



**Acceptable Use of NICVA's ICT facilities
(Acceptable Usage Policy)**

Author: ICT Unit
Issue Date: 10 December 2006
Issue Number: 1.3
Approver: HR Officer, Head of ICT
Status: Approved Version 1.2
Review Date: January 2009

Review History

Version	Review Date	Reviewer	Change Summary
1.1	December 2005	HR Officer, Head of ICT	1 st Draft
1.2	December 2006	HR Officer, Head of ICT	Changed 5.1
1.3	January 2008	HR Officer, Head of ICT	Added 4.4

Contents

1. Introduction

1.1	Reasons for having this policy	Page 4
1.2	Precautionary and Disciplinary Measures	Page 4
1.3	How it is published	Page 4

2. General User

2.1	Hardware and Software Purchasing	Page 5
2.2	Installing/Copying Software	Page 5
2.3	Transfer and storage on the NICVA Network	Pages 5 & 6
2.4	Fault/Incident Reporting	Page 6
2.5	Care of equipment/Health & Safety	Page 6

3. Email Policy

3.1	When to use Email	Page 7
3.2	Use of Distribution Lists	Page 7
3.3	General points on Email use	Pages 7 & 8
3.4	Email etiquette	Page 8

4. Internet Policy

4.1	Use of the Internet	Page 9
4.2	Downloading Files/Music	Page 9
4.3	Instant Messaging Services (IM)	Page 9
4.4	Social Networking Sites	Page 10

5. Security

5.1	Physical Security	Page 11
5.2	Marking Equipment/Assets Register	Page 11
5.3	Backups	Page 11
5.4	Anti Virus/Firewalls	Pages 11 & 12
5.5	ICT Monitoring	Page 12

6. Other

6.1	AUP Review	Page 13
6.2	Reference Material	Page 13
6.3	Contacts	Page 13

Appendix

1. Introduction

NICVA recognises the need for its staff to have access to the Internet and Email in order to successfully complete their work. Technology is an essential part of many people's lives, enhancing productivity and creativity. This Acceptable Usage Policy (hereinafter known as the 'AUP'.) applies to all users of NICVA's ICT Facilities (*desktop or portable*) and is intended as a guide to acceptable and unacceptable practice.

1.1 Reasons for having this policy

This policy exists for the protection and guidance of NICVA and NICVA staff by giving users ground rules for acceptable use of the equipment etc. so there are no misunderstandings. They should also provide guidelines if, for example, misuse occurs. The AUP also demonstrates to potential funder's that NICVA is professional in its approach to managing users and/or facilities.

All NICVA's ICT facilities and information resources remain the property of NICVA and not of particular individuals, units or departments (*see Appendix, Note 1*). By following this AUP we'll help ensure ICT facilities are used:

- legally;
- securely;
- without undermining NICVA;
- effectively;
- in a spirit of co-operation, trust and consideration for others;
- So they remain available.

1.2 Precautionary and Disciplinary Measures

The AUP relates to all ICT facilities and services provided by NICVA. All staff, students, volunteers and executive committee members are expected to adhere to it.

Deliberate and serious breach of the AUP may lead to disciplinary measures which may include the offender being denied access to computing facilities.

1.3 How is it published

This document is available in both electronic and hard copy versions, copies will be given to new staff on induction and will be readily available for current staff.

Location on Intranet;

[\\server\location](#)

2. General Use

ICT equipment and facilities belong to NICVA and are naturally provided for work use. You are trusted to make reasonable personal use of them as long as this does not:

- interfere with job performance;
- give rise to additional cost;
- interfere with the activities of other users;
- support any work other than that of NICVA;
- Breach any rules relating to content (*see section 4.1 Use of the Internet*).

2.1 Hardware and Software Purchasing

The ICT Unit will be solely responsible for sourcing, evaluating and the purchasing of all ICT hardware/software. Unit Head's in conjunction with the Head of ICT will have the final decision if/when equipment is required.

2.2 Installing/Copying Software

Get permission from ICT Unit before you install any software (*including public domain software – see Appendix, Note 2*) on equipment owned and/or operated by NICVA. Copying software for use outside NICVA agreements is illegal and may result in criminal charges.

2.3 Transfer and storage on the NICVA Network

Keep master copies of important data on NICVA's network and not solely on your PC's local C: drive or floppy discs. Otherwise it will not be backed up and is therefore at risk.

Ask for advice from ICT Unit if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disc space very quickly and can bring NICVA's network to a standstill.

Be considerate about storing personal (*non-NICVA*) files on NICVA's network. (*Note Appendix, Note 3*).

Don't copy files which are accessible centrally into your personal directory unless you have good reason (*i.e. you intend to amend them or you need to reference them and the central copies are to be changed or deleted*) since this uses up disc space unnecessarily.

Housekeeping should be conducted regularly and any files no longer required should be deleted. This is an important task and should be compared with managing paper based information systems. Therefore it is important to consider the following points when following good file management practice:

- Consider confidentiality of content of the files stored;

- Consider the storage space it demands;
- Consider the information's usefulness and the possible legal requirements to retain it for a minimum period. (*Please contact your line manager for guidance relating to appropriate retention periods*).

It is your responsibility to ensure that any information you have ownership of is controlled appropriately. ICT equipment and facilities (*PC's and Laptops*) and the information they contain are valuable assets. Staff should take all reasonable steps to ensure the security of these assets at all times.

2.4 Fault/Incident Reporting

The primary purpose of reporting faults/incidents is to help prevent further problems, not to attach blame. All faults/incidents on ICT Equipment must be reported to the ICT Unit immediately upon discovering the fault. The ICT Unit will deal with in due course.

2.5 Care of equipment/Health & Safety

Don't re-arrange how equipment is plugged in (*computers, power supplies, network cabling, modems etc.*) without first contacting The ICT Unit.

Don't take food or drink into rooms which contain specialist equipment like servers (*See Appendix, Note 4*).

Mobile working equipment (*i.e. Laptops/PDA's/Mobile Phones*) are the sole responsibility of the user, careful attention should be drawn when handling aforementioned equipment as they are not as robust as a desktop computer.

3. Email Policy

3.1 When to use email

- Use it in preference to paper to reach people quickly (*saving time on photocopying / distribution*) and to help reduce paper use. Think and check messages before sending (*just as you would a letter or paper memo*).
- Use the phone (*including voicemail if no reply*) for urgent messages (*email is a good backup in such instances*).

3.2 Use of Distribution Lists

- Only send Email to those it is meant for; don't send (*i.e. send to large groups of people using email aliases*) unless absolutely necessary since this runs the risk of being disruptive. Unnecessary (*or junk*) email reduces computer performance and wastes disc space.
- If you wish to send other non work related information or requests (*i.e. information or opinions on political matters outside the scope of NICVA's campaigning, social matters, personal requests for information etc.*) it is better to use a Webmail (*see Appendix, Note 4*) account or a personal email account at home; don't use the standard (*work*) aliases.
- Keep NICVA's internal email aliases internal. If you are sending an email both to a NICVA alias and outside of NICVA, use the alias as a blind carbon copy (*i.e. the bcc address option*) so that the external recipient does not see the internal alias.
- Don't send emails with attachments to large groups of people - either note in the email where it is located for recipients to look, or include the text in the body of the email. Failure to do this puts an unnecessary load on the network.

3.3 General points on email use

- When publishing or transmitting information externally be aware that you are representing NICVA and could be seen as speaking on NICVA's behalf. Make it clear when opinions are personal. If in doubt, consult your line manager/Unit Head.
- Check your in-tray at regular intervals during the working day. Keep your in-tray/inbox fairly empty so that it just contains items requiring your action. Try to decide what to do with each email as you read it (*i.e. delete it, reply to it, save the whole email in a folder, or extract just the useful information and save it somewhere logical*).

- Keep electronic files of electronic correspondence, only keeping what you need to. Don't print it off and keep paper files unless absolutely necessary.
- Treat others with respect and in a way you would expect to be treated yourself (*i.e. don't send unconstructive feedback, argue or invite colleagues to publicise their displeasure at the actions / decisions of a colleague*).
- **Don't forward emails warning about viruses** (*they are invariably hoaxes and ICT Support will probably already be aware of genuine viruses - if in doubt, contact them for advice*).

3.4 Email etiquette

- Being courteous is more likely to get you the response you want. Address someone by name at the beginning of the message, especially if you are also copying to another group of people.
- Make your subject headers clear and relevant to your reader(s) (*i.e. Don't use subject headers like 'stuff/help/hello'*).
- Try to keep to one subject per email, especially if the content is complex. It is better for your reader(s) to have several emails on individual issues, which also makes them easy to file and retrieve later. One email covering a large variety of issues is likely to be misunderstood or ignored.
- Capitals (*i.e. NOW*) can also be used to emphasise words, but should be used sparingly as it commonly perceived as 'shouting'.
- Don't open email unless you have a reasonably good expectation of what it contains,
 - Do open report.doc from an Internet colleague you know
 - Don't open explore.zip sent from an address you've never heard of, however tempting.
 - Alert ICT Unit if you are sent anything like this unsolicited.
 - This is one of the most effective means of protecting NICVA against email virus attacks.
- Keep email signatures short. Your name, title, phone/fax and web site address may constitute a typical signature. (*If you need assistance when setting up your personalised Email signature, contact the ICT Unit.*)
- Out of Office. Its good practice to use the 'out of office assistant' when you are not available. The Out of Office Assistant informs people when you are in

and out of the office, it will reply to senders with a detailed message that you can set up to include the date of your return and who to contact for immediate assistance. *(If you need assistance when setting up your personalised Email signature, contact the ICT Unit).*

4 Internet Policy

4.1 Use of the Internet

When visiting an Internet site you should be aware that your identity (*which is linked to NICVA's*) may be logged. Therefore, any activity engaged in, undertaking given or transaction made may impact on NICVA.

Please be aware of the following conventions:

- Always ensure that NICVA is neither embarrassed nor liable in any way by your use of the Internet.
- You **must not download** any software or executable files (executable files have either a.COM or.EXE extension and are called COM files and EXE files, respectively) unless you have obtained prior permission from the ICT Unit. This also includes laptops.
- It is good practice that all non-business related sites (*i.e. sports, news etc*) are accessed during your 'own time'. An employee's own time would be defined as time when they are not on duty (*i.e. not signed in for work or on a lunch or sanctioned break*). Users may access these non-business related sites, but are personally responsible for what they view.
- It is prohibited to use the internet or NICVA email to carry out activities for personal gain (*gambling, share dealing etc*).
- Obscenities/Pornography: Don't write it, publish it, look for it, bookmark it, access it or download it.

4.2 Downloading Files/Music

Staff are not permitted to download any software or other material from the internet without express permission from the Head of ICT. Illegal downloading of material may contravene copyright law. NICVA has a legal responsibility to ensure that all material and software used must comply with licensing regulations

4.3 Instant Messaging Services (IM)

Instant Messaging Services, such as MSN/Yahoo/ICQ Messenger are permitted for occasional use and you are trusted to make reasonable personal use of them as long as this does not:

- interfere with job performance;
- give rise to additional cost;
- interfere with the activities of other users;
- support any work other than that of NICVA;

- Breach any rules relating to content.

4.4 Social Networking Sites

NICVA understands the popularity and usefulness of social networking sites and supports their use by staff provided:

- No offensive or inappropriate pictures are posted;
- No offensive or inappropriate comments are posted;
- Photos and/or comments posted on these sites do not depict NICVA-related activities.

Staff must remember that they are representatives of NICVA.

Please keep the following in mind as you participate on social networking websites:

- Before participating in any online community, understand that anything posted online is available to anyone in the world. Any text or photo placed online becomes the property of the site(s) and is completely out of your control the moment it is placed online – even if you limit access to your site.
- You should not post any information, photos or other items online that could embarrass you, your family, or any other member of NICVA. This includes information that may be posted by others on your page.
- Never post your home address, local address phone number(s), birth date or other personal information.
- ICT can and do monitor these web sites regularly.

NICVA staff should be very careful when using online social networking sites and keep in mind that sanctions may be imposed if these sites are used improperly or depict inappropriate, embarrassing or dangerous behavior.

5 Security

In recent years there has been an increase in the use of computers to store and retrieve data. This together with the advances in telecommunications makes secure access to confidential data more problematic than in the past. The purpose of the security measures is to outline the general procedures that are to be followed by anyone using ICT facilities within NICVA.

5.1 Physical Security

Don't attempt to gain unauthorised access to information or facilities. The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (*including servers and client computers*) or to modify its contents. If you don't have access to information resources you feel you need, contact the ICT Unit

Don't disclose personal system passwords or other security details to other staff, volunteers or external agents and don't use anyone else's login; this compromises the security of NICVA. If someone else gets to know your password, ensure you change it or get the ICT Unit to help you (see *Appendix, Note 6*).

If you leave your PC unattended without logging off/locking, you are responsible for any misuse of it while you're away.

ALWAYS check floppy disks/USB flash drives for viruses, even if you think they are clean (*contact the ICT Unit to find out how*). Computer viruses are capable of destroying NICVA's information resources. It is better to be safe than sorry.

Information about people: If you're recording or obtaining information about individuals make sure you are not breaking Data Protection legislation (*If you require further clarification on this issue, contact NICVA's Information Officer*).

5.2 Marking Equipment/Assets Register

All of NICVA's ICT equipment is security marked with sequentially numbered, tamper resistant labels. The Equipment is registered against its corresponding number in an Assets Register Database. This is renewed and updated when equipment is purchased or decommissioned.

5.3 Backups

The information on NICVA's ICT systems are backed up on a daily basis, at the end of each week a 'weekly' system backup is made and those Tapes (*backup media*) are stored in a fire proof safe. It is imperative that you do not store important work-related information on your local C: drive, it will not be backed up and is therefore at risk.
(*see section 2.1 Transfer and storage on the NICVA Network*).

5.4 Anti Virus/Firewalls

NICVA deploys anti-virus software to protect the ICT systems from virus attacks. This software is updated as soon as a new software release becomes available. NICVA have also in place various methods of scanning inbound/outbound Email correspondence for spam/virus and pornographic content.

5.5 ICT Monitoring

'Electronic monitoring': Any information available within ICT facilities will not be used to monitor the activity of individual staff in anyway (*i.e. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files etc.*) without their prior knowledge. Exceptions are:

- in the case of a specific allegation of misconduct, when the Management Team can authorise accessing of such information when investigating the allegation
- when the ICT Unit section cannot avoid accessing such information whilst fixing a problem. (*In such instances, the person concerned will be informed immediately and information will not be disclosed wider than is absolutely necessary. In the former case their access to ICT facilities may be disabled pending investigation.*)

6 Other

6.1 AUP Review

The AUP will be reviewed annually by the ICT Unit. Following review, update and consultation with Human Resources, the agreed AUP shall be submitted to the head of Human Resources and ICT for approval.

6.2 Reference Material

Guide to using Email

http://www.emailaddresses.com/email_guide.htm

Netiquette

'Netiquette' is network etiquette, the do's and don'ts of online communication. Netiquette covers both common courtesy online and the informal 'rules of the road' of cyberspace. This page provides links to both summary and detail information about Netiquette for your browsing pleasure.

<http://www.albion.com/netiquette/>

6.3 Contacts

Name	Job Title	Ext.	Email

Appendix

Note 1

- In-house software: This is software written by staff or volunteers using NICVA's equipment. It is NICVA's property and must not be used for any external purpose. Software developers (*and students/volunteers*) employed at NICVA are permitted to take a small 'portfolio' of such in-house software source code/executables, which they may have developed, for use in subsequent work, subject to agreement with the ICT Manager.

Note 2

- Public domain software or Freeware/Shareware: This is software that is available free of charge, usually by downloading from the internet.

Note 3

- Personal Data: As a guideline, keep your personal data down to 1MB. Ten emails require 0.15MB on average (*depends a lot on whether they have attachments*). A 10-page word processed document requires about 0.1MB. Screen saver images require much more disc space and vary greatly - some may be as large as 2MB.

Note 4

- ICT Office/Server Room: This room on the 1st floor contains NICVA's ICT file/email/web/database server.

Note 5

- Webmail accounts are personal email accounts that are stored on the Internet and can be accessed from anywhere with a standard browser (*Inter Explorer, Netscape*) i.e. home or cybercafe. The ICT Unit can advise you on setting up/choosing such an account.

Note 6

- Personal passwords: Disclosure to other staff, volunteers or external agents: This may be necessary in some circumstances. Such a practice is allowed only if sanctioned by a member of the Management Team after discussion with the ICT Unit. If the password is disclosed for a one-off task, the owner must ensure that his/her password is changed (*by contacting the ICT Unit*) as soon as the task is completed.

Note 7

- Email aliases are pre-defined 'shortcuts' for distributing internal email to specific groups of people (*The ICT Unit can tell you what these are and how to use them*).