ST MARY'S CHURCH NEWICK PAROCHIAL CHURCH COU NCIL

POLICIES FOR THE USE OF CHURCH COMPUTERS, AND PRIVATE COMPUTERS WHICH HAVE ACCESS TO OR STORE CHURCH INFORMATION

The Parochial Church Council adopted this policy on Thursday 14th November 2019

- There are at least 7 people within St. Mary's Church undertaking voluntary work for the Church using private computers storing sensitive information relating to vulnerable adults and children which the PCC needs to be aware of. Plus a part-time Administrative Assistant to Rev'd Paul Mundy and the editor for the Parish Magazine who have had laptops purchased by the PCC.

- **Personal Responsibility** 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.

  Privacy – Will not reveal any personal information (e.g. home address, telephone number, social networking details) of others unless to those preparing documents for Church Use, Pastoral Team and Emergency Services

- **Internet access** is readily available but unfortunately, computers are vulnerable to security risks such as viruses, malware, or keyloggers (which record users' keystrokes). 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. Sensitive data is often transferred via the internet or stored in 'cloud' servers in locations remote to users. There is potential for email and other accounts to be hacked and data accessed by unauthorized 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. It is important that after using the computer for Church use the User logs off correctly.

- **Emails** frequently arrive containing spam (unsolicited email) and may have dubious or risky content. Email users must not open anything suspicious. Instead such items should be marked as JUNK to be checked later by someone with IT skills who can identify whether those items are safe or not. Bearing in mind that clergy and members of the congregation share group emails, adhering to safe practice with emails is important.

- **Passwords -** These should be changed regularly for every website or account online. Similar or identical ones are easy to hack into once one of them is 'broken'. The recommended safe practice is for passwords to be recorded and stored securely. If the secure storage is compromised all passwords would need to be renewed.
  Passwords are not shared with other users.

- **Data Protection** Act –
- Data Protection Forms authorizing permission to keep information has been completed by members of the Church congregation.
- Not send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting.
- Will not attempt to harm or destroy any data relating to Church Information
- Not publish any photo's without the consent of the people / parents in the photo
- DRB checks are currently carried out where required.

- **Documentation**
  Where papers are held for Church administration purposes these should be treated as confidential unless clearance is obtained from the relevant person(s), keeping them in a safe and secure place.

These policies aim to ensure that the PPC takes full account of all legal requirements, including but not limited to GDPR and safeguarding requirements, for the use of Church computers and private computers with access to/storage of Church information".

Rev'd Paul Mundy & Chairman for the PCC.....

Date.....

I note and agree with this policy

Name ……

Date ……..

I undertake that any papers I have in my possession will be kept in a safe and secure place.

Name ……..

Date…….