Videoconferencing safety

Videoconferencing is a very powerful way to collaborate, with considerable potential benefits for education. However, like any communication technology, videoconferencing can be misused. Janet Videoconferencing is designed to be flexible so as to allow a wide range of educational uses. This inevitably means that safety relies more on end users and organisations making their own appropriate choices than on restrictions built into the services. This factsheet provides some guidelines on how to set up and use videoconferencing safely.

Setting Up Conferencing Equipment

Safe videoconferencing begins with the initial setting up and registration of the videoconferencing device, which may be anything from a dedicated studio to a laptop with built-in microphone and camera. As videoconferencing is a two-way technology, cameras and microphones should be located in rooms where there is the least risk of private activities being accidentally seen or overheard.

In most cases, registering a videoconferencing device will place it in a directory that can be read by all other users of the same service. The name associated with the device will normally be that of the person doing the registration, but another name may be appropriate in some cases.

Unless special controls are arranged it should be assumed that Janet Services and their directories of users will be available to all users of Janet, whether staff or students, in schools, colleges, universities or elsewhere. Other videoconferencing services may be available to anyone on the Internet. For this reason it is unlikely that these videoconferencing services will be suitable for unsupervised use by young people. In general, videoconferencing devices should only be placed in locations where physical access to them can be controlled and monitored: this may involve locking them away when not in use.

Network access to the videoconferencing device should also be restricted where possible, by using controls on routers, gateways or firewalls. For example, controls may be used to require all calls to take place via Janet videoconferencing or a local or regional gatekeeper: this will ensure that the device and its users benefit from security measures implemented by those services. Where the videoconferencing device can be managed across the network (for example, through a web interface), passwords and router controls must be used to ensure that this interface cannot be misused by unauthorised local or remote users.

Incoming Calls

As soon as a videoconferencing device is registered in a directory others may attempt to call it at any time. If the device is set to answer such calls automatically then a conference may be set up without any further human action. Once this happens the device is likely to transmit sounds and pictures to an unknown remote location, with only a small on-screen indication

that this is happening (which will not be visible if the monitor is turned off).

There are two ways to avoid this:

- Always disable the auto-answer function. This means that all conferences will need to be pre-arranged by phone or e-mail, but it is the safest option.
- Alternatively, enable auto-answer, but ensure that the camera and microphone are always switched off when a videoconference is not in progress. This will allow callers to use their videoconferencing software to request a conference, but the local user controls what can be seen and heard. However, with this option, there is a risk that a user will forget to switch off at the end of the conference, leaving the system 'live'.

Participating in Conferences

When participating in a videoconference it is easy to forget who may be able to see and hear you. All conference participants should therefore follow good practice both before and during conferences:

- Find out in advance how the service you are using controls people joining, monitoring or recording a conference. This will usually be part of the service documentation.
- Do not assume that the person who answers your call is the person named in the directory for that device.
- Ask everyone who can see or hear the conference to introduce themselves. If a participating site is forwarding the conference to others—through their own multipoint conferencing unit, for example – or has technicians able to see or hear the conference, they should remind the other participants of this.
- If a conference is being recorded, all participants should consent to this in advance and should be reminded of the fact during the conference. Conference participants may hold individual intellectual property rights in any recording and may wish to have control over how it is used.

Use of JVCS is logged to assist with investigating faults and complaints, for billing (where necessary), reporting and capacity planning. Those registering videoconferencing devices with Janet videoconferencing should be aware that logs will show all activity from the device as being their responsibility, so should ensure that they control access to the device or access credentials carefully.

Videoconferencing Policy

It is recommended that all organisations using videoconferencing develop a policy on which services may be used, which members of the organisation can use them, and under what conditions. The documentation for the Janet Services will help to determine which services are appropriate and whether additional controls are needed. Other videoconferencing services designed for specific groups of users may provide fewer or more security controls: see their documentation for details and adapt your local policy as appropriate. The policy should also include rules on acceptable conduct in videoconferences to prevent misunderstandings, offence or breach of privacy. Where a conference takes place over JANET, it is also subject to the Janet Acceptable Use Policy [1].

Links
[1] http://community.ja.net/library/acceptable-use-policy