

## **APPENDIX 37 – COMPUTER POLICY**

NICVA recognises the need for its employees 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 policy applies to all users of NICVA's computers (desktop or portable) and is intended as a guide to acceptable and unacceptable practice.

Users with access to email and internet facilities must read this document and agree to abide by its contents. This has been developed in light of the requirements of the Lawful Business Practice Regulations 2000, which require employers to inform staff that interceptions (even of private communications) might take place. Users of NICVA's internet and email facilities should therefore not have expectation of privacy in their use.

### **Inappropriate Material**

Inappropriate material is that which may be judged to contravene NICVA's Harassment Policy. If you receive this type of material then it is your responsibility to remove/delete it from NICVA's network and ensure that no offence is caused to anyone inside or outside the organisation by the distribution of it. Tools are available that can identify inappropriate material and NICVA reserves the right to use these automatic scanning tools to identify the presence of or even prevent the possibility of this type of material being created. NICVA will take appropriate disciplinary action against any users whose use of the internet or email facilities contravenes this computer policy.

### **Email**

Computer equipment and facilities (such as email) 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:

- (1) Interfere with job performance.
- (2) Give rise to additional cost.
- (3) Interfere with the activities of other users.
- (4) Support any work other than that of NICVA.
- (5) Breach any rules relating to content (see section above inappropriate material).

Email can be monitored at NICVA's discretion.

### **Mail Content**

It is essential that the same care is taken with the content of messages as with printed documents. Information sent by email can never be considered totally secure and all messages sent via email can be identified as originating from NICVA - even those messages which are posted anonymously. Therefore:

- (1) Whether internal or external to NICVA, messages containing inappropriate material (as defined above) must not be freely circulated in order to prevent recipients being offended.
- (2) You should not send confidential information outside NICVA, unless you are given authorisation by your line manager.
- (3) It is important to note when using email, that if you don't want the recipients to distribute the mail more widely you should give instructions to support this.
- (4) Emails that do not need to be kept should be deleted.

### **Internet**

NICVA's internet connections are intended for activities that either support NICVA's work or the professional development of staff. Limited, appropriate personal use of the internet during breaks is acceptable as long as it does not:

- (1) Interfere with job performance.
- (2) Give rise to additional costs.
- (3) Interfere with the activities of other users.
- (4) Support any work other than that of NICVA.
- (5) Breach any of the rules relating to content.

'Trading at work' through sites such as (but not limited to) ebay is not permitted and is an example of misconduct. Trading in this context means both buying and selling goods whilst in the workplace. This activity is not considered as appropriate personal use.

Employees must not wipe out their internet trail by clicking on the 'Clear History' facility of their browser. Any attempt to disrupt lawful monitoring by an employee will amount to misconduct.

NICVA reserves the right to withdraw this facility if necessary. 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.

## **Viruses and Protection**

A virus is a piece of software, designed by an individual(s), to deliberately cause malicious damage. A virus could destroy all computer capabilities leaving the entire business without the ability to transact normally. Computer viruses are generally introduced unintentionally but the effect remains the same. To minimise the risk certain precautions must be taken:

- (1) You must not download software from the internet unless with prior approval from the Head of ICT.
- (2) Email attachments from suspicious or unknown sources must not be opened under any circumstances. These emails must be deleted on receipt. Under no circumstances should these files be forwarded to other users. Staff should be alert to suspicious known or unknown sources.
- (3) You must ensure that you do not introduce unauthorised content from disks, CDs or from other PCs.
- (4) All viruses detected should be reported to the Head of ICT immediately.

## **Good Practice**

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:

- (1) Consider confidentiality of content of the files stored.
- (2) Consider the storage space it demands.
- (3) 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. Computer equipment and facilities (PCs 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.

## **Legal and Contractual Commitments**

Binding legal or contractual commitments can be created by email communication, sometimes unintentionally. Users should not commit NICVA to an agreement unless authorised to do so. Furthermore it is the policy of NICVA that internet/email communications should not, under normal circumstances, be used for the creation of legal or contractual obligation