Home-Start Network
General Data Protection Regulation Policy

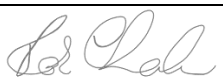
We inspire **growth**

We prioritise **kindness**

We achieve **together**

Document Title	**General Data Protection Regulation Policy (GDPR) (Mandatory)**
Distribution	**For use by Home-Starts UK wide**
Policy Owner	**Assistant Director of Quality and Impact**
Ratified	**May 2023**
Review frequency for local Home-Starts:	**Annually**
Review Cycle	**Annually, or following significant changes in legislation**
Source **Directorate/Department**	**Network Impact**

This is a controlled document. It should not be altered in any way without the express permission of the policy owner or their representative. On receipt of a new version, please destroy all previous versions. If you are reading a printed copy of this document, you should check @Home Intranet website to ensure that you are using the most current version.

POLICY APPROVED BY	
Name:	**Home-Start in Suffolk (Rob Thacker)**
Signed (Chair):	
Date:	**October 25th 2023**
Review Date:	**October 2024**

General Data Protection Regulations (GDPR) Policy

Section	From	To	Date	Reason	By
1.4		Inserted that there should be a trustee who has responsibility for GDPR	Sept 2023 (to allow local Home-Starts to nominate a trustee if they don't have one)	To reflect the requirements of QR Standards	HSUK
Appendix 1	Changes to retention periods and exclusions	Extended periods in cases where there are Safeguarding issues.	April 2023	To comply with legal changes and good practice and to clarify exemptions	HSUK
Appendix 3	Additional detail provided to Subject Access Requests	See section	April 2023	To clarify how to confirm the identity of the person making the request	HSUK

1 Introduction

1.1 Aims and objectives

The lawful and appropriate management of personal data is a legal requirement for Home-Start.

This policy sets our commitment to protecting personal data and how we will implement this with regards to the collection and handling of personal data. The relevant legislation that this policy conforms to can be found in Appendix 2.

Failure to comply with data protection legislation could lead to financial penalties, regulatory action, and reputational damage.

This policy applies to everybody who handles or processes our data. This would include, but not exclusively:

- All Staff, including temporary staff
- Trustees/Advisers
- Volunteers
- Fundraisers
- Consultants

1.2 Legal Aspects

In the UK, data protection law is made up of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. Together, they regulate the collection and use of personal data – information about identified or identifiable individuals. Please note that from January 2021 references to the GDPR should be read as references to the equivalent articles in the UK GDPR (the GDPR in the UK post-Brexit).

1.3 Policy Scope

The policy applies to all personal data that Home-Start holds relating to living identifiable individuals regardless of the category of data or the format of the data. Personal data is any data which could be used to identify a living individual e.g. name, address, email, postcode, CCTV image, photograph and film. Special categories of personal data is any information about racial or ethnic origin, political opinions, religious beliefs, health (mental and physical), sexual health, trade union membership, biometric data, and criminal convictions.

The policy applies to personal data held or accessed on Home-Start premises or accessed remotely via home or mobile working. Personal data stored on personal and removable devices are also covered by this policy.

1.4 Policy Principles

Data protection laws describe how organisations must collect, handle and store all personal data. Ensuring and demonstrating compliance is underpinned by the following principles.

Personal data must be:

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- 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, using appropriate technical or organisational measures.
- The controller (Home-Start) shall be responsible for, and be able to demonstrate compliance with the above principles.

1.4 Responsibility for Compliance

- **Trustees** are ultimately responsible for ensuring that Home-Start meets its legal obligations. There should be a trustee who is nominated to have lead responsibility for GDPR/Data Protection.
- **All staff** have a responsibility for ensuring personal data is collected, stored and handled appropriately and must ensure that it is handled and processed in line with this policy and the data protection principles.
- **The GDPR/Data Protection (DP) Lead** is responsible for monitoring compliance with this policy and the data protection legislation; managing personal data breaches and data subject rights; recording and maintaining appropriate records of processing activities and the documented evidence required for compliance.

1.5 Compliance

Home-Start will comply with our legal obligations and the data protection principles by:

Processing Lawfully and Fairly

Home-Start will ensure processing of personal data, and special categories, meets the legal basis as outlined in legislation. Individuals will be advised on reasons for processing via a freely available Privacy Notice.

Where data subjects' consent is required to process personal data, consent (e.g. use of photos for website/Annual Report) will be requested in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Data subjects will be advised of their right to withdraw consent and the process for Data subjects to withdraw consent will be simple.

Purposes
Personal data will only be used for the original purpose it was collected for. These purposes will be clear to the data subject. If Home-Start wish to use personal data for a different purpose, we will notify, and seek consent from the data subject, as appropriate, prior to processing.

Adequate and Relevant data
Home-Start will only collect the minimum personal data required for the purpose. Any personal data discovered as excessive or no longer required for the purposes collected for will be securely deleted. Any personal information that is optional for individuals to provide will be clearly marked as optional on any forms.

Accurate
Home-Start will take reasonable steps to keep personal data up to date, where relevant, to ensure accuracy. Any personal data found to be inaccurate will be updated promptly. Any inaccurate personal data that has been shared with third parties will also be updated.

Retention
Home-Start will hold data for the minimum time necessary to fulfil its purpose. Timescales for retention of personal data are outlined in the Records Retention Schedule (Appendix 1).
Data will be disposed of in a responsible way to ensure confidentiality and security.

Security
Home-Start will implement appropriate security measures to protect personal data.
Personal data will only be accessible to those authorised to access personal data on a 'need to know' basis.

Employees, trustees and volunteers will keep all data secure, by taking sensible precautions and following the relevant Home-Start policies and procedures relating to data protection.

1.6 Data Sharing

In certain circumstances Home-Start may share personal data with third parties. This may be part of a regular exchange of data, one-off disclosures, or in unexpected or emergency situations.

Appropriate security measures will be used when sharing any personal data.

Where data is shared regularly a contract or data sharing agreement will be in place to establish what data will be shared and the agreed purpose.

Home-Start will consider all the legal implications of sharing personal data prior to doing so.

Data subjects will be advised of any data sharing in the Privacy Notice.

Data Processors
Where Home-Start engage Data Processors (e.g. outside contractors such as suppliers of IT systems, payroll or pensions providers) to process personal data on our behalf, we will ensure:

- Data processors have appropriate technical security measures in place.
- No sub-processors are used without prior written consent from Home-Start in Suffolk
- An appropriate contract or agreement is in place explaining the full requirements of the data processor.

1.7 Security Incident and Breach Management

Occasionally Home-Start may experience a personal data breach; this could be if personal data is:

- Lost, for example via misplacing documents or equipment that contain personal data, through human error, or via fire, flood or other damage to premises where data is stored.
- Stolen; theft or a result of a targeted attack on our network (cyber-attack).
- Accidently disclosed to an unauthorised individual.
- Inappropriately accessed or used.

All security incidents or personal data breaches will be reported and managed by the Data Protection Lead. The Information Commissioner's Office, HSUK (through the Reportable Incident process) and the individuals affected will be notified promptly, if required. All breaches will be managed using the Breach procedures within the Confidentiality policy.

1.8 Individual Rights

Home-Start will uphold the rights of data subjects to access and retain control over their personal data held by us.

Home-Start will comply with individuals:

- Right to be Informed – by ensuring individuals are informed of the reasons for processing their data in a clear, transparent and easily accessible form and informing them of all their rights.
- Right to Access – by ensuring that individuals are aware of their right to obtain confirmation that their data is being processed; access to copies of their personal data and other information such as a privacy notice and how to execute this right.
- Right to Rectification – by correcting personal data that is found to be inaccurate. We will advise data subjects on how to inform us that their data is inaccurate. Inaccuracies with be rectified without undue delay.
- Right to Erasure (also known as 'the right to be forgotten') - we will advise data subjects of their right to request the deletion or removal of personal data where processing is no longer required or justified.

- Rights to Restrict Processing - we will restrict processing when a valid request is received by a data subject and inform individuals of how to exercise this right.
- Right to Data Portability – by allowing, where possible, data to be transferred to similar organisation in a machine-readable format.

- Right to Object – by stopping processing personal data, unless we can demonstrate legitimate grounds for the processing, which override the interest, rights and freedoms of an individual, or the processing is for the establishment, exercise or defence of legal claims.

See Appendix 3 below – Process for responding to Subject Rights Requests, including where exemptions may be applied to withhold certain types of information.

1.9 Privacy by Design

Home-Start has an obligation to implement technical and organisational measures to demonstrate that we have considered and integrated data protection into our processing activities throughout the organisation.

Trustees will be responsible for ensuring a Data Audit is completed and retained, this becomes a Record of Processing required by Article 30 of GDPR.

When introducing any new type of processing, particularly using new technologies, we will take account of whether the processing is likely to result in a high risk to the rights and freedoms of individuals and carry out Data Protection Impact Assessment.

All new policies including the processing of personal data will be reviewed by the Data Protection Lead to ensure compliance with the law.

2. Training

All staff will be aware of good practice in data protection and where to find guidance and support for data protection issues.

Adequate and role specific training will be available regularly to everyone who has access to personal data, to ensure they understand their responsibilities when handling data.

3. Breach of policy

Any breaches of this policy, may be considered under the Home-Start disciplinary procedures, and may result in disciplinary action being taken, including dismissal.

Regular audits will be undertaken to check compliance with the law, this policy and any relevant procedures.

Appendix 1 Retention Periods

Retention Periods in Home-Start	
Personnel files of employees and trustees should be retained for six years after they leave the organisation. *Exception: If there are any allegations against an employee, trustee or volunteer in relation to safeguarding included in the records, this information must be kept on file, including for people who leave the organisation, at least until the person reaches state pension age, or for 10 years if that is longer.	
Application form	For successful candidates – data to be retained for the duration of employment and shredded/deleted when the employment ends. Sufficient information in order to provide a reference may be retained. For unsuccessful candidates – data should be retained for six months.
Shortlisting information	For unsuccessful candidates – should be retained for six months
Staff file* References received Successful candidate shortlisting information Eligibility to work in the UK ** Sickness records Leave records Parental leave References provided Disciplinary records	'Personnel files of employees should be retained for six years after they leave the organisation. With consent from the person to do so, information needed for future references can be kept for longer, as long as consent is renewed from time to time. *Exception: where there is a third party legal involvement, for instance if there are any allegations in relation to safeguarding included in the records, this information must be kept on file, including for people who leave the organisation, at least until the person reaches normal state pension age, or for 10 years if that is longer. ** Evidence used as verification for eligibility to work in the UK should be destroyed once validated – but hold the record that checks have been carried out for the 6 year period past employment
Records relating to an injury or accident at work	12 years
DBS/PVG/ACCESS NI checks	The disclosure form should not be retained, but a record of the DBS number; date of issue of disclosure; level of disclosure; position for which it was requested; summary of decision taken in regard to recruitment; summary of any disputes over accuracy should be retained and whether the disclosure was satisfactory or not should be kept on file.

Retention Periods in Home-Start	
	Details of convictions etc. should be held separately. Only keep a record of whether it was satisfactory or not. DBS information can be held for a minimum of 6 months and maximum of 3 years. Information should only be shared with the recruiting manager (who should be trained in handling data securely) and with governance officers e.g. Safeguarding Trustee/Chair. If there are no issues the information should be destroyed after 6 months. If there are issues the information should be retained up to three years.
Trustee files	Personnel files of trustees should be retained for six years after they leave the organisation. With consent from the person to do so, information needed for future references can be kept for longer, as long as consent is renewed from time to time. *Exception: If there are any allegations against a trustee in relation to safeguarding included in the records, this information must be kept on file, including for people who leave the organisation, at least until the person reaches state pension age, or for 10 years if that is longer.
Volunteer files	Volunteers' records should be retained for two years. With consent from the person to do so, information needed for future references can be kept for longer, as long as consent is renewed from time to time (5 years max). *Exception: If there are any allegations against a volunteer in relation to safeguarding included in the records, this information must be kept on file, including for people who leave the organisation, for 10 years from resigning from the role.
Family files, 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.

Retention Periods in Home-Start	
Family files, where a safeguarding concern was referred by Home-Start to Children's Service (CS), 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	Records which involve child abuse[i] should be held for 75 years in line with The Independent Inquiry into Child Sexual Abuse (IICSA). This includes cases referred to Children's Services by Home-Start when the record should be retained for 75 years. If the record involves children where a (Record of Concern and Action) was referred by Home-Start to Children's Services (CS) but that CS say that the case did not meet the threshold for support from CS records should be retained until the child reaches the age of 25 years old (based on NHS and NSPCC guidelines). Records where a Record of Concern and Action are recorded but where the case is not referred to Children's Service should be retained until the child reaches the age of 25 years old. Records that do not relate to the child abuse but that relate to the family are retained for standard retention period (7 years) from the date of ending Home-Start support. Records should be stored securely and is marked with the date (month/year) by when should be destroyed and when this time is reached should be securely destroyed. NB – a service could retain data for a longer period (further five years) if the data subject (DS) gave their consent to retain records. NB: exceptions could be managed by Data Protection Impact Assessment (DPIA), approved by the Local Home-Start board. NB : where there is a third party legal involvement, for instance if there are any allegations in relation to safeguarding included in the records, this information must be kept on file, until 7 years past legal proceedings
Financial Records	
Financial records	Six years
Payroll and tax information	Six years

Retention Periods in Home-Start	
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	10 years after the person leaves
Rental or Hire Purchase Agreements	Six 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 – Legislation

The legislation that the policy conforms to:

- UK General Data Protection Regulation (UK GDPR)
- UK Data Protection Act 2018 (DPA 2018)
- Privacy and Electronic Communications Regulations (PECR)

Appendix 3 - Subject Access Request Checklist and Log
Please note-THIS RELATES TO REQUESTS FROM INDIVIDUAL CLIENTS (THE DATA SUBJECT) AND NOT FROM ORGANISATIONS

Individual:
Date of Request:

	1.4.1.1 Action	**Date**	**Staff**
A	An individual requests personal data **(one month starts here)**	1.4.2 DD/MM/YYYY	
B	Data Protection lead informed	*DD/MM/YYYY*	
C	Subject Access Form sent to individual (if appropriate) ***(proof of ID & clarify type of data required)*** Subject Access Form sent to individual (if appropriate) • *Proof of ID 30 days starts from here.* • *Clarify type of data required* *Time starts from proof of ID*	*DD/MM/YYYY*	
D	Subject Access Form returned	*DD/MM/YYYY*	
E	DP & senior staff break down request into manageable strands *(identify parameters to search that would satisfy criteria of the request)*	*DD/MM/YYYY*	
F	**Locate data.** Use DPIA or Record of Processing to help find where, who, how data is stored (which systems)	*DD/MM/YYYY*	
G	**Conduct searches**. This may include: • Email accounts / mailboxes / Office 365 • Saved files and folders • HR/Finance systems • Data Management systems • Client/Family files – electronic or paper • Hard-copy paperwork (drawers, folders, letters, notebooks) • Speaking to staff Keep log of searches conducted within all systems	*DD/MM/YYYY*	
H	**Collate data** (from all sources) • File data extractions into secure electronic folders • Home-Start may need to print material • Order material (by date or source)	*DD/MM/YYYY*	
I	**Analyse data** - Risk, retention and judgement undertaken on material: **Removal of data** • Duplication (e.g. Cc/Bcc emails) • Any information not related to request Establish if any exemptions should be applied (see below**)	*DD/MM/YYYY*	

	Authority • Have you got authority from relevant people? • 3rd party compliance sought? 2 Redaction • Does it contain personal information about other individuals? • Any other exempt information to be redacted?		
J	2.1 Format data • Printed/hard-copy documents to be scanned back in • Accurately label and number all files/folders • Consider encryption / password-protect / back-up of information	*DD/MM/YY YY*	
K	2.2 Final checking • Authorisation confirmed to pass over data (Chair/DP lead) • Approval gained on an appropriate response/letter	*DD/MM/YY YY*	
L	**Data transfer (to subject)** • Check with subject how they want to receive data extracted • **Analyse risks** associated with using post, email, shared folders, USB sticks and other formats of data sharing	*DD/MM/YY YY*	
M	2.3 Provide data • Supply information requested by the subject • Explain any exemptions that have been applied • Ensure communication includes right to reply	*DD/MM/YY YY*	

** The Data Protection Act 2018, allows some personal data to be exempted from disclosure under a Subject Access Request. Please see the ICO's guidance on exemptions at (Exemptions | ICO).

Common exemptions likely to apply to personal data held by Home-Start are:

SCHEDULE 2, PART 3, 16 – Protection of the rights of others [Data Protection Act 2018 (legislation.gov.uk)]

Information about individuals other than the data subject making the request is likely to be exempt unless they have provided their consent for their specific personal data included in the request, to be released to the requester.

[What should we do if the request involves information about other individuals? | ICO]

SCHEDULE 3, - Information relating to health, social work, education or child abuse [Data Protection Act 2018 (legislation.gov.uk)]

Under the Data Protection Act 2018, Home-Start, as a charity working to support children and families, is permitted to apply the health, social work, education and child abuse exemptions, where it is considered that releasing the personal data to the data subject making the request has the potential for serious harm to that data subject. Before applying this exemption, the data protection

lead should read the below guidance from the ICO and ensure that all aspects have been considered.
[Health, social work, education and child abuse information]

[ii] The definition of child abuse, any act against a child, psychological or physical that harms or damages the child