



60 Newmarket Street, Grimsby, North East Lincolnshire, DN32 7SF
Telephone: 01472 269666 Website: www.foresight-nelincs.org.uk

Internet and Social Networking Policy

Use of the internet by staff, volunteers and service users of Foresight North East Lincolnshire Ltd is permitted and encouraged where such use supports the goals and objectives of the organisation.

However, Foresight has a policy for the use of the internet whereby staff, volunteers and service users must ensure that they:

- use the internet in an acceptable way
- do not create unnecessary risk to the organisation by their misuse of the internet
- comply with current legislation including the Prevent Strategy

Unacceptable behaviour

- In particular the following is deemed unacceptable use or behaviour by staff, volunteers and service users:
- visiting internet sites that contain obscene, hateful, pornographic, terrorism or otherwise illegal material
- using the computer to perpetrate any form of fraud, or software, terrorism, radicalisation, film or music piracy
- using the internet to send offensive or harassing material to other users
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- hacking into unauthorised areas
- publishing defamatory and/or knowingly false material about the organisation your colleagues, service users and volunteers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format
- revealing confidential information about the organisation in a personal online posting, upload or transmission - including financial information and information relating to our service users, volunteers, staff, business plans, policies, and/or internal discussions
- making contact with vulnerable adults and children/young people or associating with them through any social networking sites (this includes having names on 'friend' lists).

- Uploading photographs of staff, trustees, service users, volunteers onto any sites including social networking sites such as Facebook without the consent of the staff member, Trustee, service user or volunteer
- Uploading any photographs or information of children / young people onto any social networking or any other internet sites
- Uploading photographs or information of children / young people for funding purposes without written consent from parents / carers
- Uploading photographs or information of terrorism, extremism or radicalisation onto any social networking or any other internet sites
- undertaking deliberate activities that waste staff and volunteer effort or networked resources
- introducing any form of malicious software into the operational network

The following is the procedure to be used by all staff, volunteers and service users regarding the use of personal mobile phones, social networking websites and personal email accounts within the centre.

1. Mobile Phones

When attending the centre staff, volunteers and service users are responsible for their own property, and Foresight will not be held liable for damage, loss or theft of such items.

Mobile phones should not be used during work hours, lessons or courses, and should be switched off unless for work purposes or an emergency situation dictates otherwise. If a personal emergency arises all staff (including tutors) must inform the operations co-ordinator or the Chief Officer immediately. Staff who do not comply with this policy will be disciplined.

Foresight will not be held responsible if service user or volunteers exchange personal contact details, including their contact numbers.

Contact numbers of any other staff member, volunteer or service user should not be given out without the explicit permission of that particular person.

Mobile phones should not be used to take photographs or video recordings of any staff, volunteers or service users without explicit permission of that particular person, or group of people.

2. Social Networking

The use of Foresight's computers and laptops is strictly limited to learning provisions and Foresight business, and should not be used for personal use, with regards to social networking websites. Staff accessing such sites on Foresight IT equipment will be disciplined.

Staff, volunteers and service users are solely responsible for whom they do and do not accept as friends, members and/or groups on social networking websites, and as such Foresight will not be held accountable for any occurrences that may result.

Staff, volunteers and service users should ensure that the content of their social networking accounts, including pictures are appropriate for all that will view or have access to.

Comments and other content must not be derogatory towards Foresight, or those with whom Foresight is linked or working with including young people, staff and other organisations.

Do not reference or cite company staff, partners, volunteers or service users without their expressed consent within your personal page or comments.

3. Email

Staff, volunteers and service users should observe the same care in language used as detailed in the social networking section above.

A record of emails sent and received should be kept back up electronically for reference and made available to a line manager if required.

Company-owned information held on third-party websites

If you produce, collect and/or process business-related information in the course of your work, the information remains the property of Foresight. This includes such information stored on third-party websites such as webmail service providers and social networking sites, such as Facebook and LinkedIn.

Monitoring

Foresight North East Lincolnshire Ltd accepts that the use of the internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the organisation.

In addition, all of the organisation's internet-related resources are provided for business purposes. Therefore, Foresight maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

Sanctions

Where it is believed that an employee has failed to comply with this policy, they will face the organisations disciplinary procedure. If the employee is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the employee's disciplinary record.

Agreement

All company employees, Trustees, contractors or temporary staff who have been granted the right to use the company's internet access are required to sign an agreement confirming their understanding and acceptance of this policy.

This information is also available in other formats, languages and picture format upon request.