COMPUTER USE POLICY

Computer Security Manager:

Broadland Computers Ltd
Greenacres
Brick Kiln Lane
Ingham
Norwich NR12 9SY
01692-581766 / 07939-127066
Enquiries@broadlandcomputers.co.uk

Scope of Policy: Computer systems and equipment, including networks and internet access, in use within the New Victory Hall.

Approved uses: Training

OBJECTIVE

This policy sets out the guiding principles for use of New Victory Hall computer equipment, networks and internet services.

PRINCIPLES

Computer use must comply with the standards and practices of all Village Hall service provision and on no account are the New Victory Hall computers and networks to be used for accessing and/or downloading inappropriate content in the form of software, images, audio files or other variations of pornographic or undesirable material. They must not be used to communicate such files, images or access forums where they might be exchanged. Communications must be restricted to approved uses and under no circumstances be used to express or exchange defamatory, racist, sexist, anti-religious or any other form of offensive communication. These statements are made here to set the tone of the policy and are not an exclusive list of inappropriate use.

POLICY

1. The purpose of this Policy is to enable the New Victory Hall to have a computer environment that its users can trust.
2. The Trustees have approved this Policy
3. Computer systems will be protected against unauthorised access.
4. Internet access is only available to approved users
5. Regulatory and legal requirements will be met
6. The role and responsibility for co-ordinating computer security will be performed by the Computer Security Manager.
4. Any exceptions to these policies must have the written approval of the Trustees.
5. This Policy and its supplementary policies will be reviewed at least annually, by the Computer Security Manager in conjunction with the Trustees' IT Systems Manager.
6. **IT IS THE RESPONSIBILITY OF ALL USERS, HIRERS, AND THEIR USERS TO ADHERE TO THIS POLICY**

SYSTEM ACCESS

1. Computer assets must only be used in accordance of the guiding principles of the New Victory Hall and the terms and conditions of Hall use.
2. External Users (third parties, suppliers, etc.) who use New Victory Hall systems or data must be authorised to do so by the Trustees or under the terms and conditions of the hire agreement.
3. The computers and peripherals, including network devices should be secured in a locked cupboard within the New Victory Hall when not in use.
4. Wireless access, if available must be through a secure hidden connection with strong password protection and device address restriction.
5. Access to the physical network must remain secure and it must not be possible for any unapproved party to make a connection to the BT circuit.

CODE CONTROL

1. Only licensed software programs to be installed on the New Victory Hall computer systems and licence keys to be held securely by the Computer Security Manager.
2. New Victory Hall computers and networks must be protected at all times by up-to-date anti-virus and access prevention systems. Network devices must be configured to block inbound connections.
3. Any incidence of malicious code, whether actual or suspected, should be reported immediately to the Computer Security Manager who will treat the event as a security incident.
4. Use of attachable external media should be avoided but when use is necessary and approved within the context of the use of the computer systems, it must be restricted to the exchange of legitimate data files and not be used to add or remove software or inappropriate content.

INTERNET AND E-MAIL USE

1. Computer users should be aware there is no such thing as confidential e-mail unless appropriate security measures are put in place. Nothing should be written in any e-mail, either internal or external, that is confidential or could potentially bring The New Victory Hall into disrepute.
2. Correspondence via e-mail should not contain any personal data.
3. E-mail must not contain any material that may be deemed threatening, harassing, defamatory, libellous, offensive or obscene.
4. It is strictly forbidden to run non-approved software on New Victory Hall computers, whether or not such software is received via the Internet. Files found in contravention of this may be deleted without notice. File attachments received in e-mail that may reasonably be assumed to be non-business-related should not be opened.
5. Computer users who use the Internet on New Victory Hall computers must not visit sites which could contain material which may embarrass New Victory Hall or its Trustees or offend other volunteers or users in any way.
6. Mail (both incoming and outgoing) and Internet browsing may be monitored to ensure compliance with this policy.
7. All connections to the Internet must be via the secure New Victory Hall Internet connection unless explicit permission has been given in advance by the Computer Security Manager

Backup

1. The system backup and restore responsibility lies with the Computer Security Manager within the terms of the contract for supply of services.
2. In the event of system crash or corruption the Computer Security Manager will restore the system to its base configuration.
3. The New Victory Hall does not provide computer systems for purposes other than training and does not operate a data backup regime. New Victory Hall computer systems should not therefore be used to store any data that must not be subject to risk of loss or deletion.

Approval

Signed Ian McFadyen ______________________________

(On behalf of the New Victory Hall Management Committee)

Name Ian McFadyen

Date: March 2010

Position: Chairman