# Appendix 5

## Use of Church IT

All Church owned IT equipment must be set up to automatically download and apply security updates and have functioning and up to date antivirus software installed.

Any sensitive personal information that is stored must be encrypted and must not be shared by email, or other electronic communication unless encrypted.

All portable IT equipment must be protected with a password, which must not be shared. If compromised, a password should be changed immediately.

Passwords should be as secure as possible and must not be written down.

IT equipment must be kept secure and must not be left unattended when in a public environment. When IT equipment has to be left unattended in a vehicle, it must be hidden from view.

All Church owned equipment should be returned on leaving a post.

### Use of the Internet

The Church 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 the Church can potentially accompany use of these media. All workers are to abide by the following communication guidelines.

Internet access should be limited to appropriate Church use only. For example, visiting pornographic adult sites and gambling sites is totally prohibited.

Use of the Internet in attempts to gain unauthorised access to remote systems is prohibited.

### Ensure integrity

Electronic communications should be consistent with the teaching of scripture and the values of the Church.

Nothing should be written online that would not be said in person as a representative of the Church.

Staff 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 an Church colleague.

### Promote credibility

Facts should be checked to ensure they are correct; in proper context and that positions are justifiable. Response to those who disagree should be in a spirit of love and grace.

Electronic communications should not be used to resolve interpersonal / church conflicts that are best handled face-to-face. It is highly recommended that any potentially difficult posting should be reviewed by an Church colleague before sending.

### 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.

### Do not engage in polarising political speech

As a charity we cannot be seen to endorse or support political candidates. Nothing in public communications should lead people to believe that the Church 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 Church Secretary or Minister.

It is recognised that Workers may wish to speak in their own right on political issues when posting 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.

### 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 Church workers. Any member of staff who uses electronic communications to disparage the name or reputation of the Church, its practices, or its Ministers, Trustees, or Workers will be subject to discipline, up to and including immediate termination of employment.

### Limit expression in written words

Written words can easily convey the wrong message as they do not have the “non-verbal” channels that accompany face-to-face communication - body language, facial expressions and tone of voice that can help ensure proper context are missing. Staff should re-read everything prior to sending to check if there is any possibility of misunderstanding and consult a colleague if in any doubt.

### Specific guidance for communication with children and vulnerable adults

All interaction via social media sites with children and vulnerable adults should be via the Church’s platform accounts and not through the any Church staff’s personal individual platform accounts.

It is the Church’s default practice not to make one on one connections with young people through social media, though it is acknowledged that this is a useful communication tool. On rare occasions it might be necessary, but this should be for a specific purpose and then the conversation terminated. It is expected that each sub-group within the Church will find its own way of using social media to communicate within the law and in a way that is a positive, safe, experience for all members of the group.

### Personal Use

The Church recognises that personal access the web at work helps employees to maintain a positive work life balance.

Limited and ‘reasonable’ personal use of the web is permitted. Personal use of all other systems is prohibited.

Web access may be monitored to ensure compliance with policy. Employees that choose to make personal use of Church systems do so in acceptance of the monitoring measures outlined in this policy.

Personal use of these systems is a privilege. The Church reserves the right to withdraw it either individually or globally at any time without notice or explanation.

### Sensitive Information

The following is information that the Church believes is Sensitive Personal Information (and needs protecting as stated in the Church IT policy.

* The Church Members’ Directory and all databases
* Minutes of meetings of Church Elders/ Deacons / Leadership/Members
* Correspondence from and to all Members
* Any personal file that a member of staff might keep on a Member
* Church financial information
* All Church Safeguarding matters