HOME-START Mid & West Suffolk ("Home-Start")
INFORMATION GOVERNANCE POLICY AND PROCEDURE

This policy contains the following:

- **The Procedure for Information Sharing and the Preservation of Confidentiality**
- **Record Retention Periods (Appendix 1)**
- **Data Protection Supporting Guidance (Appendix 2)**
- **Example Privacy Notice (Appendix 3)**

Information Governance Policy Statement

Home-Start recognises that the legitimate use of information 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 processed in line with the General Data Protection Regulation ("**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 explicit consent 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 or terrorism.

Home-Start's position on data protection and confidentiality is made clear to all connected with it. The trustees of Home-Starts are responsible for ensuring that the requirements of this policy are met throughout the local Home-Start ("**Scheme**"). Breaches of confidentiality and data protection are treated seriously and may result in the individual concerned being required to leave the Scheme.

All new trustees, employees and volunteers are provided with a copy of this policy (or extracts thereof for volunteers) as part of their induction/ training. All are expected to abide by this policy and procedures, according to their role.

Procedure

1. Families: Information and consent

1.1. Families are given clear information, verbally and in writing, which explains Home-Start's position on confidentiality and their rights under applicable data protection legislation, including their right to request access to their records.

1.2. 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; and
- for anonymised case studies.

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

1.4. Specific consent is sought from the family in order to share additional information as part of local multi-agency arrangements.

1.5. Families are informed of any communication between Home-Start and other agencies unless this will impact on the safety or welfare of a child or adult at risk.

1.6. Family records are held securely at the Scheme premises.

2. Safeguarding / Child protection

Where there are concerns about the safety or wellbeing of a child or adult at risk and it is considered necessary for their welfare and protection, information is shared with the appropriate authority in line with Home-Start's Safeguarding and Promoting the Welfare of Children/Safeguarding Adults at risk policies which over-rides this policy.

3. Trustees

3.1. Information provided to the board of trustees about families relating to the nature and level of referrals, local trends or case studies to illustrate the work and outcomes of Home-Start are all made anonymous.

3.2. Trustees ensure that the confidentiality of families, volunteers and staff, and confidential information relating to the operational work of the Scheme is maintained at all times in line with this policy and the associated procedures. The trustees should agree in what circumstances files will be accessed and by whom, e.g. trustees spot-checking files and contractors.

4. Staff and volunteers

4.1. Organisers/co-ordinators discuss the support of families with their line manager. Volunteers discuss their support of families with their organiser/co-ordinator. Discussions take place in a confidential setting, for the purposes of supervision and to ensure the best possible support to the family.

4.2. Confidentiality of families and volunteers and confidential information relating to the operational work of the Scheme must be maintained at all times in line with this policy.

4.3. Volunteers meeting together for peer support do not share information that may identify or breach the confidentiality of the family they support.

5. Family Groups

Home-Start staff explain the importance of respect and confidentiality as part of a family's introduction to a group, and to any visitors; and this is reiterated in written information provided about the group.

6. External proceedings

6.1. External auditors accessing family files for quality auditing purposes do so in the presence of the organiser/co-ordinator and sign and date the Record of Access Form on the inside front cover. They will also need to show their organisation's statement of GDPR compliance.

6.2. Where Home-Start is asked by the Police to provide information, the trustees are made aware of the request and Home-Start guidance is followed. Whilst Home-Start would not wish to be obstructive in a police investigation, confidentiality to our service users is of the utmost importance and this will mean that we would normally not pass information to the police unless it fell within one of the exceptions identified in this policy or was subject to an order of a court requiring disclosure.

6.3. If a request for information is made by a legal body, such as a solicitor, Home-Start should contact DAS for advice.

7. Support for families

7.1. Explain to children and families at the outset how and when information will be shared, including within Home-Start. A privacy notice (containing suitable a suitable consent statement) must be signed at this point. See Appendix 3 for an example privacy notice. Such notices will need to be constantly reviewed to ensure they capture sufficient consent to process personal data for the intended purposes.

7.2. Explain that information shared may relate to concerns if they arise but could also be positive information about their progress. Explicit consent will be obtained to share specific information relating to the family, the only exception being where there is a risk of significant harm to a child or serious harm to an adult at risk.
7.3. Consider the protection, safety and welfare of the child as the overriding consideration when making decisions about sharing information with official safeguarding/child protection bodies.
7.4. Wherever possible, however, Home-Start will respect the wishes of children and families when sharing information about them.
7.5. Seek advice if in doubt. This may be from the Scheme's strategic lead, local safeguarding board, your safeguarding special adviser, Home-Start UK.
7.6. Ensure that the information shared is necessary for the purpose for which it is being shared, is shared only with those who need to see it and is accurate and up to date.
7.7. Record the reasons for decisions to share or not share information in the family file.

8. Involving children in decisions about their information

Children in families supported by Home-Start will mainly be young children, but where they are mature enough (normally considered to be 12 or over) they are involved in consenting to sharing or processing information about them (also refer to the 'Consent for Children' section in Appendix 2 below).

9. Training and induction

Staff, trustee and volunteer induction and training includes information on their responsibilities with regard to data protection, record keeping, safeguarding/child protection and promoting the welfare of children. This includes signed and dated confirmation of their understanding and acceptance of this policy, the GDPR policy and the Home-Start code of conduct.

10. Liaising with other agencies

10.1. If as a requirement of funding, families receiving Home-Start's support have to be registered with a Children's Centre, Sure Start in Northern Ireland or in some areas of Scotland as part of a Children's Plan, this will be fully explained to the family at the initial visit and the nature and extent of any information sharing agreed with the family in advance.
10.2. Referrers are informed in writing when Home-Start support starts and the nature of that support, home visiting, group support or a combination of both. They are also informed, again in writing, when Home-Start support ends. With the family's consent they are informed of any changes in the nature of support or the family's circumstances as the relationship with Home-Start progresses.
10.3. **Multi-agency meetings** - Home-Start staff will attend multi-agency meetings with the family's knowledge and consent, and having discussed with them the information that will be shared, with whom and how it will be recorded. The exception being where there are concerns for the safety or welfare of a child or adult at risk and it would not be safe or practical to do so.
10.4. When sharing information about a family it supports, Home-Start adheres to the principle that the information is necessary, proportionate, relevant, accurate, timely and secure. Where professionals unconnected with the particular family are present Home-Start should emphasise the sensitive and confidential nature of the information they are sharing.
10.5. Providing reports for multi-agency meetings - Information provided about a family in a report is factual, accurate, up-to-date and substantiated and should be in writing. The organiser/co-ordinator discusses the contents of the report with the family prior to the

meeting as long as to do so would not increase the likelihood of harm to the child/children/adult at risk.

10.6. **Providing reports for Parents** - Information requested in support of a court case will be provided in witness statement format written by a member of staff, not by a volunteer. The witness statement should be approved by the trustees prior to disclosure.

10.7. **Commissioners of services** - Evidence of positive outcomes for children and their parents is essential to underpin Home-Start funding applications and for accountability purposes. Home-Start retains statistical records of their support for families and children to meet requirements. Home-Start may also, on occasions produce case studies or other information to demonstrate their support to families and to illustrate the positive impact of this support. When doing so all personal, sensitive or identifying information is removed.

11. Record Keeping & Retention Procedure

11.1. Home-Start observes established record retention periods (see Appendix 1) and a process is in place for deleting personal information once it is no longer required.

11.2. Family, volunteer, staff and trustee records are confidential, kept in accordance with Home-Start guidance and stored in a locked filing cabinet. It must be explained at the initial visit/interview/induction that a record is maintained about them and that they have the right to request access to it.

11.3. Records kept are factual, accurate, up to date, signed and dated by the organiser/co-ordinator and/or administrator. Access for this normal maintenance of the file and for supervision purposes is not recorded. A note of all other access for specific purposes must be recorded (giving reason, date and signature) on the data protection access form at the front of the file, including access by the family, a nominated trustee (agreed by the board of trustees) or Home-Start UK for quality assurance purposes.

11.4. Home-Start ensures that all manual or electronic records are password protected/encrypted. All passwords must be complex (containing upper and lower case letters, a number and ideally a symbol) and must be changed regularly.

11.5. Data containing personal information, including family, volunteer or personnel files, is backed up and kept securely.

11.6. Access to personnel files is restricted to the individual's line manager, to trustee/s if appropriate, and to HSUK reviewers for the purpose of Quality Assessment review. There must be a data protection access form attached to each file.

11.7. Care is taken to ensure that families are not identifiable on notice boards, whiteboards, accessible card index files, social media, websites etc.

11.8. Records are securely destroyed in line with this policy (detailed in Appendix 1).

11.9. Statistical information about the number and location of families supported and the type of work undertaken may be shared with funders in line with the requirements of the Service Level Agreement or contract. Information that may identify a family is not shared except with the specific permission of the family.

12. Family files

12.1 The home-visiting volunteer completes the volunteer diary (family contact sheet) after each visit to the family, and returns them at least monthly to the scheme; these are kept in the relevant section of the family file.

12.2 When family support has ceased, the family file will be clearly marked with the expiry date and will be retained and destroyed in strict accordance with the Home-Start Record Retention Periods specified in Appendix 1 of this policy, and will be shredded when the appropriate date is reached. Where it is a requirement of, for example, a funder or local authority to retain files for a longer period this time frame may change.

13. General

13.1. Home-Start complies with the Statement of Recommended Practice (SORP) in relation to its financial record keeping and reporting.

13.2. Home-Start stores insurance policies and employer's liability insurance certificates securely.

13.3. Home-Start stores documents relating to the ownership or leasehold of premises securely.

13.4. As an organisation undertaking DBS/PVG/ACCESS NI checks to help assess the suitability of applicants for positions of trust, Home-Start complies fully with legislative procedures and recommended codes of practice regarding the processing of Disclosures and Disclosure Information.

Signature of Chair: _____ Name: C Read

Date Policy and Procedure adopted: 10th May 2018

APPENDIX 1
RECORD RETENTION PERIODS

Record Retention Periods in Home-Start	
Employment In general the personnel file should be retained for **6 years,** but need only contain sufficient information in order to provide a reference. Copies of any reference given should be retained for 6 years after the reference request. ***Exception:*** *if an allegation has been made about the member of staff or trustee the personnel record should be retained until they reach the normal retirement age or for 10 years, if that is longer.*	
Application form	Duration of employment, shred when employment ends ***Exception: With the same exception as detailed for a volunteer below).***
References received	May destroy 1 year after received, otherwise shred at end of employment.
Passports/Driving Licence/Eligibility to work in the UK	Duration of employment and for a further two years after employment ends.
Sickness records	3 years (i.e. at the end of employment, the previous 3 year's records will be in the file, assuming they have been employed for at least that period of time).
Annual leave records	2 years
Unpaid leave/special leave records	3 years
Records relating to an injury or accident at work	12 years
References given/information to enable a reference to be provided (including sickness records)	6 years from end of employment
Recruitment and selection material	6 months after decision
Disciplinary records	6 years after employment ends
Trustee files	6 years after standing down as trustee ***Exception: With the same exception as detailed for a volunteer below).***
Volunteer files	The volunteer file is retained for 12 months after the volunteer has ceased to be a Home-Start volunteer. Sufficient info in order to provide a reference may be retained. ***Exception:*** *if an allegation has been made about the volunteer, the volunteer file should be retained until the volunteer reaches normal retirement age or for 10 years if that is longer.*
DBS/PVG/ACCESS NI checks/PVG check by Disclosure Scotland and Access NI Checks **Potential Employees and Volunteers:**	Documented record of each as received and satisfactory (or otherwise) then destroy securely in compliance with DBS/PVG/ACCESS NI/PVG Scotland* or Access NI guidance. Disclosure Information will not be kept for any longer than is absolutely necessary once a decision has been made about a potential applicant (staff, volunteer or trustee). Normally this will be for up to a period of 6 months, to allow for the consideration and resolution of any

Record Retention Periods in Home-Start	
Disclosure Information	disputes or complaints. If, in very exceptional circumstances, it is considered necessary to keep Disclosure Information for longer than six months, the scheme will consult the DBS/PVG/ACCESS NI about this and will give full consideration to the Data Protection Act. Throughout this time, the usual conditions regarding safe storage and strictly controlled access will prevail. A record will be maintained of all those to whom disclosures or Disclosure Information has been revealed. ***Disclosure information requested under the PVG scheme:** Under the PVG scheme (Scotland) and in accordance with the Data Protection Act, the original paper or electronic image of the disclosure information will not be retained and should be destroyed in line with the Safe Storage and Handling of Disclosure Information Policy (Scotland). However, prior to disposal of the original document, schemes should record the date of issue, the individual's name, the disclosure type, purpose for which it was requested, the unique reference number and details of the disclosure information. The information recorded by the scheme should be held for the period of time that the employee/volunteer remains in paid or unpaid work for Home-Start.
Family and volunteer records	
Family records, where no safeguarding concern	The family file is retained for 12 months from the date of ending Home-Start support. The file is stored securely and is marked with the date (month/year) it should be destroyed. The file will be securely destroyed at the appropriate date.
Family records, where a safeguarding concern was referred by Home-Start, or the family were subject to a child protection plan or a Child in Need Plan and any files containing a Record of Concern and Action	The family file is retained for 6 years from the date of ending Home-Start support. The file is stored securely and is marked with the date (month/year) it should be destroyed and stored securely. The file will be securely destroyed at the appropriate date.
Volunteer files	The volunteer file is retained for 12 months after the volunteer has ceased to be a Home-Start volunteer. Sufficient info in order to provide a reference may be retained. ***Exception:** if an allegation has been made about the volunteer, the volunteer file should be retained until the volunteer reaches normal retirement age or for 10 years if that is longer.*

Record Retention Periods in Home-Start	
Financial Records	
Financial records	6 years
Payroll and tax information	6 years
Corporate	
Employers Liability Certificate	40 years
Insurance policies	Permanently
Certificate of Incorporation	Permanently
Minutes of Board of Trustees	Permanently
Memorandum of Association	Original to be kept permanently
Articles of Association Variations to the Governing Documents	Original to be kept permanently Original to be kept permanently
Statutory Registers	Permanently
Membership records	20 years from commencement of membership register
Rental or Hire Purchase Agreements	6 years after expiry
Other	
Deeds of Title	Permanently
Leases	12 years after lease has expired
Accident books	12 years from the date of the last recorded accident, see also records of injuries/accidents at work, above
Health & Safety Records	12 years

APPENDIX 2
DATA PROTECTION SUPPORTING GUIDANCE

Data Protection Principles
Current data protection legislation stipulates that anyone processing personal data must comply with six underlying data protection principles. These principles are legally enforceable and set out the fundamental responsibilities of organisations when processing personal data. Home-Start is responsible for, and must be able to demonstrate, compliance with these principles at all times.

The principles require that personal information must be:-

- Collected lawfully, fairly and transparently (data subjects must be able to clearly understand what you are collecting, why, what you will use it for and how long you will keep it and must, where consent is used as the lawful basis for processing, give active consent to this via an 'opt in').
- Obtained for a specified, explicit and legitimate purpose and not processed in a manner incompatible with those purposes.
- Adequate, relevant & limited to what is necessary in relation to the specific purpose for which it is processed.
- Accurate and kept up to date (If are going to hold it, we get liability for ensuring it is up to date).
- Kept in a form where the data subject can be identified only for as long as is necessary e.g. have a specific expiry date which cannot be indefinite and must be communicated to the subject. (We must tell the subject how long we will keep their data and why. After this it has to be erased or anonymised).
- Be processed in a manner that ensures its security (this can mean technically or organisationally but must be documented and there is a specific push around encryption).

Data Controller
This is a person who, alone or jointly with others, determines the purposes and means of the processing of personal data. In other words, the controller decides "what" personal data will be processed "what for" and "how" it will be done.

Data Processor
This is a person who processes personal data on behalf of a controller e.g. a company that processes your payroll or a cloud provider that offers data storage.

Processing of Data
Processing includes anything done with personal data -"*whether or not by automated means*" such as:

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

Personal Information/Data
Any information relating to an identified or identifiable natural person; 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;
- data concerning health, a natural person's sex life or sexual orientation.

The processing of these types of personal data is strictly prohibited unless such processing is on one of a limited number of bases as set out in the GDPR. One of these is that we have obtained "explicit" consent (see 'Consent' section below).

Data Subject
The data subject is the natural person to whom the personal data relates.

Rights of individuals
- Right to be **informed** – informed of their rights under data protection laws in a concise, transparent, intelligible and easily accessible manner, usually through privacy notices
- Right of **access** – subject access requests (see 'Subject Access' section below)
- Right to **rectification** – if data is inaccurate or incomplete
- Right to **erasure** – 'right to be forgotten' – The right to, on request, remove all personal data held about that data subject
- Right to **restrict processing** – right to block processing such that we are only allowed to store enough data about the data subject to ensure the restriction is respected in the future and not to process the data in any other way
- Right to **data portability** – the right for the 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 (see 'Data Portability' section below)
- Rights re: **automated decision making** and **profiling**

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 a express written "opt-in" consent statement which clearly lays out what you are collecting, why, what you will use it for and how long you will keep it.

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 relevant individuals' 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.

Consent from 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).

Subject Access
Home-Start recognises that under the current legislation any individual whose personal data is held by Home-Start has a right to request access to their personal data. Such a request is known as a "Subject Access Request".

Any such request should be made in writing, to the chair/senior worker of the Scheme. If Home-Start receives a Subject Access Request, they must provide the relevant 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 they believe that any information held on them is incorrect or incomplete then they should write to their line manager as soon as possible setting out the information which they believe needs correction.

Data Portability
The data subject's right to data portability:
- only applies to their personal data that has been provided to Home-Start; where processing is based on consent or for the performance of a contract; and when processing is carried out by automated means;
- allows individuals to obtain and reuse their personal data for their own purposes across different services; and
- allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Home-Start must respond to any request made by a data subject to exercise this right within one month and without charge. This can be extended by two further months but only where the request is complex or Home-Start receives a number of requests (Home-Start must still inform the data subject within one month and explain why it requires the extension).

Confidential References
Home-Start is not obliged under data protection legislation to provide, in response to Subject Access Requests made to it, copies of any confidential references about employees (or past employees) written by Home-Start.

Home-Start will make reasonable attempts to gain consent from any such referees.

The Main Responsibilities of each local Home-Start:

- Ensure its compliance with of all of its legal and contractual requirements relating to the processing of information, including but not limited to the six data protection principles set out in the GDPR;
- Ensure personal information (including information falling within the "special categories of data") is processed lawfully and fairly and, through appropriate management and systems, observe fully the conditions regarding the fair collection and use (and all other means of processing) of information.
- Meet its legal obligations to specify the purpose for which the information is used and the length of time it will be held for.
- Collect and process appropriate information only to the extent that it is needed to fulfil operational needs or to comply with legal requirements.
- Ensure the quality of information used.
- Ensure personal information is held for no longer than is necessary for the purpose for which it is processed.
- Map your information flows (document what personal data you hold, where it came from and who you share it with) and continually assess whether consent (or any other basis relied upon from time to time) is the most appropriate lawful basis for processing personal data.
- Amend, and regularly monitor, the contents of 'Privacy Notices' to capture explicit consent to process personal data (where consent is used as the lawful basis for processing) and to provide all the information to the data subject as required under the data protection legislation, including why you need to process their information, how you will keep it secure and those rights detailed in the 'Rights of Individuals' section above.
- Where capturing consent, pay special consideration to the position of children and carefully consider and monitor methods of verifying that a child's consent is authorised by a parent (or equivalent).
- Ensure it has adequate systems, processes and plans in place to meet the principles of data protection by design and data protection by default (such as data pseudo anonymization) and such that data subjects' rights can be fully exercised in accordance with the applicable data protection legislation. These rights include the right to be informed that processes are being undertaken, the right to access one's personal information, the right to prevent processing in certain circumstances, the right to correct, rectify, block or erase information that is regarded as wrong information, the right to data portability, the right of access, the right to withdraw consent to the processing of their personal data and the right to be forgotten.
- Ensure everyone who processes personal information understands they are responsible for following all internal policies and good data protection practice, and has been appropriately trained to do so.
- Ensure all personal data and other confidential information is kept secure at all times, including:
    - Providing all necessary direction and support regarding information security;
    - Establishing a framework to initiate and control information security within the organisation, including establishing and maintaining the measures detailed in the 'Security Compliance' section below;
    - Considering security in the context of human resources, such as screening, contracts and training;
    - Considering communications security, such as sharing data across consortia/ hubs/ mergers;
    - Setting authorisation and access control limits;

    - Identifying organisational assets, defining appropriate protection responsibilities and drawing up guidance on the handling of assets;
    - Ensuring information security is considered throughout the development and maintenance of systems;
    - Setting clear operational procedures and responsibilities for issues such as malware controls, back up procedures and restrictions on software installations; and
    - Carrying out rigorous risk assessments for the transfer and/or transport of information out of the office.
- Ensure media is disposed of securely when no longer required using formal procedures/reputable company (this company should be a registered waste carrier with a certificate of destruction verified by the Environment Agency).
- Ensure robust business continuity and disaster recovery plans are in place and are tested on a regular basis.
- Ensure there are written agreements/contracts in place with all suppliers (to include the minimum contractual requirements set out in the 'Contractors/Third Party Data Processors' section below) and effectively manage any changes to the contractual arrangement.
- Complete and maintain an information risk register, associated data protection impact assessments and a resulting action log.

The Main Responsibilities of Trustees/ Employees/ Volunteers
In addition to contributing to the satisfaction of the Scheme responsibilities above (as relevant to the individual's specific role) and any other role specific responsibilities set out in this policy or the GDPR policy, all trustees/ employees/ volunteers 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 seek guidance from their line manager if they are unclear as to the application of the GDPR to their role.
- Read and comply with the GDPR Policy and this 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 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.

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 failures 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.

Personal Data Breach
A personal data breach is defined under the GDPR as "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).

Any data loss must be reported immediately to the Data Protection Lead who will assess the situation/impact. If it a reportable breach, the Data Protection Lead (in their absence, the Chair) must report the incident to the Information Commissioner's Office/ seek legal advice from DAS and notify Home-Start UK. (Breach Response Flowchart)

Circumstances for notification of breach *-if the breach is likely to result in* ***risk to the rights and freedoms of individuals*** *the Information Commissioners Office (as the supervisory authority) and Home- Start UK should be notified*

- *Without undue delay*
- *Where feasible, not later than 72 hours after becoming aware of it*
- *If data breach* ***likely to result in high risk to rights and freedoms*** *of an individual the controller must also* ***communicate the breach to the individual*** *without undue delay*

Data in Transit

There may be occasions when it is necessary for personal data and other confidential information to be taken outside of the office e.g. if a member of staff is asked to attend a case conference. This includes data in all formats including but not limited to paper or electronic storage (PC's tablets, laptops and removable storage media i.e. USB memory sticks, PDA's or any form of networking equipment). All employees are personally responsible for taking reasonable and appropriate precautions to ensure that such data taken outside of the office is secure at all times. For example, media shall be protected against unauthorised access, misuse or corruption during transportation - this would include encryption of e-mails, computers being password protected and memory sticks being encrypted.

It is not possible to be fully prescriptive in this policy as to the action which should be taken to ensure security as there may be a number of different situations where data may be taken out of the office. It will be necessary for Schemes to rigorously risk assess the means of storing the data and the security measures needed for each individual instance to allow the Scheme to make considered judgements in terms of how they handle data whilst delivering their service. If in any doubt, employees should seek support from their line manager.

When sending information by post, the Scheme must take all steps necessary to ensure the recipient's details are accurate and that only the named person has access to the information.

When sending information via a web portal, the Scheme must ensure there is robust password-protected access control in place and that only the intended recipient has access to it.

Contractors/Third Party Data Processors

Schemes must only use data processors that will:

- Provide "sufficient guarantees" that processing will meet GDPR requirements and ensure the protection of individual rights.
- Undertake due diligence: e.g. satisfy yourself that any data processor adopts appropriate security measures (technology and practice).

- Ensures appropriate safeguards if processing outside EEA (cloud storage may qualify as processing outside EEA).

All contractors who process personal information supplied by Home-Start will be required to confirm in writing that they will abide by the requirements of the applicable data protection legislation (including from 25 May 2018, the GDPR) with regard to all personal information provided and/or accessed via but not limited to paper or electronic storage. Contractors will be required to ensure that they and all of their staff who have access to personal data held or processed for, or on behalf of, Home-Start are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the data protection legislation.

Any third party contractor (e.g. an IT engineer) accessing personal information incidental to their work for the Scheme will sign an undertaking ensuring strict confidentiality will be maintained. Employees and contractors should understand their responsibilities and should be suitable for the roles for which they are considered.

The contracts between Home Start (acting as the data controller) and its processors should include, as a minimum, reference to:

- the subject-matter and duration of processing;
- the nature and purpose of processing;
- the type of personal data being processed and the categories of data subjects;
- the obligations and rights of Home Start as the data controller;
- Home Start's and the processor's responsibilities to maintain a record of processing activity carried out in connection to services being provided under the contract;
- the facility for data subjects to update their personal information (such as renewal forms);
- all staff and representatives receiving a copy of a data protection policy or guide;
- personal data breaches being referenced in the processor's disciplinary policies;
- all staff and representatives being made aware of the consequences of their actions (criminal liability if they knowingly or recklessly disclose personal information); and
- the processor's obligation to:
    - Only act on the written instructions of Home Start;
    - Ensure people processing personal data are subject to a duty of confidence;
    - Take appropriate measures to ensure the security of processing (including but not limited to spot-checks, audits and the security compliance measures discussed below);
    - Only engage sub-processors with the prior consent of Home-Start and under a written contract;
    - Assist Home-Start in providing subject access and allowing data subjects to exercise their rights under the GDPR;
    - Assist Home-Start in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
    - Delete or return all personal data to Home-Start as requested at the end of the contract; and
    - Submit to audits and inspections, provide Home-Start with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell Home Start immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

If a contractor/ third party data processor fails to comply with its contractual requirements relating to data protection, a risk assessment should be carried out and careful consideration should be had as to whether to terminate their contract.

Security Compliance
Schemes should ensure that they audit/monitor security risks and have appropriate security measures (both technical and operational) to protect the security of personal data, such as:-

- office access controls
- use of lockable cabinets
- password and asset control (where an employee leaves or a contract is terminated, ensure that passwords are changed and all organisation assets in their possession are promptly returned)
- encryption/password protection where personal data sent by email
- regularly delete sent emails and restrict server access
- review levels of access to records
- procedures and risk assessments for taking information off-site (e.g. hard copy files/laptops/memory sticks)
- encryption, back-up systems and recovery, regular testing

Right to work documentation
Home Office guidance "An employer's guide to acceptable right to work documents" https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/441957/employers_guide_to_acceptable_right_to_work_documents_v5.pdf has the following 3 steps:-

Step 1 – Obtain **original** versions of one or more acceptable documents
Step 2 – Check the document's validity **in the presence** of the holder
Step 3 - **Make and retain a clear copy of all documents checked** (hardcopy or scanned unaltered copy e.g. jpeg or pdf), and record the date the check was made. "The recommended wording for this is "The date on which this right to work check was made: (insert date & sign)"

A separate manual or record indicating the date copied documents were checked (and by whom) is also recommended (using the same wording) so that it is easily available if requested.

APPENDIX 3
EXAMPLE PRIVACY NOTICE/ CONSENT STATEMENT

Below is an example privacy notice capturing consent for the processing purposes contained within the example. When considering and drafting any privacy notice you should consider the personal data you will be processing, the specific purposes for which you are processing that personal data and to whom you will be sharing personal data (both internally and externally). The example is based on consent being the most appropriate lawful basis for the processing of the personal data in question and its content will be reviewed from time to time as ICO guidance around the GDPR develops over time.

PRIVACY NOTICE and CONSENT STATEMENT

In the course of the scheme and Home-Start UK ("**we**"/"**us**") providing support and friendship to your family and monitoring and evaluating your needs, we collect and hold certain personal information about you. We will only do so with your explicit consent and in accordance with all applicable data protection legislation, including the General Data Protection Regulation.

Information collected

The personal information collected by us will be limited to that which is essential to allow us to provide the support you require and deserve. This will include:

- Names, genders, addresses, telephone numbers and e-mail addresses.
- Employment, immigration statuses, disabilities (such as physical or learning disabilities) and racial/ethnic origins.
- Data concerning health (such as substance abuse, domestic abuse, mental health, depression and pregnancy).
- Details of any ancillary support services/agencies being used by the family (such as family GP, health advisors, social workers, mother & baby clinics, children's centres, CAMHS, CPN/mental health, debt counselling, legal support, employment, housing support, education and dentistry).
- In the case of children, additional information as to whether the child is subject to assessment needs (such as CAF/UNOCINI) or a child care/protection plan, or is a child in need.

We may also collect information from any individual/agency that has referred your family to us.

How we will use your personal information and who it will be shared with

Internal

Our volunteers discuss your support with the appropriate organiser/co-ordinators, who in turn discuss your support with their line managers. Discussions take place in a confidential setting, for the purposes of supervision and to ensure the best possible support to your family. Volunteers meeting together for peer support do not share information that may identify, or breach the confidentiality of your family.

All information provided to our board of trustees for the purpose of assessing the level of referrals, local trends or case studies shall be anonymised.

External

We will, on an anonymised basis, use your personal information to demonstrate the impact of our services. Any case study information shared will always be on anonymised basis unless we have further explicit consent from you.

We will inform funders and your health visitor (and other agencies involved with your family) that you have sought support from us (including the nature and level of such support) and provide them with *[general information*]. In the event your family has been referred to us, we shall share the same information with your referrer (this will include any changes to the support and informing the referrer when the support comes to an end).

We may share your personal information with Home-Start UK for the specific purposes of statistical analysis and the promotion of our work nationally as well as any reporting requirements for funders who support the network on a national level. This will be on a pseudo-anonymised basis (meaning that we will take steps to limit the ability to for your personal information to be identified. This will normally include the anonymization of names and full addresses).

We may share your personal information with our external auditors for quality auditing purposes but only in the presence of your organiser/co-ordinator and only after the auditors have providing us with all necessary written undertakings to preserve the security and confidentiality of your information.

We will share personal information with law enforcement or other authorities if required by applicable law (including, in line with our Safeguarding and Promoting the Welfare of Children/Safeguarding Adults at risks policies, where there are concerns about the safety or wellbeing of a child or adult at risk and it is considered necessary for their welfare and protection).

We will not share your personal information with any other third party without first obtaining your explicit consent.

How long your personal information will be kept

We will keep your personal information after we have finished providing our support to respond to any questions, complaints or claims made by you or on your behalf, to show that we treated you fairly and/or to keep records required by law. We will not keep the information for longer than necessary. We keep different types of information for different lengths of time (further details can be found in our Information Governance Policy which is available on request).

Keeping your personal information secure

We have appropriate security measures in place to prevent your information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality. We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

Your Rights

You have a number of important rights which you may exercise in relation to your personal information free of charge. In summary, those include rights to:

- access your personal information and to certain other supplementary information that this Privacy Notice is already designed to address;
- require us to correct any mistakes in your information which we hold;
- require the erasure of personal information concerning you in certain situations;
- receive the personal information concerning you which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit those data to a third party in certain situations;

- object at any time to the processing of personal information concerning you for direct marketing
- object to decisions being taken by automated means which produce legal effects concerning you or similarly significantly affect you
- object in certain other situations to our continued processing of your personal information; and
- otherwise restrict our processing of your personal information in certain circumstances.

For further information on each of these rights, including the circumstances in which they apply, visit the Information Commissioner's Office ("**ICO**") website at https://ico.org.uk/for-the-public/.

If you would like to exercise any of the rights, please email, call or write to us using the details in 'How to contact us' below, let us have enough information to identify you, let us have proof of your identity and address, and let us know the information to which your request relates.

How to complain

Please report any complaint to the details set out in 'How to contact us' below. We hope we can resolve any query or concern you raise about our use of your information. You also have the right to lodge a complaint with the ICO who may be contacted at https://ico.org.uk/concerns/ or telephone: 0303 123 1113.

How to contact us

Please contact us if you have any questions about this Privacy Notice or the information we hold about you as detailed below:

By signing this form you confirm you have read and understood the contents of this Privacy Notice and Consent Statement and consent to us processing your personal information in accordance with this Privacy Notice. You may withdraw your consent at any time by using the contact details set out in 'How to contact us' above.

Parent(s) signature: ..... **Date:** .....

..... **Date:** .....