

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

Telephone : (01524) 419021

Fax : (01524) 411541

Community
Legal Service



E-mail: signpostsmarc@signposts.org.uk

Website: www.signposts.org.uk

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

Pamela Beswick – Chief Executive



Help Point

Also:-

Preston Office: (01772) 759413 Carnforth Office: (01524) 732807

Signposts ICT/Internet and Technical Equipment Policy

This policy is intended to avoid or mitigate any associated risks and to protect Signposts and its staff from any possible liabilities.

All people who access our services including young people are encouraged to use the Internet in pursuit of their own development only, and the achievement of organisational tasks. However, any staff accessing sites deemed unsuitable in relation to the work of Signposts e.g. pornography, racism, terrorism etc, will be disciplined. Staff should also be aware that emails should comply with high standards of professionalism and should contain the relevant corporate information including charity and company numbers. Please discuss with your Line Manager if you are unsure.

Signposts computers must not be used in any way to access information from other computer systems (computer hacking) as this is against the Computer Misuse Act.

Young People and clients should not have access to staff computers unless their computers are for office and client and youth work use. All personal and work files etc should be password protected and the computer should not be left unsupervised at any time when it has been booted up via password.

The CEO and DCEO have the right to request sight of company equipment without prior notice.

Staff/Volunteers

Staff and Volunteers who are authorised may access email and internet for the purposes of obtaining information and advice for or on behalf of Signposts or a client or in connection with the day-to-day business of the Organisation.

Personal use is limited to access authorised by the worker 'heading up' and is subject to availability. Usage is restricted by the issues listed in item 3 'Restrictions'.

Passwords must be protected and may not be disclosed to any member of staff or client without authority.

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

Clients Over the age of 18

A computer will be made available at agreed times for the use of clients over 16 who are proficient in the use of the equipment – subject to availability, assistance will be given to those who are not.

Young People

- Young people should only be allowed to access the Internet if they have understood the restrictions placed on them by the Organisation.
- Young people should only be allowed access to the Internet within a supervised and observed environment.
- Workers should ensure they discuss personal safety issues with young people on a regular basis
- During each access session a named worker should be responsible for supervising access at any given time during that session.

2. General Procedures – Computer Use

- Separate user names and passwords will be used for Signposts business and general use to protect Signposts' own email and files for security
- Clients may use the facility free of charge subject to availability
- Users must try to book a time slot and adhere to the agreed time, however, all effort will be made to give access to the internet at other times subject to availability of equipment
- Users are requested to limit use of the system to obtaining information and advice materials relating to their enquiry
 - Users will be monitored regularly should they require assistance during their time slot

3. Restrictions

Users may not :-

- Use the internet to obtain, download, send, print display or otherwise transmit or gain access to sites that are of an illegal nature, obscene or abusive.
- Download unauthorised software or materials that contravene rules and regulations governing copyright or does not comply with the Data Protection Act 1998
- Download software and/or files that may be likely to corrupt the system such as those containing a virus
- Make alterations or amendments to the system settings
- Damage, disable or otherwise harm the operation of computers

4. E-Mail

Staff must note that e-mail has similar legal status to the written word and any views expressed via Signposts e-mail must be as appropriate as if they have been written on Signposts letterhead.

All correspondence (internal and external) should be stored in appropriate folders or remain in the inbox for a minimum of 6 months.

It should be noted the e-mail can be unreliable so very important information should be backed up with a hard copy or a phone call to ensure it has reached all of the intended recipients.

Staff preparing to go on holiday or who know they will be out of e-mail contact for more than 2 days should generate an 'out of office reply' which lets others know when to expect a response to their e-mail. Also note that the CEO and DCEO will access e-mails remotely if necessary.

As a matter of good practice staff contact details should also be displayed on the bottom of all e-mails sent out.

- Users wishing to send emails must be authorised to do so.
- Names, addresses and other personal or confidential information must not be transmitted through electronic mail that may contravene the Data Protection Act.
- Users must report any unpleasant material, virus's or other unusual or unexpected events.
- Users must not send bulk mail messages (junk mail or spam) of any kind
- Users must not open email that cannot be identified

All Signposts e-mails should have a disclaimer template which reads:

"Any view or opinions expressed are solely those of the original author. The information transmitted by this e-mail and any attachments is confidential and intended solely for the individual to whom it is addressed. If you are not the intended recipient, please do not copy or disclose its contents, but delete this from your system and notify the sender immediately. Whilst this e-mail has been swept by anti-virus software, you are solely responsible for ensuring any e-mail or attachment you receive is virus free. Signposts disclaims liability for any damage you suffer as a consequence of receiving any virus."

Using Technology within Work or for Communicating with Young People or Vulnerable Adults

- This includes: digital cameras, blue tooth technology, film, mobile phones, web cams, blogs, instant messaging and social network sites. (See Signposts Mobile Phone Policy).
- Any communication between staff and children, young people and vulnerable adults should remain within professional boundaries
 - Staff should never use or give out their personal contact details
 - Personal subject matter should be avoided
 - Workers should not take photographs or film without consent from young people or vulnerable adults and their parents/guardians or carers and never on personal mobile phones
 - Young people and vulnerable adults should be aware they are being photographed or filmed and the reasons why
 - Text messaging is not an appropriate way to respond to a young person in crisis or risk of harm
 - If text messaging is used to communicate group meetings, times etc then high professional standards should be followed
 - Staff should be aware of developments in technology and the impact that may have on their sessions or the people they work with for both cultural and safety reasons.

Inappropriate texts, photos or emails should not be deleted and must be kept as evidence. It should be reported to a colleague or manager immediately. If this is not possible a professional note or record should be made and shown to a colleague at the earliest opportunity.

Disclosure of Information/Data Protection

The law requires that certain types of information must be available to Councillors, Auditors, Government Departments, Service Users and the Public. If you are in any doubt as to whether you can release any particular information, always check with your Line Manager first and refer to Signposts' Data Protection Policy.

Staff must not use any information obtained in the course of their work duties for personal gain or benefit, nor should they knowingly pass it on to others who might use it in such a way. Staff must not communicate confidential information or documents to others who do not have a legitimate right to know. Furthermore, such information which is stored on computer systems must also only be disclosed in accordance with the requirements of the Data Protection Act 1998 (or as subsequently amended). Please refer to Signposts' Data Protection Policy.

Maintenance

In dealing with problems with IT equipment or programmes the contact for help is MASNo other organisation/individual should be hired to investigate and repair a problem.

Purchase of Computer Hardware and Software

Computers must be ordered through Main Office or be approved by the DCEO. It is essential that all hardware can be returned to the place of purchase easily in case of repair needs.

Software for all Signposts computers must be licensed and approved by Main Office. This will be put onto new computers by an approved source. Any requests for new or improved software must go through Main Office. No software or programmes not used by Signposts should be installed.

Housekeeping

Work should be kept in sub folders under one main folder in the hard drive – this will make it easy to back up and keep the hard drive tidy.

Back Up Procedures

Where a worker has sole/major responsibility for a machine they they are responsible for backing up the hard drive and e-mail correspondence **weekly using**
If a computer is shared then the line manager must allocate the back up duties to one member of staff.

Virus Checking and Firewalls

Staff must run the recommended anti virus programme once a week and all external media (including floppy discs, cd's and files downloaded from the internet) should be virus scanned before use.

Signposts uses an e-mail facility which automatically scans incoming messages and files. All Signposts computers will have a firewall set up to protect the computer and information once connected to the internet. These must not be disabled for any reason.

This Policy must be read in conjunction with Signposts other Policy Documents in particular:

Child Protection and Vulnerable Adults
Mobile Phone Use
Data Protection

Chief Executive
Updated December 2009