Internet, Email and Fax Policy

Turas Training

Approval date:

Revision date:

1.Responsibility for approval of policy	Board of Directors/Trustees
2.Responsibility for implementation	Project Coordinator
3. Responsibility for ensuring review	Project Coordinator

1. Policy Statement

Turas is committed to ensuring internet, email and fax usage that protects the organisation and its interests, and ensures requirements are met concerning dignity at work for all employees, and the protection of the individual's right to privacy.

2. Purpose

2.1. To ensure that TURAS has clear policies outlining its internet and email usage.

2.2. To set out practical guidelines for transferring person-identifiable information (information which could be used to establish the identity of an individual) by fax.

2.3. To outline procedures in relation to social networking.

3. Scope

This policy applies to all email, internet and fax usage through the organisations email, internet and fax system or on any work hardware being used in or out of work premises. It applies to all staff, service users and visitors within the organisation. It also includes people from other agencies conducting in reach services in Turas for the time they are on the premises.

4. Email and Internet Use

4.1. The email system is to be used solely for the purposes of Turas and not for personal purposes of the employees.

4.2. Employees are permitted to use the internet for personal purposes during lunch breaks. However the limits of internet use outlined in this policy must be clearly followed.

4.3. Where an employer has allowed the use of the company's communications facilities for private use by employees, such private communications may be subject to some surveillance, for example, to ensure adequate virus checking, and compliance with the policy.

5. Sending Emails

5.1. Email is effectively on official headed paper and can be traced back to place, date and time of sending. Staff members need to ensure they are satisfied with email content and that it has been approved at the appropriate level. Important email correspondence should use the 'confirm receipt' function.

5.2. Staff are not to instigate or forward "unofficial mail" to users either within or outside the office which may be offensive or disruptive to others or which may be construed as harassment.

5.3. Staff are not to use another's email account, or allow another employee to send from their email account. If sharing computers in an office staffs are to log off when leaving the computer.

5.4. All e-mail's leaving the Office should have the following automatically appended:
"The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and / or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer".

6. Opening Emails

6.1. Do not open any files that look suspicious or are from an unknown sender.

6.2. Should you receive material which you find offensive or abusive or time wasting respond to it just as you would an offensive letter: complain directly to the sender and bring it to the attention of the sender's employing organisation as appropriate

6.3. In the case of any Spam mail don't issue any reply.

7. Security

7.1. Do not leave your computer without securing the session by password or signing off.

7.2. If you think someone knows your password, ask for it to be changed as soon as possible. Maintaining the privacy of your password is your responsibility and consequently you are responsible for any abuses taking place using your name and password.

8. Inappropriate Email and Internet Use

8.1. Emails may not contain statements or content that is libellous, offensive, harassing, illegal, derogatory, or discriminatory. Inappropriate or offensive messages such as racial, sexual, or religious slurs or jokes are prohibited. Sexually explicit messages or images, cartoons or jokes are prohibited.

8.2. Staff are not to use communal email systems to disseminate non work related information, except with the prior approval of line management

8.3. Staff are not to make derogatory comment regarding gender, marital status, family status, sexual orientation, religion, age, disability, race or membership of the travelling community.

8.4. Internet must be used in a way that complies with current legislation, is deemed acceptable to the organisation, and does not create unnecessary risk to the organisation. In particular the following is deemed unacceptable use or behaviour by employees:

8.4.1. visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material

8.4.2. using the computer to perpetrate any form of fraud, or software, film or music piracy

8.4.3. using the internet to send offensive or harassing material to other users

8.4.4. downloading commercial software or any copyrighted materials belonging to third parties, unless this download is permitted under a commercial agreement or other such licence

8.4.5. hacking into unauthorised areas

8.4.6. sending defamatory and/or knowingly false material about Turas

8.4.7. undertaking deliberate activities that waste staff effort or networked resources

8.4.8. introducing any form of malicious software into the organisations network.

9. Monitoring of Email and Internet Systems

9.1. The organisation can not at any time access private email accounts.

9.2. Monitoring of sites accessed on work computers may be undertaken by the organisation to ensure adherence to the internet and email policy or other relevant organisational policies.

9.3. Records of which sites have been accessed may be referred to if required in a situation of suspected breech of internet usage policy. If any illegal activity is suspected in relation to private email usage Garda will be contacted, in certain circumstances Garda will be entitled to access private email.

9.4. The organisation may access work email accounts and emails. In this instance staff will be informed prior to the accessing of email correspondence if at all possible. In relation to the privacy of emails received from people not in the organisation, all content will be treated confidentiality by the relevant line manager.

10. Guidance when Using Fax Machines

10.1. The fax machine should be used to transmit person-identifiable information in exceptional circumstances; such as the urgent transfer of information. Where such transfer is essential, the following guidelines should be followed:

10.1.1. Information should be restricted to the minimum necessary and only those items that are essential to the purpose.

10.1.2. Information should be anonymised where possible to limit identification of the service user or patient. Where possible use initials as opposed to name and address. Names and addresses could be sent by another method such as delivery via post/hand or telephone. Only use name and address when absolutely necessary such as in those circumstances where there are no other common items between the parties.

10.1.3. Do not use fax to transmit highly confidential or sensitive information.

10.1.4. Do not use fax for routine matters when other methods will suffice.

10.1.5. Faxes should always be accompanied by a cover sheet with a confidentiality statement (Appendix I)

10.1.6. Where possible, contact the recipient to inform them a confidential fax is being sent, and request confirmation upon receipt of the fax within an agreed time scale.

10.1.7. Upon completion of the fax, retain the printed record of transmission as confirmation that the fax was successful.

10.1.8. Printouts should not be left unattended at the fax machine.

11. Sanctions

11.1. Where it is believed that an employee has failed to comply with this policy, disciplinary actions will be implemented.

12. Privacy in the Workplace

12.1. Employees in the workplace in Ireland have a legitimate right to a certain degree of privacy in the workplace. However, their right to privacy must be balanced with the legitimate rights and interests of the employer. Any personal data from or related to an employee's work e-mail account or his or her use of the internet that is legitimately stored by an employer must be accurate and up to date and not kept for longer than necessary.

12.2. The employer must put in place appropriate technical and organisational measures to ensure that any personal data it holds is secure and safe from outside intrusion.

13. Social Media

13.1. Turas does not discriminate against employees who use social media sites (facebook, twitter etc) for personal use on their own time. However:

13.1.1. Bloggers are personally responsible for their commentary.

13.1.2. Staff cannot use the Internet to harass, threaten, discriminate against, or disparage other employees or anyone associated with Turas. Negative statements about Turas, its services, its team members, its service users, or any other related entity may lead to disciplinary action.

13.1.3. Staff cannot post photographs or videos of service users, other team members without express written consent and authorisation from management.

13.1.4. Staff can not write anything that conflicts with any areas of confidentiality, or negatively reflects on the professionalism of the organisation. A useful rule is that employees should not write anything that they would not let a service user read.

13.2. Staff should not use social media such as facebook and twitter to engage with service users unless this is a stated part of a Turas programme. If a service user asks to be 'a friend' on facebook, the request should be turned down, and the service user informed that it is the organisations policy.

13.3. If social media is permitted as part of a programme, staff should take care to conduct exchanges in with the same level of professionalism that they would conduct a face to face conversation. Staff should also make service uses aware that comments left can be viewed by others, and therefore that they should be careful about information they may wish to keep confidential.

13.4. If the organisation uses video clips on a media format such as YouTube, it is important that permission has been received.

Appendix I: Confidential Fax Cover Sheet

Address
Unit C & C1 Bluebell Business Park, Old Naas Rd, D12

Phone 01 450 5396
Fax 01 450 5069
Email info@turastraining.ie

Turas Training

Fax

To: **From:**

Fax: **Pages:**

Phone: **Date:**

Re: **cc:**

☐ Urgent ☐ For Review ☐ Please Comment ☐ Please Reply ☐ Please Recycle

Confidential

The information contained in this fax is confidential, privileged and should only be reviewed by the individual named above. If you are not the intended recipient, please immediately notify the sender by telephone and return this fax to the sender. Thank you.