IT Security Manager: Broadland Computers lTd
Address: Greenacres, Brick Kiln Lane, Ingham, Norwich, NR12 9SY
Telephone no: 01692 581766 / 07939 127066
Email: enquiries@broadlandcomputers.co.uk

Scope of Policy Computer systems and equipment, including networks and internet access, in use within the Queen Elizabeth Hall, Worstead

Approved Uses Training

Objectve This policy sets out the guiding principles for use of Queen Elizabeth 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 Queen Elizabeth Hall computers and networks to be used for accessing and/or downloading inappropriate content in the form of software, images, audio files 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 exlcusive list of inappropriate use.

Policy
- The purpose of this Policy is to enable the Queen Elizabeth Hall to have a computer environment that its users can trust
- The committee have approved this Policy
- Computer systems will be protected against unauthorised access
- Internet access is only available to approved users
- Regulatory and legal requirements will be met
- The role and responsibility for co-ordinating computer security will be performed by the IT Security Manager
- Any exceptions to these poicies must have the written approval of the committee
- This Policy and its supplementary policies will be reviewed at least annually, by the IT Security Manager in conjunction with the committee
- It is the responsibility of all users, hirers, and their users to adhere to this Policy

System Access
- Computer assets must only be used in accordance of the guiding principles of the Queen Elizabeth Hall and th terms and conditions of Hall use
- External Users (third parties, suppliers, etc) who use the Queen Elizabeth Hall systems or data must be authorised to do so by the committee or under the terms and conditions of the hire agreement
- This computer and peripherals, including network devices should be secured in a locked cupboard within the Queen Elizabeth Hall when not in use
- Wireless access, if available must be through a secure hidden connection with strong password protection and device address restriction
- 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
- Only licensed software programs to be installed on the Queen Elizabeth Hall computer systems and licence keys to be held securely by the IT Security Manager
- Queen Elizabeth 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
- Any incidence of malicious code, whether actual or suspected, should be reported immediately to the IT Security Manager who will treat the event as an incident
- 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 & Email Use
- Computer users should be aware there is no such thing as confidential email unless appropriate security measures are put in place. Nothing should be written in any email, either internal or external, that is confidential or could potentially bring the Queen Elizabeth Hall into disrepute
- Correspondence via email should not contain any personal data
- Email must not contain any material that may be deemed threatening, harassing, defamatory, libellous, offensive or obscene
- It is strictly forbidden to run non-approved software on Queen Elizabeth 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 email that may reasonably be assumed to be non-business-related should not be opened
- Computer users who use the internet on Queen Elizabeth computers must not visit sites which could contain material which may embarrass Queen Elizabeth Hall or its committee or offend other volunteers or users in any way
- Mail (both incoming and outgoing) and internet browsing may be monitored to ensure compliance with this policy
- All connections to the internet must be via the secure Queen Elizabeth Hall internet connection unless explicit permission has been given in advance by the IT Security Manager

Backup
- The system backup and restore responsibility lies with the IT Security Manager within the terms of the contract for supply of services
- In the event of system crash or corruption the IT Security Manager will resore the system to its base configuration
- The Queen Elizabeth Hall does not provide computer systems for purposes other than training and does not operate a data backup regime. Queen Elizabeth Hall computer systems should not therefore be used to store any data that may be be subject to risk of loss or deletion

QEHW Signature 

(On behalf of the Queen Elizabeth Hall Management Committee)

Name Rodney Chapman

Date 01/11/2019

Position Chairman