Broadband & WiFi in Village Halls

Increasingly local businesses and other organisations, including village halls and community buildings, are looking to install and offer broadband and WiFi access to their users. There are a number of issues that should be considered when planning this, including costs, security and WiFi coverage:

Initial Connection

Many Halls and Community buildings do not have an official post office address. This can cause problems as some ISP's may not accept orders for new service without an address. If this is the case:

- Request an official address from the Post Office. When this is done then most ISP's will accept an order.
- Find an ISP who will accept an order for an "unserved" building. There may be a requirement for an initial survey before an order is confirmed.
- Place an order for a new telephone line with BT.com then upgrade to broadband. This could mean that you have to agree to a minimum contract term on the new service.

Costs

Potential costs and issues:

- Installation, connection, on-going charges.
- Village halls need a Business contract (not Residential) – shop around for best deals on price comparison websites
- Consider how the on-going costs will be met. Review the standard hire charges for the hall.

When shopping around for best deals and prices, you need to balance cost with reliability and service support. Try a few price comparison websites for deals in your area and make sure you check any contract Terms and Conditions. Most comparison sites will have reviews and ratings for all ISPs they include.

(Check our "ISP Questions" and "Handout 1" leaflets available on www.ConnectingCumbria.org.uk/Digital-Inclusion for more advice).

Security

End User access to wifi needs to be managed, unless the hall management committee decides to offer unmanaged and unfiltered access.

The risk of allowing unmanaged access is that people use the broadband service to download/upload content that is illegal, criminal, copyrighted or pirated. This could lead to a degree of liability for those providing the WiFi.

In addition, there has been a growing incidence of broadband routers being hacked, allowing hackers access to any device using the router. This results in things like:

- loading the Miraj virus onto a router to support DDOS attacks, and could also lead to
- infecting devices which then connect via the router (e.g. PC's, Tablets and webcams) and
- blocking internet access to all users

BT

Cumbria County Council

Department for Culture Media & Sport

Funded by UK Government

NOW'S THE TIME FOR SUPERFAST BROADBAND
gov.uk/gosuperfast
HM Government

There are a number of simple actions that can be taken to minimise risk:

1. Make sure that the router is in a secure area with physical access for authorised users only. Allowing anyone to log into a router directly using an Ethernet cable is a risk, as they can make unauthorised changes.
2. Change/Update the administration ID and passwords for the router: (N.B. This is not the public WiFi access password).

   Any configuration/password changes are made by logging into the router. Connect to router and enter the IP address (usually on the back of the router or instruction booklet e.g.192.168.1.1) into the search field of your internet browser. This allows access to router management.

   Change the router admin User ID and password to prevent unauthorised changes to router configurations and make hacking the router more difficult. Some ISP's recommend this when first setting up.

   - ✓ Go into "Security" and change the user ID and Password. Choose a unique ID and Password.
   - ✓ This only needs to be done once (unless the Admin ID and password are given to an unauthorised user). Keep the ID and password in a secure place.
3. Change the public WiFi access password (current one is usually on the back of the router) on a regular basis.
   - ✓ Login to router using the same process as above and change the WiFi password.
   - ✓ Recommend changing the public access code regularly (at least monthly) to prevent unauthorised access.
   - ✓ Consider changing the code for any commercial hall booking
4. Most routers now include a Firewall which is usually switched to the lowest security setting. Make sure the 'parental control' setting is switched on to prevent access to unsuitable websites Use any Firewall settings on the router to set the level of restriction (see the router instruction manual for specific routers).
5. Include the use of WiFi in your hiring agreement for those using the hall. A model hiring agreement is available free of charge to village halls in Cumbria on request from ACTion with Communities in Cumbria, visit: www.cumbriaaction.org.uk/ContactUs.aspx.

WiFi Coverage

WiFi coverage from the router across the building may be OK, but signal strength reduces as you move away from the router and may not cover all of the hall or centre.

- Using WiFi hotspots can improve coverage in any open areas, particularly for multiple users. These don't have to be expensive and are easy to set up and move about. Signal strength across different areas can be simply tested using a PC or Tablet.
- WiFi hotspots use the existing electrical circuitry in the property to rebroadcast the broadband signal around the hall. There are many types and brands available from BT, Amazon, PC World and other suppliers, shop around and chose one you're happy with.
- More information here: www.shop.bt.com/mini-sites/connected-home/home-hotspots/

More Information Links:

https://us.norton.com/costly-mistakes-wifi/promo

www.computerworlduk.com/security/are-public-wi-fi-hotspots-really-major-security-risk-3623447/

http://futurethinking.ee.co.uk/what-small-businesses-need-to-know-about-the-legal-and-security-risks-of-offering-public-wi-fi-services/

www.premitel.uk/consultancy/expert-advice/how-do-i-ensure-that-my-wifi-hotspot-service-is-legal/