National Video Conferencing Service

National VC Service – 3rd Party Code of Connection

Code of connection process

The applying Service Recipient shall forward a printed, signed and scanned copy of this completed code of connection to the National VC Service by email to vc.support@nhs.net.

This form is only required to be completed once per Service Recipient, updated and resubmitted after any change in the contact details,

This Code of Connection document refers to, and should be read in conjunction with, the VC service good practice guidelines that can be located at www.sctt.org.uk/resources.

National Video Conferencing Service

Introduction

Security Agreement

The National VC Team in conjunction with National Services Scotland provides the infrastructure to allow VC Service Recipients to make and receive video calls across the SWAN network and externally via an Internet gateway.

As part of delivering the VC network, the VC team provide security services such as:

- security management of the VC core service infrastructure;
- communication regarding planned maintenance and changes in the VC infrastructure;
- logical and physical access controls to core equipment and locations, including authorisation and any necessary security training and awareness of VC staff; and
- monitoring the network for any security attack or breach; to report any such incident; and to take steps to resolve the incident.

VC Service Recipients are responsible for:

- implementing and complying with their sector's or their local security policy;
- managing all risks associated with Service Recipient owned and managed systems;
- managing all risks associated with Service Recipient premises and staff; and
- managing all risks to which the Service Recipient may be exposed as a result of using the VC Service.

Compliance

Security Policy

The Service Recipient is committed to ensuring the confidentiality, availability and integrity of VC services and information passed using VC.

The Service Recipient meets all legal obligations, in particular those set out in the Data Protection Act relating to information security, by implementing appropriate information security policy, standards and guidance relevant to its sector.

National Video Conferencing Service

Risk Management

The Service Recipient recognises that VC makes possible a number of video and audio connections that may expose the Service Recipient to risk, including connectivity with unauthorised VC users. The Service Recipient is responsible for managing the risks associated with using the VC Service.

The Service Recipient ensures that all devices that will be connected to the VC Network are subject to internal information security risk assessment and management.

VC Security

The Service Recipient is responsible for preventing malicious traffic originating from within their organisation. In the event of such traffic being detected, the Service Recipient accepts that the VC Team may take steps to limit the traffic or to mitigate the impact of any such traffic. In the extreme case this may extend to suspension of the VC service to the Service Recipient until the situation is resolved.

Incident reporting and management

The Service Recipient must immediately report any security incident, or condition that represents a risk to the security of the VC Service by email to vc.support@nhs.net or by phone to the VC Service Desk on 01224 816666.

Use of VC Equipment

Safety of Supplied Equipment

Where VC and networking equipment has been provided, the Service Recipient is responsible for ensuring the following:

- the safe operation of the equipment, including regular PAT testing;
- equipment is safely stored to avoid damage;
- equipment is appropriately cleaned to prevent an infection risk;
- equipment is used in a safe manner to avoid toppling or falling;
- the device is not physically tampered with;
- no attempts are made to hack the device or interfere with the inbuilt security settings;
- WiFi networks are secure;
- equipment is used by authorised personnel only.

National Video Conferencing Service

Use of Supplied Internet Connection

Where an internet connection has been supplied as part of the VC service:

- The Service Recipient must abide by the Terms and Conditions of Service associated with the Internet Service Provider.
- The Service Recipient must ensure the integrity of the local network by maintaining adequate security for wired and wifi connections. Unauthorised devices should not be connected to the network.
- Sufficient bandwidth to undertake video calls should be maintained at all times.

Use of Attend Anywhere

Where services are provided via the Attend Anywhere video consulting platform the Service Recipient must ensure that:

- Security of the system is maintained. Users must not share passwords or attempt un-authorised access.
- Locally administered accounts are only created for authorised users (staff members or volunteers).
- Staff members or volunteers accessing the system must have the appropriate level of Disclosure to comply with the Protection of Vulnerable Groups (Scotland) Act 2007.
- User accounts of staff members or volunteers are deleted upon leaving.

VC Code of Conduct

The Service Recipient is responsible for ensuring that the VC system is used in a responsible manner and in line with appropriate service guidelines. VC equipment and services must not be used for:

- making malicious calls;
- undertaking commercial activity;
- engaging in behaviour likely to cause offence.

National Video Conferencing Service

Statement

The signatories confirm that they have read and will comply with all the conditions set out in this agreement.

Service Recipient	
Organisation name	
Company/ Charity/ other registration number	
Organisation postal address	Line 1 Line 2 Line 3 City Post Code
Service Recipient Senior Manager or equivalent	
Name	
Email	
Telephone	
Signed	
Date	