The North of England Refugee Service:

ICT Code of Conduct

Document Originated:	08/12/99	Written by Refugee Council
Approved:	00/00/00	By: Board of Directors
Last revised:	July 2013	By: Roy Blewitt
Next Revision:	July 2014	By: Quality Task Group
Document Controlled By:	QTG	

Summary:

This Code of Conduct sets out what is expected from all users at the North of England Refugee Service (NERS) in respect of e-mail and Internet access. It is important that all staff read, understand, and take ownership of the principles within the document, in order for the NERS, staff and volunteers to effectively fulfil their legal obligations and to promote best working practice.

Contents of policy:

IT CODE OF CONDUCT

1. Introduction

1.1 The North of England Refugee Service has invested heavily in information and Communications Technology (ICT) in order to provide a more efficient, professional and up to date service to our main client group – refugees and asylum seekers.

1.2 This Code of Conduct has been developed in order to facilitate efficient ways of working, minimise risks, and set out guidelines on relevant legislation, roles and responsibilities and good practice, and clearly specify the underlying values and principles. This document will be reviewed periodically to reflect learning from experience.

1.3 Some of the benefits of the ICT systems include: hosted virtualised desktops; a more efficient and flexible telecoms system; faster retrieval of information; reduction of paperwork; increased security and improved disaster recovery and business continuity processes.

1.4 However, it is important that users also recognise the risks. These include:

- Legal risks - receiving, storing or transmitting material that is in violation to any law, e.g. defamation, copyright infringement, inadvertent formation of contracts etc.
- Employer's liability - an employer's responsibility to do its utmost to ensure no law is broken or systems misused.
- Employer's liability for third party harassment – an employer must do all within its control to protect employees from harassment by third parties.
- Data Protection – an employer must take steps to safeguard personal and sensitive data and ensure an individual's right to privacy, consistency, and consent.
- Security – risks to the organisation in the event of files being lost, viruses corrupting information, or the system crashing.
- Fraud and the misuse of computer equipment.
- Loss of reputation – the consequences of misuse of the systems, which could result in a loss of confidence and belief in the stated aims and values of the NERS.

1.5 IT systems are provided for the NERS's stated objectives and are owned by the NERS, as is all the information held on these systems. All the equipment, including laptop computers, remain the property of the NERS, and may be recalled to the workplace at any time, and must in all cases be returned if a member of staff leaves.

1.6 This document should be considered in the context of other relevant policies, such as the NERS's Disciplinary Procedure, Grievance Procedure, Equal Opportunities Policy, Code of Conduct, and Health and Safety Policy.

1.7 In addition to this Code of Conduct, the NERS will provide support by way of training and supervision, and will ensure all users have a clear understanding of their responsibilities as set out in this document. Therefore, any misconduct on the part of staff who claim ignorance as a defence will still be treated as a disciplinary matter.

2. Principles

2.1 Before being given access to the network all users (including all NERS staff, contractors, clients, volunteers, sessional staff, students on placements and trainees), must have read this IT Code of Conduct. They have to understand their responsibilities as a user, and have agreed to abide by the principles of the document. However, where a modem connection is used, personal use should be kept to a minimum.

Relevant training will be given where appropriate and at managers' discretion (e.g. when someone is employed on a short term contract).

2.2 Personal use is permitted, provided:

- It is in your own time, i.e. it does not interfere with your work.
- It does not incur any cost to the NERS. Although the use of e-mail and network connection to the Internet does not incur any additional costs, implications of staff time are to be considered.
- It is not used to compromise the NERS's beliefs or values.
- You understand and accept that all data may be monitored.

2.3 Access to others e-mail files or files stored on network, for instance when someone is absent, may be granted to a manager who needs to access them. Such access must only be given with the relevant line manager's approval.

2.4 If deemed necessary User names and passwords of all staff, volunteers and students can be centrally reset to enable data to be accessed by the relevant line manager.

2.5 Printed reports showing usage and contents of e-mail messages will be produced, when evidence is required for investigation of misuse, as per the NERS's disciplinary procedures.

2.6 There may be occasions when Web sites that are against the values of the NERS need to be visited, for example, the staff may need to access sites in order to keep up and be able to respond quickly to negative political and public opinion. To protect the individual and the NERS, managers must be aware of such access to these sites, and sensitivities are to be considered when displaying sites that may be offensive to others.

Accessing such Web sites for infrequent and short periods is not considered a violation of this Code of Conduct, as there may be occasions when the address or heading of a site is misleading. However, you must exit the site as soon as it becomes clear it is not the one you want.

2.7 Users must never use the system to criticise, discipline, or berate colleagues, groups, or individuals, both within the organisation and externally.

2.8 For legal reasons as well as for ethical and principled reasons, the NERS will not tolerate any forms of harassment, victimisation, or threatening behaviour that could adversely affect any individual or group. When using electronic communications, staff is expected to follow the same conduct and behaviour as set out in the organisational Code of Conduct.

2.9 As with any NERS policy, failure to comply with these guidelines and principles can lead to disciplinary action being taken. It is important that if you are unsure of any aspect of this document, you first check with your manager, Human Resources or the CEO.

3. Roles and Responsibilities

3.1 It is the role of all users to use all computer equipment as an effective and efficient tool to enable the NERS's objectives to be met.

3.2 All users have a responsibility to:

- Understand and comply with the policy and procedures.
- Undertake relevant training.
- Avoid putting yourself and the organisation at risk.
- Protect your personal password and under no circumstance share it with anyone.

- Take care of any equipment allocated to you, and bring to the attention of the line manager any misuse or misconduct relating to the network.

3.3 Managers and team leaders should be role models and lead by example. Responsibilities include:

- Gaining detailed knowledge of the policy and procedures.
- Ensuring new staff, volunteers (and all users) receive a copy of this Code of Conduct and understand the principles before they are given access to the network.
- Determining shared network access and retrieval, i.e. decide what is appropriate for storing in shared directories and who is responsible for administrating shared areas.
- Ensuring security breaches and potential risks are reported and corrective action is taken.
- Effectively managing the Code of Conduct, e.g. investigate and/or take disciplinary action for breaches of the procedures, with advice from HR.

3.4 The IT team has a role in providing expert technical advice and support to users, and in providing managers with information regarding use of the systems. Responsibilities are to:

- Set up and delete access as requested by managers.
- Respect confidentiality.
- Ensure recommended virus protection measures are in place.
- Ensure that the NERS keeps within software licensing law, e.g. by licensing installed software, keeping records of authorised software, and deleting unauthorised software.
- Provide Monitoring reports when requested by relevant line managers.

4. Security

4.1 Anyone who works on a temporary basis (including volunteers, students on placements and trainees) can also have access to shared directories. Temporary staff should be familiarised with the IT Code of Conduct and be given their own username and password, with relevant access to shared areas.

4.2 Managers are responsible for informing the IT Team when any staff member, permanent or temporary, leaves the organisation who has a username and access to the network so that their username and access to the Network can be terminated.

4.3 Security issues to consider are breaches of confidentiality, spreading viruses, and fraud. To minimise these risks, **you must:**

- Maintain a secret password and do not share it with anyone.
- Store all files on the network, for security and backup purposes. Floppy discs, memory sticks, data CDs should not be used for transferring work, for example to a home computer, and not be used for permanent storage.
- If you suspect a security problem inform your manager immediately.

You must not:

- Log anyone on to the network using your own username and password. All legitimate users should have their own username and password and they should not change them without prior authorisation of the RIES Contract Manager.
- Log onto the network using someone else's username and password.
- Install any software. Only I.T. Team support staff and their contractors should be installing software with authorisation from the Senior Managers. Any 'exceptions' must have written permission from the Senior Managers.
- Pass on chain letters, including virus warnings, 'good luck' e-mails and 'charity' appeals (these are often not genuine, and can contain viruses).

4.4 Online transactions through commercial websites should only be used where the connection is securely encrypted, and with appropriate authorisation from budget holders.

4.5 For your own protection, do not send information concerning bank accounts or credit card details in **e-mail** communications, unless there is a secure encrypted connection in place between both parties.

5. Data Protection

5.1 The Data Protection Act 1998 is an EU initiative that came into effect because of the growth of the "Information Society". In particular, in response to concerns about the threat to personal privacy that the manipulation and transfer of data by computers can pose.

5.2 Breaking the Data Protection Act contravenes the law and may result in the NERS being prosecuted, fined and/or our reputation being damaged. In some circumstances disciplinary action can be taken against individuals knowingly contravening the law.

5.3 Under this Act, any sensitive or personal data, including that held on manual filing systems, must:

- Be stored securely.
- Be processed with the explicit consent of the person the data relates to.
- Only be obtained and used for the specified purpose for which it was requested.
- Be kept up to date and accurate.
- Not be kept longer than is necessary.
- Not be sent to a country or territory outside the European Economic Area unless that country has an adequate or similar level of protection (e.g. USA is *not* an acceptable territory).

5.4 Individuals who have personal data stored on our electronic and paper systems must be informed we are keeping their data, why we are keeping it and who we are disclosing it to. They also have the right to view any data relating to them on request, and ask for any inaccuracies to be corrected.

5.5 Check with your manager if you're uncertain about what you may disclose or whether information should be classified as restricted or confidential.

5.6 Never refer to sensitive or personal information without need, or talk about it socially, and beware of people trying to obtain information to which they're not entitled, particularly over the phone (e.g. the police)

5.7 Refer to the section on confidential information in your Contract of Employment. Further information on The Data Protection Act is available from Human Resources.

Legal Risks and Compliance

6.1 As outlined in the introduction, increased IT functions bring risks to the organisation. The main risks that can have grave consequences for the NERS are loss of reputation, legal costs defending liability cases, and the costs to the organisation in terms of fraud, theft, or wilful damage.

6.2 Any action taken by staff which brings the NERS into disrepute, or affects clients, users, and others in an adverse way, will be investigated, with the potential for instant dismissal for incidents of gross misconduct.

6.3 Under this policy, the following is categorised as **<u>unacceptable</u>** and may result in disciplinary action:

- Posting, transmitting, re-transmitting or storing material that is in violation of any law, and is defamatory, indecent, obscene, or threatening.
- Posting, transmitting, re-transmitting or storing any racist or other material contrary to the values of the NERS.
- Breaching copyright, trade secret, patent or other intellectual property laws.
- Installing NERS software on your own computer – this is fraud.
- Installing or downloading software (programmes) from the Internet, without approval from SMT. This includes 'free' software from magazines or any external sources.
- Copying software and giving it to others, e.g. Tutorial programmes for trainees.
- Altering or falsifying data, or impersonating a user.

6.4 The NERS has an obligation to safeguard its resources, staff, volunteers, students on placements and its client group. You must inform your manager if you think any of the above is occurring. For instance, inform your manager if you think there is software on your computer that isn't approved or properly licensed.

Approved by the Board of Directors*:* Signature: …………..………….

Position: ….…………………….

Date: ……………………………

APPENDIX 1

Courtesy and Good Housekeeping

To ensure we all comply with the basic rules of courtesy, and to practise good housekeeping, always consider the following:

- Always be polite. It is easy to compose an inflammatory message and send it out without giving yourself time to write a considered response.
- Consider who needs to read your message. For messages to wide audiences, set up a separate distribution list, e.g. team lists.
- Use lower case for e-mail messages because using capitals in e-mail is shouting.
- Send longer items and reports as attachments or shortcuts, and compress or zip large files so that you don't congest the mail server/system.
- Use a meaningful and descriptive subject heading to let the recipient know what the message is about before they open it.
- Only use a high priority (urgent) indicator where really appropriate.
- Don't assume messages have been read, e.g. the recipient may be away.
- Be aware that forwarding jokes and non-work material creates network congestion and slows down everyone's work.
- **Always 'preview' attachments sent from friends (non-work), as double clicking on the file may set off a virus. Delete and then reply to sender asking them not to send such attachments again.**
- Avoid using graphics, logos, images etc, unless necessary as they increase the size of attachments and use up more storage space on the system.
- Remember that messages intended for internal use only can sometimes end up in a public forum.

Good Housekeeping:

- Check your mailbox for new messages at regular intervals and respond promptly to messages in your inbox. If appropriate, forward them to another member of staff.
- Select the 'Reply' on the toolbar so that you only respond to those who need a reply, rather than all addressees.
- When replying to a message, ensure that the recipient knows what you are referring to. The system automatically includes the original message into your reply.
- **Only print out e-mails if absolutely necessary**. An advantage of e-mail is that it can reduce the amount of paperwork you have.
- Set up folders to store messages that you need to keep.

- Delete (or archive) unwanted e-mails at regular intervals to avoid overload of information. Do not store messages in your In-box as this slows down the system.
- Make appropriate arrangements for your e-mail to be forwarded or checked by others during periods of long absence.
- Consider nominating a person responsible for overall housekeeping in your team. All users should also delete old/obsolete files, ensure documents are named consistently and are stored on correct folders.
- Although it is up to the teams and individuals to decide what information they keep on shared areas, the underlying principle of the NERS network is to make information and data available as widely as possible. Teams are therefore encouraged to share documents with others as much as possible.

APPENDIX 2

Guidance for Managers

Managers should use their discretion on providing training to temporary staff or those on contract as it may not always be practical to spend much time on training. However, all new staff or users who have access to the network must be given a copy of the IT Code of Conduct, time to read and absorb the contents, and have a briefing with their manager confirming they understand the document and their responsibilities.

Managers need to be able to give guidance on the systems and procedures for managing, and sharing information on shared directories. It may be that the manager allocates responsibility to one person in the team to manage shared files (update, sort, clear files).

Shared files and directories should be a regular agenda item at team meetings, as a forum for consulting and informing all members of the systems, problems, agreed protocols, etc.

Types of misuse are covered extensively in this document, however managing them requires different degrees of monitoring.

Misuse of time:

- If a staff member is not meeting work objectives or targets, pick this up at supervision.
- Discuss and identify the problem with the individual. Do not make assumptions about the cause of the problem.
- If it is identified that using e-mail or the Internet is proving more time-consuming, ask the staff member to monitor their time, and review this on a regular basis at future supervisions.
- If there is still no improvement after an agreed period of time, Internet access can be withdrawn. This should have been discussed earlier and not come as a surprise to the staff member.

Misuse of Equipment:

- Reports will be produced that highlight web sites visited, the date and time, and the length of visit. As per telephone monitoring, these reports are used to

- Reports will also be used as evidence when investigating gross misconduct, e.g. allegations of copying or downloading software, or visiting pornographic sites.

Allegations of Harassment/Victimisation:

- Any allegation of harassment or victimisation will be investigated under the appropriate policy.
- Monitoring reports may be requested to provide evidence for such claims. However, authorisation for such reports must be approved by a Senior Manager, with advice from HR.