of the office, all lock bags are returned to the office at the end of the day

- taking no identifiable information to home visits
- ensuring data held electronically is password protected
- ensuring secure email is used for personal and confidential data
- gathering GDPR compliance information from our IT support and suppliers
- ensuring PCs, tablets and phones are password protected when unattended.
- ensuring that PC, tablet or phone screens are not visible to others
- requiring Staff, Volunteers and Board members to delete notes and copies of files
- ensuring conversations are not held in public relating to Home Link Family Support work
- seeking appropriate permissions to take and use photographs of individuals for use in publications or on our website
- ensuring all personal data is disposed of securely.
- ensuring that all new projects and services consider privacy and data protection from the start, we will utilise Privacy Impact Assessments (PIAs) where relevant

Lawful Basis For Processing Data

The GDPR requires Home Link Family Support to have a valid lawful basis for processing personal data.

GDPR sets a high standard for consent. Consent means offering individuals real choice and control. Genuine consent must put individuals in charge and build trust and engagement.

1. Consent

Consent means offering individuals real choice and control over their personal information. All data subjects must actively and knowingly opt-in to consent. They must be made aware of what they opting in for, what it will be used for and the length of time for which it will be kept.

Consent must be:

- Freely given, specific, informed and unambiguous.
- By a statement or by clear affirmative action signifying agreement to the processing of personal data relating to him/her (by means of an “opt-in” as opposed to an “opt out” action).
- Verifiable e.g. records of how and when consent was given should be kept.

For special categories of personal data, in addition to the above, the consent must be “explicit”. The data subject should sign an express written “opt-in” consent statement which clearly lays out what we are collecting, why, what we will use it for and how long we will keep it.

Our *Privacy Notice* clearly states the service we will provide and how we will process our Service Users' data.

Service Users can state which professionals or organisations they will allow us to contact and share information with. We provide each Service User with a *Fair Processing Summary*. This includes details of professionals and organisations with whom we may need to share information. In addition to the *Privacy Notice* we gather separate permissions from Service Users to share their information on our *Information Sharing* form.

Consent is gained from Service Users during a face-to-face meeting with a member of Home Link Family Support Staff. This Staff member explains the *Privacy Notice, Fair Processing Summary* and *Information Sharing* form to the Service User, and witnesses the consent given by the Service User's signature.

We include details of how Service Users can withdraw consent and how they can complain if they feel there is a problem with how we processed their data. We provide contact details for the Information Commissioner's Office.

2. Vital Interests

Vital interests can be used as a lawful basis if we need to process personal data to protect someone's life. Where there is a child protection concern, we have a duty to pass this on to the relevant professionals. We will inform Service Users of this at the time, as long as there is no significant risk to the child by doing so.

Subject Access Rights (SARs)

Individuals have a right to access any personal data relating to them that is held by Home Link Family Support. Any Service User, Staff member, Volunteer or Board member wishing to access their personal data can contact Home Link Family Support to make a Subject Access Request. The GDPR also introduces a right for individuals to have their personal data erased. This is known as 'the right to be forgotten'.

Data Breaches

The GDPR makes it the duty of all organisations to report certain types of personal data breach to the Information Commissioner's Office. This must be done within 72 hours of becoming aware of the breach, where feasible.

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen

- alteration of personal data without permission
- loss of availability of personal data

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay.

We have measures in place to identify breaches, we have investigation and internal reporting procedures in place. This allows us to decide whether or not we need to notify the relevant supervisory authority and the affected individuals. This will also allow us to decide whether we need to invoke the Home Link Family Support Disciplinary policy.

Serious breaches of personal data can incur a substantial fine for the organisation and can result in Staff dismissal where a member of Staff is found responsible for the breach.

We will keep a record of any personal data breaches, regardless of whether we are required to notify the Information Commissioner's Office.

Procedure For Review

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998.

Further Information

Further detail of the requirements of the General Data Protection regulation can be found at the Information Commissioner's website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Associated Documents

Privacy Notices
Fair Processing Summary
Information Sharing form
Data Protection Principles, Guidelines and Best Practice
Subject Access Request (SAR)
Records Management policy

Created May 2018
Review May 2020