**Bluntisham Baptist Church INFORMATION TECHNOLOGY POLICY**

|  |  |
| --- | --- |
| **Primary Responsibility** | **Trustees** |
|   |   |
| **Issued** | **Date November 2023** |
| **Status** | **Vs 1.1 Agreed** |
| **Review Period** | **3 years** |
| **Next Review Date** | **November 2026** |

**DISTRIBUTION**

|  |  |
| --- | --- |
| **Original** | **Church Office** |
| **Copy** | **Website** |
| **Copy** | **Trustees** |

**If printed this document is UNCONTROLLED**

**Information Technology Policy**

**1.0 Overview**

This policy addresses the use of Information Technology (IT) equipment, the Church Website and Social Media sites. Users are responsible for their behaviour and communications. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy.

**2.0 Church Equipment either on Church Premises or at Home**

**2.1 IT Equipment**

2.1.1 All church owned IT equipment should have the following set up on it to protect the user and any sensitive personal information which is stored about church members.

1. Functioning and up to date Antivirus software on Windows PCs.
2. If used by children / vulnerable adults a suitable content filtering software.
3. Ideally, Sensitive Personal Information should not be stored.  If Sensitive Personal Information has to be stored the data must be encrypted.
4. Sensitive personal information should not be shared by email, or other electronic communication unless encrypted.

5. All computers must comply with the Data Protection & GDPR policy.

**Note:** Sensitive Personal Information is defined as: personal data which consists of information concerning a person’s racial or ethnic origin, political opinions, membership of a Trade Union, physical or mental health condition, sexual life, commission or alleged commission of any offence, a record of any proceedings for any offence committed or alleged, or a record of any sentence or proceedings.

2.1.2 All church owned equipment may be subject to audit at any point in time with the approval of the deacons.

2.1.3 If Sensitive Personal Information is stored on personally owned computers used for church business, then these criteria also apply to the personally owned computers.

2.1.4 Church IT equipment should be listed detailing the location of the equipment and who it is linked to.

2.1.5 Unattended Computers, Macs and PCs should be secured at church (either in the office or other secure location) or in the users home.

**2.2 Church Internet and Wifi**
It is important that computers used in connection with church activities have adequate security software and that programs and operating systems are regularly updated to ensure that security fixes are applied in a timely fashion. This should be updated annually or in line with the security program i.e. A multiple year subscription.

There is potential for email and other accounts to be hacked and data accessed by unauthorised users. Changing passwords regularly and ensuring that they are robust (not obvious like dates of birth) and kept secure (not accessible by unauthorized users), reduces this risk considerably. You should be aware that every Internet site you visit is capable of determining who you are, and whom you represent.

As a result of this;

* Passwords on church owned computers should be changed annually, this is the responsibility of the user.
* Wi-Fi Passwords in all church buildings (not including the manse) should be changed annually.
* Passwords to individual devices should not be shared i.e. to open an individuals laptop that contains sensitive information.
* Wi-Fi passwords should only be shared to those who have read and understood this agreement e.g. administrator, techie team, hirers and Sunday School Leaders.

Accordingly, access to the Internet should include the use of good judgment, common sense, and careful discretion. The following rules apply:

1. Internet access should be limited to appropriate Church use only. Visiting adult sites or access for more than minor personal use is prohibited.
2. Use of the Church’s Internet in attempts to gain unauthorized access to remote systems is prohibited.
3. The Church Wifi is only to be used by approved people and gives unfiltered access to the Internet.

2.3 If the Church policy has been seriously violated by the ministers, officers, employees, volunteers or members, they will be subject to disciplinary procedures, up to and including immediate termination of employment / Church Membership and even criminal proceedings.

**3.0 Church Web Page and Social Media Policy**

3.1 General Policy

Bluntisham Baptist Church (BBC) values the potential good that comes from web pages, social networking pages, blogs, texting, instant messaging, e-mail and other forms of electronic social networking/communication. Simultaneously we recognise that misunderstanding, personal offense, hurt, legal exposure and damage to church community can potentially accompany use of these mediums.

The Apostle Paul instructs that “Everything is permissible but not everything is constructive. Nobody should seek his own good, but the good of others.” With the principles of 1 Corinthians 10:23-33 in mind, all church employees and volunteers are to abide by the following communication guidelines.

All information shared on the Church Website, Church Facebook page or other social media site should be considered public domain information. It is available to anyone visiting the Church. There is an important exception of the Church Directory which is password protected.

3.2 Ensure Integrity

Electronic communications should be consistent with the teaching of scripture and the values of BBC. Nothing should be written online that would not be said in person as a representative of the church (Proverbs 10:9). If a public dialogue gets heated, it is best to stop using a public forum and make the conversation private (Matthew 18:15-17). Leaders are expected to have the foresight to anticipate, within reason, how their words and/or actions may be perceived by their audience and to those under their care.  It is highly recommended that any potentially difficult posting should be reviewed by the Deacons.

3.3 Promote Credibility

Facts should be checked to ensure they are correct; in proper context and that positions are justifiable (1 Corinthians 13:5-7). Response to those who disagree should be in a spirit of love and grace (Luke 6:28-30). Electronic communications should not be used to resolve interpersonal conflicts that are best handled face-to-face. It is highly recommended that any potentially difficult posting should be reviewed by the deacons.

3.4 Keep Confidences and Avoid Libel

Communications should not inadvertently share confidential information (sometimes we deal with a lot of confidences in church work so extra care must be taken with this). With any public postings the author is legally liable for what is written. Laws governing slander, libel, defamation and copyright apply. Outside parties can pursue legal action against individuals for postings.

 3.5 Do Not Engage in Polarising Political Speech

As a charity the government does not tax BBC as if it were a business, because of this however, there are certain restrictions placed on charities such as ours, specifically we cannot be seen to endorse or support political candidates. Nothing in public communications should lead people to believe that BBC is endorsing a political candidate or party.  Any public posting on a political issue which is made speaking on behalf of the church must be agreed by the Deacons.  It is recognised that Church ministers may wish to speak in their own right on political issues when posting on private blogs, facebook postings, tweets etc., but they should make it clear that this is their own view and not necessarily the view of the church and church IT platforms should not be used in these cases.

3.6 Respect the Church and its Staff

Since electronic communications are public (or easily made public), we expect everyone associated with us to be respectful to the church and leaders, employees, volunteers and members. Any employee or member who uses electronic communications to disparage the name or reputation of the church, its practices, or its ministers, officers, employees, volunteers or members will be subject to discipline, up to and including immediate termination of employment / Church Membership.

3.7 Limit Expression in Written Words

Remember that written words can easily convey the wrong message. Written words do not have the “non-verbal” channels that accompany face-to-face communication. Missing are body language, facial expressions and tone of voice that can help ensure proper context. As such, reread everything prior to sending. See if there is any possibility of misunderstanding. Every year the church deals with many relational problems brought on by poor word choices or communications sent in anger/haste. A good motto is “Think before you press send”.

3.8 Specific Guidance for Communication with Children and Vulnerable adults

Although paper records are preferred, there are times when information needs to be stored electronically. In this (rare) case:

* Electronic records should be password protected and backed up regularly. A secure server (e.g. a cloud based server) is preferable. Systems should be virus protected. Data must never be stored on personal computers, USB drives or other removable media unless it is securely encrypted.
* Passwords should be hard to guess and always stored separately.

3.10 Conclusion

BBC understands the good that comes from electronic communications and social networking. It is not our desire to create consternation or dampen creativity when it comes to the use of these media. At the same time we recognise the tremendous potential for hurt and misunderstanding that go with these media. We trust that by following these guidelines and common sense, we are all able to both reap the rewards of electronic communications and avoid their potential pitfalls.

Related Policies:

Data Protection Policy

GDPR Policy

Safeguarding Policy