COMPUTER USAGE POLICY FOR THE DIOCESE OF LANCASTER (THE "DIOCESE")

1 ABOUT THIS POLICY

1.1 This policy highlights the standards that are expected of anybody who has a role in the Diocese[1] and the usage of computer systems[2] that is appropriate to that role. This policy applies to paid employees, volunteers and clergy. Misuse of these systems may lead to sanctions being taken both internally and externally. **nb** The Diocese has limited computer capacity in terms of mainframe and users.

2 PERSONNEL RESPONSIBLE FOR THE POLICY

2.1] The Diocesan trustees have overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework. Day-to-day responsibility for operating the policy and ensuring its maintenance and review has been delegated to the Head of Committees/Commission and Services and Parish Priests with the assistance of the Data Protection Officer.

3 EQUIPMENT SECURITY AND PASSWORDS

3.1 Diocesan personnel are responsible for the security of equipment allocated to or used by them. provided to them. Diocesan personnel should lock, shut down or suitably secure equipment when not in use. Strong passwords should be used and log on ids and passwords must never be shared. They must be kept secure.

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. (see also the BYOD policy]

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 The Diocese has the right to block certain content and users should not attempt to access blocked content or password protected areas.

4.3 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. Nothing that can be considered offensive or otherwise inappropriate, words or material, should be put in e-mails as there is no control over to where that email may be forwarded.

5.2 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 manger informed.

[1] Diocese covers all Parishes, Commissions and Committees

[2] Computer Systems covers all electronic devices that are currently on the market and in the time to come.

5.3 Care should be taken with the content of e-mails. Care should also be taken regarding distribution lists. The bcc option should be used. Does a reply need to go to all recipients?

6 USING THE INTERNET

6.1 Websites that have an immoral or subversive content must be avoided at all times. Any accidental access should be reported and recorded.

7 PERSONAL USE OF DIOCESAN SYSTEMS

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

8 MONITORING

8.1 CCTV is in use at many of the Diocesan premises.

8.2 Where it is technically possible e-mails 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.