St. Edward the Confessor

IT and Social Media Policy

1.0 Overview

This policy addresses use of Information Technology (IT) equipment on church premises and also remotely e.g. church web site and social media sites. It is specifically designed to protect all users.

2.0 Church Premises Equipment

2.1 IT Equipment

2.1.1 All church owned IT equipment should have the following set up on it to protect the user.
1. Automatic downloading and applying of security update patches.
2. Functioning and up to date antivirus software.
3. Sensitive personal information should not be stored on church computers.
4. Sensitive personal information should be stored on removable devices (e.g. memory stick) and kept locked away.

2.1.2 All church owned equipment may be subject to audit at any point in time.

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.

2.2 Church Internet and Wifi

You should be aware that every Internet site you visit is capable of determining who you are, and whom you represent. 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 personal use is prohibited.
2. The Church Wi-Fi is password protected and is to only be used by approved people.

3.0 Church Web Page and Social Media Policy

3.1 General Policy

All information shared on the church web site, church Facebook page or other social media sites should be considered public domain information. It will probably have also been printed and available to anyone visiting the Church. Therefore details of events, reports, contact information for organisations including email addresses and telephone numbers can be shared publicly on the Internet.

3.2 Ensure Integrity

Nothing should be written online that would not be said in person as a representative of the church. If a public dialogue gets heated, it is best to stop using a public forum and make the conversation private.

3.3 Promote Credibility

Facts should be checked to ensure they are correct. 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 administrator.

3.4 Keep Confidences and Avoid Libel

Communications should not share confidential information.

3.5 Specific Guidance for Social Media

The following guidelines relate to the use of Facebook but apply in principle to all social media platforms to ensure safe practice.

- One named person as an administrator for the page who can approve contacts and give access to others.

- All information – news, events, information or reminders should be posted rather than using one to one private/inbox messages.

- Keep up to date with Facebook policies e.g. age, privacy settings etc., noting that at present Facebook requires all users to be over the age of 13 years.

- Ensure that permission has been given for photo use, particularly children, and that no picture is tagged or used as a personal profile picture.

3.6 Conclusion

St Edward's Church 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.

The following information at St Edward's Church is sensitive personal information and needs protecting as detailed in our Data Protection Policy.

1. Church Electoral Roll
2. Funeral, Baptism and Wedding details.
3. Financial information of giving by individuals.

3.7 Administrator

For the purposes of this policy the named administrator is Mr J Gostelow

Agreed by PCC April 2024