General Data Protection Regulation (GDPR) and Confidentiality Policy



Home-Start _____ (hereafter called Home-Start)

Title	**General Data Protection Regulation (GDPR) and Confidentiality Policy (Mandatory)**	09/10/2024
Author	Tanya Samuels HSUK Quality Specialist with support from RGDP (Data Protection consultant)	
Approver	Impact Sub committee	21/10/2024
Owner	Director of Network Impact	
Published	Published on @Home	24/10/2024
Review frequency	Two years	
Next publication date		24/10/2026

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.

This policy adopted: 19/3/26 **(date)**

Date policy to be reviewed: MAR '27 **(date)**

Signed (Chair) A. Allen **Name:** ANDREA ALLEN

Below is a list of policies and documents that are also relevant to Data Protection. You may find it helpful to refer to any of these additional documents when reading and using this policy.

- Safeguarding and Protecting Adults
- Safeguarding and Protecting Children (UK wide)
- Reporting Serious Incidents and reputational threats to HSUK
- There are a number of resources, training materials and templates available to support GDPR available on @Home https://at.home-start.org.uk/Interact/Pages/Content/Document.aspx?id=6494&SearchId=0
- Record Retention table (Appendix 1)

Policy Statement

The lawful and appropriate management of personal data is extremely important to Home-Start [add name]

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:

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

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.



The Data Protection Principles

- Those who share sensitive personal information with Home-Start have a right to expect that it will be treated as confidential

- Personal and confidential information in any form obtained by Home-Start will be handled in compliance with data protection law and only in the ways relevant to the purpose of providing support as set out in our Privacy Notice.

- Access to the information we hold is limited to those who have a genuine need to see and use it in order to fulfil their roles in delivering our service.

- Everyone who works for or with Home-Start understands their duty to maintain the confidentiality and relevance of information that is shared with or by them and the consequences of breaching that confidentiality.

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 insert name) shall be responsible for, and be able to demonstrate compliance with the above principles



Responsibilities for compliance

Trustees are ultimately responsible for ensuring that Home-Start meets its legal obligations in terms of:

- being fully committing to the principles of confidentiality and the management and security of information they receive in the course of their duties
- being responsible for ensuring that everyone in Home-Start understands and is committed to maintaining confidentiality
- ensuring that dated and signed records are kept of where access to sensitive information is required along with the reasons for that access
- ensuring that procedures are in place that mean that the information collected is only what is needed to deliver the service, that it is kept securely in whichever form it takes and is only available to those who need to know (see Data Protection policy)
- ensuring that procedures are in place for sharing information securely and in line with the Privacy Notice
- being responsible for dealing with any breach of confidentiality including, if necessary, ending an individual's association with Home-Start, reporting breaches to the relevant authority and Home-Start UK, and cooperating with any investigation/ prosecution.

Home-Start [insert name] has a **trustee with lead responsibility for GDPR** who is responsible for monitoring compliance with this policy and the data protection legislation; supporting the Data Protection Lead at Home-Start [insert name] and providing assurance to the board that GDPR practice is compliant with policy.

All staff have a responsibility for ensuring personal data is collected, stored and handled appropriately and handled and processed in line with this policy and the data protection principles in terms of:

- following the principles set out in the policy and the associated Privacy Notice in all their work
- maintaining the confidentiality and security of all their records in line with our Data Protection policy
- ensuring that information they hold about others and information they provide about themselves is accurate, up to date and only what is needed to provide the service
- recognising that everyone involved with Home-Start has a right to confidentiality
- following the systems and procedures to maintain confidentiality including when sharing with other agencies where there are concerns about the safety or wellbeing of a child or



adult at risk or individuals within the family. Individuals do not need to be informed that their information is being passed onto the relevant authorities if telling them has the potential to cause further harm, or may jeopardise any investigation by Police, Social Care services or other agencies with legal investigatory powers

- knowing and following the procedures for dealing with a request for information from the police, courts or other agencies with legal powers to collect information

- being aware that breaches of confidentiality are serious matters and could result in disciplinary action, including dismissal or potential prosecution.

Home-Start [insert name] has a **Data Protection (DP) Lead** who 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.

Volunteers Responsibilities:

- making sure they understand and follow the principles of confidentiality and understand the limits around what information is collected and shared (set out in the Privacy Notice and Data Protection policy) and follow the procedures put in place by Home-Start to maintain that confidentiality

- being careful not to discuss families they support in ways that would identify them to others, making sure that any information they record about their families is held securely and is destroyed as soon as support is ended in line with our Data Protection policy

- knowing that breaches of confidentiality are serious and could result in ending their volunteering role and could make them liable to prosecution.

Compliance

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

Processing Lawfully and Fairly

Home-Start [insert name] 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 [insert name] 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 [insert name] 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 [insert name] 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 [insert name] will hold data for the minimum time necessary to fulfil its purpose. This applies to personal information stored electronically, including images. 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 [insert name] 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.

Data Sharing

In certain circumstances Home-Start [insert name] 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 [insert name] 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.

Further information and resources are available to support with this on @Home

Data Processors

Where Home-Start [insert name] 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 [insert name]
- An appropriate contract or agreement is in place explaining the full requirements of the data processor.

Security Incident and Breach Management

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

- Lost, for example 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 GDPR/Confidentiality policy.

Further information and resources around data breaches can be found on @Home.

Individual Rights

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

Home-Start [insert name] 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 @Home for further resources on the process for responding to Subject Rights Requests, including where exemptions may be applied to withhold certain types of information.

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.

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.

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.

Retention Periods are shown below. The table shows where there is a legal requirement for a retention period or a recommendation based on best practice in the sector. Legal requirements must be followed, and we strongly recommend that best practice should be followed. If a Home-Start is unsure about GDPR issues they should contact DAS, the ICO or seek advice from a legal firm or agency specializing in data protection. Decisions to deviate from the recommended retention periods should be risk assessed, discussed with the DPO and trustee with lead responsibility for GDPR and the wider trustee group and decisions recorded in minutes of board meetings. In situations where a Home-Start [insert name] has to close specialist guidance will be obtained to ensure that a balance is achieved between the risk of safely retaining important data against the risk of breaching data protection principles.

Appendix 1

Staff files

	Details	Retention Period	Legal/Best Practice Basis	Source	Exceptions
Application form And shortlisting information	**Successful candidates** retain files for the duration of employment and shred/delete when employment ends following retention periods. Sufficient information retained to provide a reference	1 yrs after leaving employment	Best Practice	Chartered Institute of Personnel Management Guidance (CIPM)	
Application form and shortlisting information	**Unsuccessful candidates**	Retention should be no more than 6 months	Best Practice	CIPM	
DBS/PVG/NI Access in NI	Retain the DBS/PVG/Access NI number, date issued, disclosure level, role/job description for, summary of decision taken regarding recruitment and any disputes over accuracy. The employer should not retain the disclosure certificate or detail (convictions etc. from it) only a record or whether satisfactory or not.	6 years after leaving employment	Legal Requirement	DBS/Disclosure Scotland/Access in NI	

Staff file* Training References Disciplinary Sickness		6 years after leaving employment 6 years * until they reach their normal retirement age or for 10 years – whichever is longer[1]	Best Practice Legal Requirement	Information and Records Management Society (IRMS) Department of Education The Statutory Sick Pay (General) Regulations 1982 (SI 1982/894) as amended Professional Standards Agency Limitations Act 1980	*If concerns have been raised about an adult's behaviour around children, the general rule is that organisations should keep the records in their personnel file at least
Injury at work		3 years	Legal Requirement	RIDDOR Limitation for legal proceedings RIDDOR 1995 and Limitation Act 1980. Special rules apply concerning incidents involving fractures, burns, sight loss, crush and amputation)	

[1] NSPCC Child Protection Records Retention and Storage Guidelines chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://learning.nspcc.org.uk/media/3324/child-protection-records-retention-and-storage-guidelines_june_2023.pdf

Trustee Files

Document	Details	Retention period	Legal/Best Practice basis	Source	Exceptions
Trustee files	Including references, induction, training etc.	6 years after leaving the trustee role *Until the person reaches normal retirement age or for 10 years whichever is longer[2]	Best Practice	CIPM	*If concerns have been raised about an adult's behaviour around children
DBS/PVG/NI Access in NI	Retain the DBS/PVG/ Access NI number, date issued, disclosure level, role/job description, summary of decision taken in regard to recruitment and any disputes over accuracy. The employer should not retain the disclosure certificate or detail (convictions etc. from it) only a record or whether satisfactory or not.	6 years after leaving LHS	Legal Requirement	DBS/Disclosure Scotland/Access in NI	

[2] For example,

- if the person is 60 when the investigation into the allegation is concluded, keep the records until their 70th birthday
- if the person is 30 when the investigation into the allegation is concluded, keep the records until they are aged 65.

Volunteer Files

Document	Details	Retention period	Legal/Best Practice basis	Source	Exceptions
Volunteer File	Individual volunteer files, including record of recruitment, references, training	6 years after leaving Home-Start *Until the person reach their normal retirement age or for 10 years – whichever is longer[3]	Best Practice	CIPM *(IRMS, 2019; Department for Education,2022)	*If concerns have been raised about an adult's behaviour around children.
DBS/PVG/NI Access in NI	Retain the DBS/PVG/ Access NI number, date issued, disclosure level, role/job description, summary of decision taken in regard to recruitment and any disputes over accuracy. The employer should not retain the disclosure certificate or detail (convictions etc. from it) only a record or whether satisfactory or not.	3 years after leaving Home-Start	Best Practice	DBS/PVG/NI Access	
Injury volunteering		3 years	Legal Requirement	RIDDOR Limitation for legal proceedings	

[3] For example,

- if the person is 60 when the investigation into the allegation is concluded, keep the records until their 70th birthday
- if the person is 30 when the investigation into the allegation is concluded, keep the records until they are aged 65.

				RIDDOR 1995 and Limitation Act 1980. Special rules apply concerning incidents involving hazardous substances.	

Family Files

Document	Details	Retention period	Legal/Best Practice basis	Source	Exceptions
General files	Family file is retained for 12 months from the date of ending HS support. Date for disposal should be added to file	12 months 6 years. Best practice indicates that files should be retained for 6 years after leaving the service. *If there are concerns about child abuse and neglect the general rule is that records should be retained until the child reaches the age of **25 years** in England, Scotland and Wales. ** In the case of child sexual abuse the records should be	Minimum Best Practice Best Practice	*NSPCC[5]	*In Northern Ireland if there is child abuse records should be retained until the child's 30th birthday

[5] NSPCC Child Protection Records Retention and Storage Guidelines chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://learning.nspcc.org.uk/media/3324/child-protection-records-retention-and-storage-guidelines_june_2023.pdf

		retained for **75 yrs**. Failure to keep and hold records if they are required for an investigation into child sexual abuse is breaking the law . Destroying those records may be consider as perverting the course of justice and can lead to prosecution and custodial sentence of the LHS trustees[4]		**The report from the Independent Inquiry into Child Sexual Abuse [IICSA]. NSPCC describe this as a 'must' equivalent to legal obligation. The IICSA recommend that ICO make this a legal requirement	

[4] If a Home-Start has to close the organisation should seek specialist advice about how to retain records for extended periods

Financial Records

Document	Details	Retention period	Legal/Best Practice basis	Source	Exceptions
Financial Records		6 years	Legal Requirement	Companies Act Section 388 recommends 3 years. Taxes Management Act 1970 (TMA) Sec.20 (Taxes Management Act 1970) may require any documents relating to tax over 6 (plus) years	
Tax and Social Security	Payroll, P45, P60, expenses	6 years plus current year	Legal Requirement	Income Tax (PAYE) Regulations 2003 (SI 2003/2682 Reg 97). The Income Tax (employments) Regulations 1993 (SI 1993/744) and amended 1996. Taxes Management Act 1970	
Pensions	Home Start records	6 years	Best Practice	Pensions regulator CIPM	
Employers Liability Certificate		40 years	Best Practice	2008 regulations removed requirement to retain for 40 years but need to be mindful of 'long tail' industrial disease claims, etc.	
Insurance policies		Permanently[6]	Legal Requirement	Limitation can commence from knowledge of	

[6] If a Home-Start has to close legal advice should be sought on retention periods

				potential claim and not necessarily the cause of the claim.	
Certificate of Incorporation		Permanently[7]	Legal Requirement	S.15 Companies Act 2006	
Minutes of Board of Trustees		Permanently	Legal Requirement	S.356 Companies Act 2006	
Memorandum of Association		Original to be kept permanently	Legal Requirement	S.356 Companies Act 2006	
Articles of Association		Original to be kept permanently	Legal Requirement	S.32 Companies Act 2006	
Statutory Registers		Permanently	Legal Requirement	Companies Act 1985/1984/2006	
Membership records		6-10 years after the person leaves	Legal Requirement	Companies Act 2006	
Rental or Hire Purchase Agreements		Six years after expiry	Legal Requirement	Limitation act 1980	
Deeds of Title		Permanently	Best Practice	HMRC guidance	
Leases		15 years after expiry	Best Practice	HMRC guidance	
Accident books	Injuries & accidents at work,	3 years	Best Practice	Statutory retention period: 3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21). (See below for accidents involving chemicals or asbestos).	

[7] If a local Home-Start has to close legal advice should be sought on retention periods

				Statutory authority: The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and Limitation Act 1980. Special rules apply concerning incidents involving hazardous substances (see below).	
Health & Safety Records		3-6 recommended	Legal Requirement	RIDDOR Limitation for legal proceedings RIDDOR 1995 and Limitation Ac 1980. Special rules apply concerning incidents involving hazardous substances.	

Appendix 2 – Legislation

The legislation that the policy conforms to:

- UK General Data Protection Regulation (UK GDPR)
- UK Data Protection Act 2018 (DPA2018)
- Data Use and Access Act (2025)
- Privacy and Electronic Communications Regulations (PECR)

Version Number	Summary of changes made	Authorised by	Date issued
V3	This policy combines the Confidentiality Policy with GDPR Policy	Director of Network Impact	Oct 2024
	Previously the policy was reviewed annually but this has now changed to be reviewed every two years	Director of Network Impact	Oct 2024
	Previously this policy included an appendix for Subject Access Request forms but this has been removed because HSUK will include a greater range of resources that will be uploaded onto @Home and this will be included here	Director of Network Impact	Oct 2024
	The retention period has been changed to show what is a Legal Requirement and what is Best Practice (which HSUK recommend that Home-Starts should follow), but if a Home-Start chooses to deviate from Best Practice we suggest this is discussed with trustees and recorded in trustee meetings	Director of Network Impact	Oct 2024