



# *Blisworth*

## **BAPTIST CHURCH**

TO KNOW HIM AND MAKE HIM KNOWN

### **Wi-Fi Access and Acceptable Use Policy**

This policy is a guide to the acceptable use of the Blisworth Baptist Church wireless network facilities and services, provided free of charge as a convenience to users of the building. Any individual connected to the wireless network to use it directly or to connect to any other network(s), must comply with this policy, the stated purposes and Acceptable Use Policies of any other network(s) or host(s) used, and all applicable laws, rules, and regulations of England and Wales.

Blisworth Baptist Church makes no representations or warranties concerning the availability or security of the wireless network, and all use is provided on an as-is basis. By using the wireless network you agree to defend, indemnify and hold harmless Blisworth Baptist Church for any losses or damages resulting from your use of the wireless network. Technical support is not provided and there can be no guarantee that you will be connected to the Internet.

Blisworth Baptist Church takes no responsibility and assumes no liability for any content uploaded, shared, transmitted, or downloaded by you or any third party, or for anything you may encounter or any data that may be lost or compromised while connected to the Wireless Network.

You are responsible for keeping your computer secure against unauthorised access and free from malicious code and viruses.

This is through minimising the risks of cyberattacks including:

1. Keeping software up to date;
2. Runup-to-date antivirus software;
3. Use strong passwords(consider using a long password that is not based on personal information) and do not tell them to anyone;
4. Change default usernames and passwords;
5. Implement multi-factor authentication;
6. Installing a firewall;
7. Be suspicious of unexpected emails (be wary of unsolicited attachments; keep software up to date);
8. Backup data.

Blisworth Baptist Church reserves the right to disconnect any user at any time and for any reason. The wireless network is provided as a courtesy to provide our hirers access to the Internet.

Inappropriate use of the wireless network is not permitted.

This policy does not enumerate all possible inappropriate uses but rather presents some guidelines (listed below) that Blisworth Baptist Church may at any time use to make a determination that a particular use is inappropriate:

- Users must respect the privacy and intellectual property rights of others;
- Users must respect the integrity of our network and any other public or private computing and network systems;
- Use of the wireless network for malicious, fraudulent, misrepresentative purposes or in any way illegal under current law;
- Use of the wireless network to upload computer viruses, carry out hacking, upload/download defamatory, offensive or illegal material;
- Activity which is defamatory, threatening or intimidating or which could be classed as harassment;
- Contain obscene, profane or abusive language;
- Contain pornographic material whether in writing, pictures, films or video clips;
- Contain offensive material regarding sex, race, religion or any disability or sexual orientation;
- Nothing may be installed or used that modifies, disrupts or interferes in any way with service for any user, host or network;
- Make available by any means any material, unless you are the copyright holder of that material, or have the licence to make that material available, or the material has been expressly put into the public domain and you can demonstrate this;
- Access network services in such a way as to deny reasonable access to the network for other users by, for example, excessive use of network bandwidth for music or video streaming or very large downloads;
- Infringe third-party rights.

Blisworth Baptist Church will not collect personally identifiable information when providing these facilities. Our router may collect technical information from your device necessary to provide access to the Internet, which may be logged to detect crime or where necessary to block access from a specific device.