Home-Start Surrey Heath GDPR policy

This policy sets out how Home-Start Surrey Heath (**Home-Start**) will implement the requirements of and comply with Regulation (EU) 2016/679 (more commonly known as the General Data Protection Regulation ("**GDPR**").

From 25 May 2018, the GDPR (and any UK national law seeking to implement its provisions) regulates the protection of individuals' personal data, replacing the Data Protection Act 1998 ("**DPA**"). Many of the core data protection principles remain the same as under the DPA, but there are significant enhancements that need to be addressed in order to comply with the GDPR.

Policy Statement

Home-Start is committed to the protection of the rights and freedoms of individuals in accordance with the provisions of the GDPR. We will comply fully with the requirements of the GDPR and will follow procedures which aim to ensure that all persons who have access to any personal data held by or on behalf of Home-Start are fully aware and abide by their duties and responsibilities under the legislation.

We will ensure that all personal information is processed properly however it is collected, retained, used or otherwise processed; on paper, in computer records or recorded by any other means. Accurate, proportionate and up to date records are kept to ensure a good framework of support and supervision for volunteers and employees, and to comply with employment, charity and company legal requirements.

In order to operate efficiently, Home-Start processes information about its staff and about people with whom it works. These may include current, past and prospective employees, volunteers, trustees and donors. Families, volunteers and employees are made aware that the scheme retains a record of Home-Start's contact or work with them, and that they can request access to records held about them.

Local Home-Starts shall ensure they have obtained all authorisations and registrations and provided all notifications necessary under the data protection legislation in order to lawfully carry out its data processing activities.

1 Definitions

For the purposes of this policy, the following definitions shall apply:

"**personal data/ information**"
Any information relating to an identified or identifiable natural person ("**data subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as 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 includes:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
- genetic and biometric data; and
- data concerning health, a natural person's sex life or sexual orientation.

"**personal data breach**"
Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

For example, loss or theft of data or equipment, unauthorised access either by a member of staff or third party, human error (such as accidental deletion or alteration of data), unforeseen

circumstances (such as fire or flood) or deliberate attacks on IT systems (such as hacking, viruses or phishing scams).

"**processing/ process**"
Processing includes anything done with personal data whether or not by automated means such as:

- collecting, storing
- organising, structuring
- using, disclosing
- erasing, destroying

2 GDPR Data Protection Principles

Home-Start will comply with the data protection principles of the GDPR to ensure all personal data is:

- Processed lawfully, fairly and in a transparent manner;
- Obtained for specified, explicit and legitimate purposes only;
- Only processed in a way that is compatible with the purpose(s) for which it was collected;
- Adequate, relevant and limited to what is necessary for the relevant purpose(s);
- Accurate and up to date;
- Kept for no longer than is necessary for the purpose(s) for which the data is processed;
- Processed in accordance with the data subject's rights under the GDPR;
- Kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage; and
- Not transferred outside of the United Kingdom without appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

3 Governance

(a) The Board of Trustees

Home-Start's compliance with the GDPR is the overall responsibility of Home-Start's Board of Trustees ("**the Board**").

The Board will review and recertify a GDPR compliance statement for use with third parties, regulatory bodies and families.

(b) Data Protection Lead

The Board will appoint a named Data Protection Lead, who shall:

- Inform and advise Home-Start and its employees who carry out processing of their obligations pursuant to the GDPR.
- Monitor compliance with the GDPR, including the assignment of responsibilities, awareness-raising and training of employees, trustees and volunteers involved in processing operations, and the related audits.
- Oversee, and provide advice where requested on the annual process of reviewing data protection impact assessments ("**DPIA**") – more detail on DPIAs is set out below.
- Oversee progress with the action log and risk register.
- Co-operate with and act as the key contact point for the Information Commissioner's Office ("**ICO**") on issues relating to Home-Start's data processing, including personal data breaches and any necessary DPIA consultations.

(c) All employees, trustees and volunteers

It is the responsibility of all employees, trustees and volunteers to adopt this policy and to conduct themselves with integrity and in a way which considers the rights and freedoms of parents and families at all times. Every individual has a critical role to play in the correct

processing and control of personal data and sensitive categories of data. In particular, they are required to:

- Familiarise themselves with the provisions of the GDPR and ensure they understand their individual responsibilities (including but not limited to keeping personal data and other confidential information secure) and to seek guidance from their line manager if they are unclear as to the application of the GDPR to their role.
- Read and comply with this policy and the Information Governance Policy (including any associated guidance and procedures issued from time to time) and attend all training sessions (including the review of all training session materials) in relation to data protection as relevant to their role.
- Ensure any information they provide in connection with their employment/engagement is accurate and up to date and inform Home-Start of any changes to information that they have provided, e.g. changes of address or changes to the bank or building society account to which the individual is paid (if applicable).
- Reporting security risks and personal data breaches in accordance with this policy and the GDPR policy.

4 Training

All employees, trustees and volunteers must receive data protection training. Training will include but not be limited to the storage and handling of information, how to identify personal data and personal data breaches and the obligations imposed by the GDPR and this policy. Evidence of this training will be kept for three years. Refresher training should be provided annually for existing staff.

5 Confidentiality

Home-Start recognises that the legitimate use of confidential information (including personal data) underpins our service. All information about parents and families is treated as confidential, to be shared only as necessary in support of the volunteer and to assist the family. Home-Start ensures that personal and operationally sensitive information is maintained confidentially and in line with the GDPR. Any disclosure of confidential information (including personal data) about a family to another person for the purpose of assisting the family is only undertaken with the expressed permission of the parent/s, *except* to protect the welfare of a child or adult at risk *or* in very limited and extremely rare circumstances where a person is suspected of a disclosable offence [1] or terrorism.

[1] Disclosable offence: drug trafficking; drug money laundering

6 Consent

Consent is one of the lawful bases to process an individual's personal data.

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 are 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 is being collected, why, what it will be used for and how long it will be kept. Home-Start is

likely to be processing such categories of data and so we must ensure that "explicit" consent is obtained before processing.

Consent for Children
Children need particular protection when Home Start is collecting and processing their personal data because, amongst other considerations, they may be less aware of the risks involved. If under 16, consent must be given by the holder of parental responsibility (this may be subject to change as data protection laws and guidance evolve from time to time).

Consent at the point of referral
A signature is required from the referrer to consent to their personal data being processed. All data subjects must know what Home-Start will do with their information and who it will be shared with.

Consent must be sought from the family before any identifying information can be collected about the family. At the point of referral a member of the family must sign the referral form. If this is not signed then personal data cannot be stored and the referral cannot be accepted. Communication with the referrer is the responsibility of the organiser/coordinator.

Consent is sought from families who have self-referred to process their information. Consent is also required to inform their health visitor or other agency, that they have requested Home-Start support and to share any information with them.

Consent at the initial visit
At the initial visit, consent is sought from the family to share general information about the kind and level of support Home-Start is providing:

- with the referrer
- with other agencies currently involved with the family
- with funders, where necessary
- for anonymised case studies

Consent records
Home Start will at all times keep records to demonstrate a data subject's consent. Such records shall be kept for no longer than strictly necessary for compliance with a legal obligation or for the establishment, exercise or defence of legal claims.

Right to withdraw consent
Individuals have the right to withdraw consent at any time and must be informed of this before giving consent. Consent should also be reviewed from time to time and refreshed if anything changes concerning the processing of any of the data subject's personal data. At the point of withdrawal, if Home Start has no other lawful basis justifying the processing of the personal data, the data shall be deleted or anonymised.

Moving Area/Schemes
Where a family moves area, seeks support from a new local Home-Start and has given its consent, appropriate information is shared with the new scheme in order to ensure the best possible support. If consent is not given and there are or have been safeguarding concerns in the family concerned, the Scheme will share appropriate information with the new scheme. We shall also maintain appropriate systems and procedures to allow all individuals to exercise their right to data portability (the right for an individual to be sent, on request, their personal data in a format which allows the data to be moved directly from one IT environment to another).

7 Process

Home-Start actively manages the personal data which is collected, retained or otherwise processed through an annual review cycle. The annual review cycle will include an identified register of information flows, associated DPIAs and a resulting action log. An information risk register will be maintained and reviewed by the board. All of this documentation should be reviewed at least annually by the Data Protection Lead.

7.1 Data protection impact assessments (DPIA)

Home-Start will identify all the areas where we process personalised information (processing activities). A register of information flows should be held and DPIAs must be carried out annually for all processing activities. A DPIA must also be carried out when any new technologies are introduced to the scheme and whenever a new processing activity is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA should contain:

- A description of the processing operations and the purposes, including where applicable, the legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate compliance.

Note: A DPIA can address more than one project.

7.2 Action log

Home-Start shall create and maintain (and the Data Protection Lead shall oversee the maintenance of) an action log. The action log shall include the information flow, the action to be taken, estimated date for completion and the responsible person or persons for this action.

7.3 Risk Register

Each DPIA will identify the risks inherent in the personal data being held and processed. These risks will be collated into a summary risk register, noting the planned mitigations and links to the action log. This register must be reviewed at least annually by the Board.

7.4 Registration

Home-Start shall ensure we have obtained all authorisations and registrations and provided all notifications necessary under the data protection legislation in order to lawfully carry out our data processing activities.

7.5 Subject access requests

Individuals have the right to access their personal data and supplementary information, amongst other things to allow such individuals to be aware of and verify the lawfulness of the processing.

Any such request should be made in writing, to the chair/senior worker of the Scheme. If Home-Start receives an access request they must provide information without delay and at the latest within one month of receipt (free of charge). If requests are complex or numerous, this can be extended by a further two months, but the individual must be informed within one month of the receipt of the request and explain why the extension is necessary.

Home-Start must verify the identity of the person making the request, using 'reasonable means'.

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 under statute and will be disposed of appropriately thereafter.

If an employee would like a copy of any of the information held on him/her they should notify their line manager. If he/she believes that any information held about him/her is incorrect or incomplete then he/she should write to their line manager as soon as possible setting out the information which he/she believes needs correction.

7.6 Accuracy

Home-Start will endeavour to ensure that all personal data held in relation to data subjects is accurate and kept up-to-date. Data subjects must notify Home-Start of changes in information held about them. Data subjects have the right to have personal data rectified without undue delay if it is inaccurate or incomplete.

7.7 Erasure

Individuals have the right to request that any of their personal data held by Home-Start be erased ('right to be forgotten'). The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Home-Start may refuse the request in limited circumstances, including for public health purposes in the public interest and the exercise or defence of legal claims.

Home-Start must pay special attention to requests relating to children's personal data. This is because a child may not have been fully aware of the risks involved in the processing at the time of consent.

To the extent that Home-Start has disclosed any personal data to any third parties, it shall inform such parties about the request for erasure, unless it is impossible or involves disproportionate effort to do so.

7.8 Personal Data Breach

All employees, trustees and volunteers must report, and co-operate in the resolution of all personal data breaches in accordance with this Section 7.8 and the flowchart at Appendix 1. This shall also include where a data protection control has failed but has not resulted in a breach (a 'near miss').

Home-Start (when acting in its capacity as data controller) is obliged under the GDPR to notify the ICO of all personal data breaches within 72 hours of becoming aware of the breach, unless the breach in question is unlikely to result in a risk to the rights and freedoms of individuals. We must internally record all breaches (including the facts relating to the breach, its effects and the remedial action taken), regardless of whether the breach is such that it needs to be notified to the ICO.

It is therefore very important that all employees, trustees and volunteers notify the Data Protection Lead (or Trustee Chair if the Data Protection Lead is not available) in accordance with the timescales set out in the flowchart at Appendix 1. Such a report should include a description of the nature of the breach including where possible, the categories and approximate number of affected individuals, the categories of data and the approximate amount of personal data affected.

The breach must be investigated and any relevant protective action taken, to prevent the breach from escalating or being repeated.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, we must directly notify all those individuals affected by the breach without undue delay. This should not be done by any employee, trustee or volunteer without first notifying the Data Protection Lead (or in their absence the Chair).

Home-Start (assisted by the Data Protection Lead) must produce:

- An action plan
- A report of the breach (including lessons learnt) for the Board of Trustees.

Home Start takes compliance with this policy very seriously. Failure to comply puts at risk the individuals whose personal information is being processed. If any individual fails to comply with this policy (including but not limited to disclosing personal data in breach of the principles set out in the data protection legislation), he/she may be committing a criminal offence carrying significant sanctions and he/she may be subject to disciplinary action and subsequently asked to leave the Scheme.

7.9 Technology

Home-Start will take appropriate technical, as well as organisational, steps to ensure the security of personal data. This will include, but not be limited to, encryption, layered security and the use of complex passwords.

When any information technology needs to be renewed (including infrastructure servers, hardware, mobile devices and software) security by design must be a key concern.

It is Home-Start's responsibility to ensure all personal and company sensitive data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

8 External processors

Home-Start will ensure that data processed by external data processors (for example service providers, Cloud services and website hosts) are compliant with this policy and all relevant data protection legislation. Their GDPR compliance statement should be seen and a written contract/undertaking entered into containing at least the minimum information required by the data protection legislation and all associated guidance notes (see the Information Governance Policy for more details).

9 Information governance

The Home-Start Information Governance Policy must be followed by all employees, trustees and volunteers in addition to this policy, including but not limited to retention procedures.

Signature of Chair: _____ Name: _____

Date policy adopted: _____ Date to be reviewed _____

Appendix 1- Breach Response

GDPR introduces a duty on all organisations to report certain types of personal data breach **within 72 hours** of becoming aware of the breach. In addition you must note:

- If a breach results in high risk of adversely affecting individuals' rights you must also inform those individuals without undue delay.
- Ensure you have robust breach detection, investigation and internal reporting procedures to help facilitate decision-making.
- You must keep a record of any personal data breaches regardless of whether you are required to notify.

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of your global turnover. For more information on Personal Data Breaches please read ICO guidance.