Home-Start Bradford District

DATA PROTECTION POLICY

Policy Statement

Home-Start Bradford District ("Home-Start") is committed to the protection of the rights and freedoms of individuals in accordance with the provisions of the Data Protection Act 1988 (the Act). We will comply fully with the requirements of the Act and will follow procedures which aim to ensure that all persons who have access to any personal data held by or on behalf of Home-Start are fully aware and abide by their duties and responsibilities under the Act.

In order to operate efficiently, Home-Start collects and uses information about its staff and about people with whom it works. These may include current, past and prospective employees, volunteers, trustees, families and donors.

Home-Start will ensure that all personal information is handled and dealt with properly however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means. All staff and volunteers having access to personal data will be required to adhere fully to the Act in carrying out their duties for us.

The trustees of Home-Start have overriding responsibility to ensure that this policy is implemented and have appointed a data protection officer – Yvonne Lowe* as the designated person special responsibility for data protection in Home-Start.

It is recommended that the data protection officer is a trustee

Procedure

What does the Act govern?

The Act relates to the processing of personal data and sensitive personal data which must be processed in accordance with the eight data protection principles.

Processing is a wide ranging activity that includes obtaining, recording, holding or storing personal data and carrying out any operations on it such as adaption, alteration, use, disclosure, transfer, erasure and destruction.

Personal data is data which relates to a living individual who can be identified from those data or from those data and other information which is in the possession of, or is likely to come in the possession of, the organisation and includes any expression of opinion about an individual. It includes information relating to an individual's name, date of birth, address and photographs.

Sensitive personal data is defined as personal data consisting of information as to racial or ethnic origin, political opinion, religious or other beliefs, trade union membership, physical or mental health condition, sexual life and criminal proceedings or convictions. Sensitive personal data has even greater conditions for processing and normally in order to process the information it will be necessary to have the explicit consent of the individual.

The Eight Data Protection Principles

The Act stipulates that anyone processing personal data must comply with eight principles of good practice. These principles are legally enforceable.

The principles require that personal information must be:-

- Fairly and lawfully processed.
- Obtained for specified purposes and not processed in a manner incompatible with those purposes.
- Adequate, relevant and not excessive for the purposes for which it is processed.
- Accurate and kept up to date.
- Not kept for longer than necessary for the purposes.
- Secure.
- Not transferred to countries without adequate protection.
- Processed in accordance with the data subject's rights.

The Responsibilities of Home-Start

Home-Start will ensure that personal and sensitive information is processed lawfully and fairly and will through appropriate management and systems:-

- Observe fully the conditions regarding the fair collection and use of information
- Meet its legal obligations to specify the purpose for which the information is used.
- 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 the information is held for no longer than is necessary
- Ensure that the rights of people about whom information is held can be fully exercised under the Act. These 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 and to correct, rectify, block or erase information that is regarded as wrong information.
- Ensure that everyone managing and handling personal information understands that they are responsible for following good data protection practice and is appropriately trained to do so.
- Ensure that personal information collected or used is secure.

The Responsibilities of Employees

All employees are required to:-

- Familiarise themselves with the provisions of the Act and ensure that they understand their responsibilities under the Act in relation to personal information they may process in their role.
- Ensure that they seek guidance from their manager if he or she is unclear as to they application of the Act.
- Access all training provided by Home-Start in relation to data protection.
- Ensure that any information they provide in connection with their employment is accurate and up to date.
- Inform Home-Start of any changes to information that they have provided, eg, changes of address, either at the time of appointment or subsequently.
- Ensure that personal data collected or used is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:-

- Paper files and other records or files containing personal or sensitive data are kept securely.
- Personal data held on computers or computer systems is protected by the use of secure passwords which should be such that they are not easily compromised.
- Personal information is not disclosed either orally or in writing or via web pages or by any other means accidentally or otherwise to an unauthorised third party.

If an employee discloses personal data in breach of the principles set out in the Act, he/she may be committing a criminal offence and he/she may be subject to disciplinary action.

Data in Transit (See Appendix A)

There may be occasions when it is necessary for sensitive and personal data to be taken outside of the office eg if a member of staff is asked to attend a case conference. This includes data in all formats-non-electronic (paper) and electronic (eg on PC's tablets, laptops and removable storage media- i.e. USB memory sticks, PDA's etc). ,All employees are personally responsible for taking reasonable and appropriate precautions to ensure that all sensitive and confidential data taken outside of the office is secure.

It is not possible to be prescriptive in this policy and procedure 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 each individual taking data out of the office to assess the security measures needed for every situation and make considered judgements in terms of how they handle data whilst delivering their service; and if in any doubt seek support from their line manager.

Any data loss must be reported immediately to the employee's line manager who will assess the situation and impact and agree the necessary action with the Data Protection Officer.

Contractors

All contractors who are users of personal information supplied by Home-Start will be required to confirm that they will abide by the requirements of the Act with regard to the information supplied by Home-Start. 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 Act.

Subject Access

Home-Start recognises that under the Act any person whose personal data is held by Home-Start has a right to request access to her or her personal data. Such a request is known as a "Subject Access Request."

An **employee** may request details of personal information which Home-Start holds about him or her. If an employee would like a copy of any of the information held on him or her they should notify their line manager. If an employee believes that any information held on him or her is incorrect or incomplete then they should write to their manager as soon as possible setting out the information which they believe needs correction.

A person (other than an employee) whose personal information Home-Start holds, or who believes Home-Start may hold, may make a Subject Access Request in writing, to the chair of the scheme, for a copy of the information held on him or her.

Home-Start will respond to all requests for personal information within 40 days of the request.

Confidential References

Copies of confidential references about employees written by Home-Start will not be provided in response to Subject Access Requests, as provision of copies of such references are exempted under the Act.

Confidential references about employees received by Home-Start are not exempted. Home-Start will make reasonable attempts to gain consent from referees prior to release. If consent cannot or will not be given Home-Start will permit release if satisfied that to do so would not prejudice the interests of the referee.

Notification to the Information Commissioner

Home-Start will notify as appropriate the Information Commissioner of its processing of personal data and ensure the updating of the information

Signed ..... Chair Home-Start Bradford District

Date .....

Review Date November 2014

Home-Start Bradford District

Appendix A - Moving or Sending Sensitive Data (data in transit) Guidance

Data in transit
This guidance will be subject to regular review and amendment as measures taken in respect of security become more advanced. Schemes will need to amend and make additions to this guidance as is appropriate to their scheme.

There are some common sense precautions which should be taken before sending or taking sensitive or confidential data outside of the office. These are:

1) Checking that more detail than is necessary is not being sent/taken i.e. will the information still meet the need if you remove the sensitive material or aggregate the data?
2) Checking that the data is correct and appropriate.
3) Checking that it is being sent to the correct person/address.
4) Risk assessing the measures proposed to keep it secure

If transferring sensitive or confidential data through a web portal you must:

1) Ensure that there is robust access control in place (i.e. unique username/password)
2) Ensure that only the people who need the data can see them

If taking data on a mobile storage device, such as a tablet PC, laptop or a USB memory stick, they must be encrypted and you must:

1) Make sure that there is no other more secure option available to you
2) Take only as much as necessary, for as long as necessary and transfer them back to their normally secure location as soon as possible
3) Keep the decryption password/token securely and separately from the device/data
4) Take all reasonable precautions to keep the device and data safe and secure eg:
    - Keep it with you whenever possible; lock it away securely when you can't
    - Never leave it in plain sight in public places
    - Never let others use your access or device
    - Delete the data from the device as soon as possible
    - Report loss/theft immediately

Post
The postal service is considered reasonably secure for small amounts or low impact data (i.e. records pertaining to an individual, but NOT including very sensitive personal data) There are precautions that must be taken to prevent loss:

1) Make sure that the recipient and destination address is correct, accurate and up-to-date
2) Clearly mark the envelope/parcel with a return address in case of incorrect delivery
3) Do not send the only copy of the data if it is practical to make and retain a duplicate. You must assess the impact of loss of the original and make a copy if that impact is unacceptable
4) If you use a courier they must be known and trusted
5) Make sure it is traceable (i.e. confirmation of receipt)
6) Physical records must be sent in a suitable container i.e. robust and secure enough to prevent accidental loss and/or tampering

Home PC/laptop

If you are working at home on your own PC or laptop you must:

1) Only have as much sensitive or confidential information open as necessary and only for as long as necessary – do not save the data on your machine and do not leave the screen open when you are not actively working on it
2) Always save the data back to their normally secure location when you have finished
3) You must not leave the computer unattended for any period of time such that others can access any sensitive data; always lock the computer or log out when you are not using it.

Physical (Paper) Records

If you are taking sensitive or confidential information with you in non-electronic (paper) records you must:

1) Make sure that there is no other option available to you
2) Never take the only copy with you if it is practical to make and retain a duplicate. You must assess the impact of loss of the original and make a copy if that impact is unacceptable
3) Take only as much as necessary and only for as long as necessary
4) Transfer it back to its normally secure location as soon as possible
5) Take all reasonable precautions to keep the records safe and secure e.g.:
   - Keep them with you whenever possible; lock them away securely when you can't
   - Use a suitable container that prevents accidental loss and/or viewing by others
   - Never leave them in plain sight in public places
   - Report loss/theft immediately

Fax

Sending sensitive or confidential information by fax is a last resort and should only be used if the need is urgent and there is no alternative available and you must:

1) Make sure the receiving fax machine is in a secure environment
2) Make sure the recipient is there to receive it at the time of arrival and that they are known and trusted
3) Make sure it is traceable (e.g. confirmation of receipt