

Main/Registered Office: Signposts, 58 Regent Road, Morecambe, LA3 1TE

Telephone : (01524) 419021

Fax : (01524) 411541

Community
Legal Service



Help Point



E-mail: signpostsmarc@signposts.org.uk

Website: www.signposts.org.uk

**“Working to Empower the Community”
in Lancashire and Cumbria**

Pamela Beswick - Chief Executive Officer

Data Protection Policy

The purpose of this document is to ensure that everyone working within or using Signposts has a clear understanding of the storing of personal information and the requirements of the Data Protection Act 1998.

In line with Signposts Confidentiality Policy, the Data Protection Policy ensures that where personal information is stored about clients that this is kept confidential and high standard of handling personal information is upheld.

Signposts Confidentiality Policy outlines where information including personal data from case work will be shared with others. Extract from Confidentiality Policy:

Signposts have a complicated management structure in that it is a Multi-Agency Resource Centre and offers both its own services and provides a base for other agencies to offer services. Enquirers need to be confident that information will not be passed inappropriately by one agency to another. The only exceptions to this are outlined as:

Although there is not a legal duty to do so, Signposts workers are authorised to speak to a third party where a person or third-party are at risk and in immediate danger. If a worker feels that action needs to be taken, they should discuss this with their line manager. If their line manager cannot be contacted then they should contact the member of staff on Strategic Duty – indicated on the location sheets. The situations where action may be required are:

- i) Where the person is clearly not in control of his or her own safety i.e. involved in an accident, suffering from a drug overdose.
- ii) Where the emotional or mental state of the person concerned is such that it puts their own, or a third parties lives or safety at risk.
- iii) Where a third party is at risk of danger or abuse e.g. where a sibling is left with the family and being abused.
- iv) Where the work falls within Signposts' Child and Vulnerable Adult Protection procedures

Charity Registration Number: 1117645
Member of AdviceUK (previously FIAC)

Company Limited by Guarantee: 5990592
Registered in England and Wales



North Lancashire
Teaching Primary Care Trust



INVESTOR IN PEOPLE

Additional major funding from Preston City Council, the FC Scott Charitable Trust and Tudor Trust

Signposts offer confidentiality to enquirers. All information received will be respected and the rights of the individual will be paramount. Signposts consists of a team of paid staff and volunteers together with substantive workers from other agencies who will be designated as part of the team. Information received by an individual worker can be shared with that team on a need-to-know basis. Confidentiality is to the team and not to the individual. However, workers should be careful to discuss enquiries appropriately in a way that would put the rights of the individual first.

Data Protection Act 1998

The Data Protection Act aims to promote high standards in the handling of personal information and so protect the individuals right to privacy.

The Act applies to organisations holding information about living individuals in electronic format and, in some cases, on paper. They must follow the eight data protection principles of good information handling which say that that personal information must be:

- Fairly and lawfully processed
- Processed for specific purposes
- Adequate, relevant and not excessive
- Accurate and, where necessary, kept up to date
- Not kept for longer than is necessary
- Processed in line with the rights of the individual
- Kept secure; and
- Not transferred to countries outside the European Economic Area unless the information is adequately protected.

The Act covers any information that relates to living individuals which is held on computer or on paper files. For example, this may include information such as name, address, date of birth and opinions about the individual or any other information from which the individual can be identified.

The information covered by Signposts Data Protection policy includes:

- Case work database
- Signposts database
- Email Communication within the Organisation
- Paper information with individual's personal details (referral and application forms)
- Enquiry notes and telephone messages
- Staff and Volunteer Personal files
- Email communication to third parties

Routine requests from individuals

Routine requests for information from clients and staff about their own files will be given provided they are identified as being the actual person. This will be done by asking for person's date of birth and/or address which can be checked against the file.

Appendix One outlines some good practice examples of how to protect information.

Information relating to personal details or case work information on file will be treated as formal requests.

Formal Requests from Individuals

Individuals have a right under the Data Protection Act to get a copy of the information Signposts holds about them on computer and in some manual filing systems. This is known as the right of subject access.

Any subject access request will be responded to within 40 days and when reasonable identification of the requester has been achieved. All formal information requests should be referred to line managers and the final agreement and content of the information will be identified and processed by the Strategic Management Team.

Signposts team structure can be found on the website www.signposts.org.uk

Requests for information from Third Parties

Signposts will not disclose any information to third parties without the agreement of the person involved or unless it comes within the exempted terms of the Signposts Confidentiality Policy (Safeguarding Vulnerable Adults and Children). Any worker who receives a request for information from third parties regardless of whether the request is linked to Confidentiality Policy should initially discuss this with their line manager. Any sharing of information will be identified and agreed within the Strategic Management Team.

Retention and destruction of staff personal data

Team Personal Files are kept in a locked cabinet and access to them is restricted.

Files are destroyed 6 years after the employee leaves Signposts in line with the appendix 3 to this policy. A database is also maintained which gives basic information needed for references etc and information will be stored in perpetuity on this system.

Where someone applies to volunteer within the service but for whatever reason does not start, once confirmation has been received that they no longer wish for their application to be pursued all pertinent paperwork will be destroyed.

Working files including submitted applications for paid staff posts advertised both internally and externally are retained for 9 months after a recruitment process has reached a successful conclusion and all information relating to unsuccessful applicants are then shredded – files are stored in a locked filing cabinet.

Following guidance from the Criminal Records Bureau, once a clearance is received and checked in line with the policy statement on the recruitment of ex-offenders its certificate number and date are recorded and the disclosure certificate is destroyed. Signposts will keep its record of all clearances in perpetuity.

Enquiry and Casework Specific information linked to the Retention and destruction of personal information

Where information on clients or staff are noted in paper form either as a written phone message or notes related to an enquiry, these will be given to a client or destroyed as soon as the information/enquiry has been dealt with (see Good Practice Guidelines Appendix 1).

Casework information will be stored within Signposts secured computer system. Paper referral forms with client signatures will be kept in locked filing cabinets.

Email encryption will be used when sending emails containing personal details.

It is particularly important that the disposal of records – which is defined as the point in their lifecycle when they are either transferred to an archives or destroyed – is undertaken in accordance with clearly established policies.

Personal data should not be kept for longer than it is needed. Electronic records are closed as soon as the client and referrer are informed of support being concluded. The database will indicate that the case has been closed. Information on closed cases will be stored indefinitely within the secure computer system with limited access to the Strategic Management Team.

Paper referral forms will be destroyed after 12 months after case closure.

Should a client return for further support a new file will be opened. Internal requests for database information for previous support at Signposts will be sourced via the Strategic Management Team.

Appendix 1 – Good Practice Guidelines

Appendix 2 – Taking Photographs

Appendix 3 - Retention of personnel and other related records (CIPD guidance)

Chief Executive

Reviewed September 2011

Data Protection Policy – Appendix 1 Good Practice

Protecting personal information:

- Keep passwords secure and change regularly.
- Lock or log off computers when away from desk.
- Dispose of confidential paperwork by shredding or using official recycling bags.
- Prevent virus attacks by taking care when opening emails, attachments or when visiting new websites.
- Work on a 'clear desk' basis by securely storing paper copies of personal information when it is not being used and ensuring paperwork is filed appropriately before leaving the office for the day.
- Visitors to sign in and out of premises and accompanied in confidential areas.
- Position computer screens away from windows to prevent accidental disclosures of personal information.
- Encrypt personal information that is being taken out of the office.
- Keep back ups of information

Meeting high standards of data protection:

- Be aware of data protection and confidentiality policy.
- Ensure all clients are aware of policies.
- Collect only personal information needed.
- Be succinct and objective when updating information.
- Update records promptly.
- Close cases promptly.
- Be aware that people will try and trick you to give out personal information.
- Carry out reasonable identity checks when asked for routine information requests and always keep information to a minimum – only give what has been asked. Routine requests could include:
 - Who is my support worker?
 - Can I check when my next appointment is with my support worker?
 - What date did I start work with Signposts?
 - When was my last supervision?
- Carry reasonable identity checks when making outgoing calls to discuss enquiries, referrals, ongoing casework and information about members of staff.
- Always inform the person making a formal request for information (subject access request) that you cannot directly deal with their request and that it needs to be formally passed to the Strategic Management Team when asked for formal requests via third party or for any case work content

Data Protection Policy – Appendix 2 – Taking Photographs

The data protection Act applies where photographs are being taken for official use which would include any purpose for promotion of Signposts services:

- Internal bulletin
- Website
- Presentations
- Displays
- Media i.e. newspaper

Photographs of activities and events are recognised as being a positive way of identifying and promoting good practice within the Signposts project.

When taking photographs permission should be sought verbally from the person being photographed. Where the photo is to be used for public display written permission should be sought.

When taking photographs of children written permission should always be sought from parents or guardians. Good practice suggests that in addition verbal consent from the child should be asked at the time of the photograph being taken.

Photograph permission forms can be found on the Signposts website www.signposts.org.uk

Appendix 3 – taken from www.cipd.co.uk/subjects/hrpract/psnlrecrd/retrecords

Statutory retention periods

The table below summarises the main legislation regulating statutory retention periods. However, if in doubt, the government's Business Link website (see Useful contacts below) advises that it is a good idea to keep records for six years (five in Scotland), to cover the time limit for bringing any civil legal action.

Record	Statutory retention period	Statutory authority
accident books, accident records/reports	3 years after the date of the last entry (see below for accidents involving chemicals or asbestos)	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended. Special rules apply concerning incidents involving hazardous substances (see below).
accounting records	3 years for private companies, 6 years for public limited companies	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006
income tax and NI returns, income tax records and correspondence with the Inland Revenue	not less than 3 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631)
medical records and details of biological tests under the Control of Lead at Work Regulations	40 years from the date of the last entry	The Control of Lead at Work Regulations 1998 (SI 1998/543) as amended by the Control of Lead at Work Regulations 2002 (SI 2002/2676)
medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677)
medical records under the Control of Asbestos at Work Regulations <ul style="list-style-type: none"> • medical records containing details of employees exposed to asbestos • medical examination certificates 	<ul style="list-style-type: none"> • 40 years from the date of the last entry • 4 years from the date of issue 	The Control of Asbestos at Work Regulations 2002 (SI 2002/2675). Also see the Control of Asbestos Regulations 2006 (SI 2006/2739)
medical records under the Ionising Radiations Regulations 1999	until the person reaches 75 years of age, but in any event for at least 50 years	The Ionising Radiations Regulations 1999 (SI 1999/3232)

Record	Statutory retention period	Statutory authority
records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)	5 years from the date on which the tests were carried out	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677)
records relating to children	until the child reaches the age of 21	Limitation Act 1980
Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity	6 years from the end of the scheme year in which the event took place	The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years after the end of the tax year to which they relate	The Statutory Sick Pay (General) Regulations 1982 (SI 1982/894) as amended
wage/salary records (also overtime, bonuses, expenses)	6 years	Taxes Management Act 1970
national minimum wage records	3 years after the end of the pay reference period following the one that the records cover	National Minimum Wage Act 1998
records relating to working time	2 years from date on which they were made	The Working Time Regulations 1998 (SI 1998/1833)

Recommended retention periods (where no statutory retention periods exist)

For many types of personnel records, there is no definitive retention period: it is up to the employer to decide how long to keep these records and it's a question of judgement rather than there being any definitive right and wrong. An employer needs to consider what would be a necessary retention period, depending on the type of record. The advice in this factsheet is based on the time limits for potential tribunal or civil claims and aims to draw sensible conclusions as to how long keeping the records will protect an employer.

Where the recommended retention period given is 6 years, this is based on the 6-year time limit within which legal proceedings must be commenced as laid down under the Limitation Act 1980. Thus, where documents may be relevant to a contractual claim, it is recommended that these be retained for at least the corresponding 6-year limitation period.

Record	Recommended retention period
actuarial valuation reports	permanently

Record	Recommended retention period
application forms and interview notes (for unsuccessful candidates)	6 months to a year. (Because of the time limits in the various discrimination Acts, for example the Disability Discrimination Act 1995, minimum retention periods for records relating to advertising of vacancies and job applications should be at least 6 months. A year may be more advisable as the time limits for bringing claims can be extended. Successful job applicants documents will be transferred to the personnel file in any event.
assessments under Health and Safety Regulations and records of consultations with safety representatives and committees	permanently
Inland Revenue approvals	permanently
money purchase details	6 years after transfer or value taken
parental leave	5 years from birth/adoption of the child or 18 years if the child receives a disability allowance
pension scheme investment policies	12 years from the ending of any benefit payable under the policy
pensioners' records	12 years after benefit ceases
personnel files and training records (including disciplinary records and working time records)	6 years after employment ceases
redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy
senior executives' records (that is, those on a senior management team or their equivalents)	permanently for historical purposes
time cards	2 years after audit
trade union agreements	10 years after ceasing to be effective
trust deeds and rules	permanently
trustees' minute books	permanently