I

PROTOCOLS FOR ALL COMPUTER USERS IN THE EXECUTION OF ANY DIOCESAN FUNCTION IN THE DIOCESE OF LANCASTER (THE "DIOCESE")

1 ACKNOWLEDGEMENT

1.1 The Bishop and the Trustees of the Diocese recognise and acknowledge that a vast amount of data is processes by people who are not employees or receive and remuneration. Consequently, personal computer equipment, in all its forms, are used on a regular basis. The monitoring of usage and suitability of equipment is a task beyond scope. However, these recommendations are given to emphasise the importance that the Diocese attaches to GDPR in order to protect the data subjects, the Diocese and those who process data under the umbrella of the Diocese.

1.2 The majority of these recommendations will be second nature to computer literate people.

2 PASSWORDS

2.1 A separate password must be used when accessing Diocesan data.

2.2 Data must be password protected when being sent via e-mail or other electronic devices. The password must be sent separately.

2.3 Users of the Diocesan mainframe must keep their passwords confidential and not share them with other users.

3 EQUIPMENT SECURITY

3.1 Diocesan personnel are responsible for the security of equipment allocated to or used by them. Diocesan personnel should lock, shut down or suitably secure equipment when not in use.

3.2 Equipment, especially mobile phones and tablets must be password protected and need to have tracking enabled and the ability to deactivate these remotely if they are lost or stolen.

3.3 Memory sticks should be either automatically encrypted or the data on them encrypted and password protected.

3.4 Virus protection systems must in place at all times and security updates implemented immediately on all equipment used for diocesan purposes.

4 SYSTEMS AND DATA SECURITY

4.1 Diocesan personnel must be alert to potential threats to cyber security and must not click on or open suspicions links or attachments

4.2 Diocesan personnel who usually have access to the mainframe but are having to use equipment that is not connected must back up the data and have it downloaded to the mainframe as soon as practical.

5 EMAIL

5.1 Diocesan e-mail accounts are for Diocesan use only.

5.2 Be aware of suspicious looking e-mails especially those with attachments.

I

5.3 Give careful consideration to what you write as there is no control over to where that email may be forwarded.

5.4 If an e-mail is received in error the sender must be contacted and advised of the same. E-mails sent out in error must be followed up with a withdrawal e-mail and the appropriate line manager informed.

5.5 Care should also be taken regarding distribution lists. The bcc option should be used. Users should consider carefully whether a reply needs to go to all recipients.

6 USING THE INTERNET

6.1 Websites that have an immoral or subversive content will not be accessed at any time. Any accidental access should be reported and recorded.

7 PERSONAL USE OF DIOCESAN SYSTEMS

7.1 Diocesan personnel who have access to the Diocesan mainframe systems should not use these systems for personal use.

8 MONITORING

8.1 Where it is technically possible emails may be monitored or retrieved.

9 PROHIBITED USE OF OUR SYSTEMS

9.1 Misuse or excessive personal use of Diocesan telephone or email systems or inappropriate internet use is not permitted and will, where applicable, be dealt with in accordance with a current contract of employment.

10 SYSTEM MAINTENANCE

10.1 Due consideration should be given to permanently deleting emails that are classed as ephemeral e.g. circulars, notification or invitation to a meeting.

10.2 Attachments should be saved in files

10.3 Frequent emptying of the recycling bin should take place.