Church Cyber Security Policy

For All Saints Headley Guildford Diocese

Purpose of the policy

Electronic communications are incredibly powerful but can be misused accidentally or maliciously. You need to keep with the following procedures in order to protect yourself, other members and the church.

Any electronic devices owned by the Church may be used if prior permission has been sought by the Incumbent and should be returned to the Incumbent when no longer in use. The user is responsible for regularly updating the device e.g. anti-virus, Windows updates etc

The majority of devices to which this policy refers, will be owned individually.

All electronic communication must be carried out in accordance with the Church Privacy Notice and this policy.

It is your responsibility to read, understand and comply with the policy.

1 PC computers

1.1 Password Security

All devices used to access church communications must have a password set in order to unlock the device.

It is good practice to ensure that a screen saver comes on after 10 mins and that passwords are changed every 3 months.

Use strong passwords with a mixture of upper and lower case letters, numbers and non-alphabetic characters. Do not use very short passwords. Do not let anyone else know your password. Do not write down your password and leave close to the computer. Do not use the same password for multiple sites or devices. Do not communicate your password to others.

1.2 Security

To safeguard devices from hacking, make sure that an up to date anti-virus programme is installed and that automatic updates are enabled. Firewalls should be used. Consider using malware software.

2 Laptop, Mobile phones, Tablets and Internet watches

2.1 Password security

These devices can be easily stolen, accessed, cloned or lost. Therefore they need to be password or biometric protected. It is good practice to update these passwords every 3 months with strong

passwords. Do not write down your password and leave close to the device. Do not use the same password for multiple sites or devices. Do not communicate your password to others.

2.2 Security

Phones and tablets generally do not need extra antivirus software installed. Make sure that your device is set to update daily.

Only download apps from an acknowledged site eg Google Play etc

Laptops should have an up to date anti-virus programme installed and set so that automatic updates are enabled. Firewalls should be used. Consider using malware software.

2.3 Physical Security

Make sure that your devices are not left in sight in vehicles or unattended in public places. If devices are in bags then make sure they are closed. Do not show expensive devices in public e.g. bars, public transport etc. Do not lend your device to others.

Consider use of software to enable your device to be tracked in the event of theft.

It is good practice to delete downloaded files once used so that in the event of theft these files cannot be accessed.

3 WiFi

When connecting to Wi-Fi at home, make sure that the router is secure and has a password enabled. When connecting to Wi-Fi elsewhere, be aware that the security may not be good so avoid downloading sensitive or confidential material.

4 Backups

4.1 Password Security

All files etc should be backed up. If USB sticks, CD ROMs, removable hard drives are used then these should be password protected. Do not write down your password and leave close to the storage media. Do not use the same password for multiple sites or devices. Do not communicate your password to others.

5 General

5.1 Email

Emails should be written with content and language suitable for church purposes. Do not use abusive, obscene, discriminatory, derogatory, defamatory or harassing language. Emails can be the subject of legal action and must be written in accordance to GDPR and the Data Protection

legislation. It is not a secure method of communication so do not send sensitive or confidential material. Any such files should be password protected or encrypted.

Use BCC if sending to a list of people so that email addresses are not routinely shared.

Be careful when opening attachments. **Do not open** if unexpected or suspicious.

5.2 Loss or Theft

In the event of any church owned device being stolen, the Incumbent should be immediately informed. If any personal device or storage media is stolen in which church information is held e.g. files etc, then the Incumbent should be informed. This may be a data breach.

Take extreme care of USB sticks and CD ROMs as these can easily be lost.

5.3 Photographs

Photographs may only be taken if permission has been given on the Consent Form. For children's photos, the parents should fill in the Child Photo permission form. Digital photos should not be given a file name that refers to the name of the person/child. Do not store these photos once they have been used.

5.4 Social media – Church account

Consent forms/child permission forms for all photos should be in place. When uploading photos, do not use the surname of the person in the post. For children, do not use first or second names. Posts should be written with content and language suitable for church purposes. Do not use abusive, obscene, discriminatory, derogatory, defamatory or harassing language.

5.5 Other Devices

5.6 The general security considerations outlined in this policy shall apply to other devices which can connect to the internet e.g. wearable technology, the 'internet of things' etc.

This policy was approved by the PCC at the meeting on July 31st 2019 unanimously

Rev Dr A Barton, chair and Rector