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

1 ABOUT THIS POLICY

1.1 Our IT and communications systems are intended to promote effective communication and working practices within the Diocese. This Policy outlines the standards Diocesan personnel must observe when accessing these systems, the circumstances in which the Diocese may monitor user access, and the action the Diocese may take in respect of breaches of these standards. **nb** The Diocese has limited computer capacity in terms of mainframe and users.

1.2 This Policy covers all trustees of the Diocese, clergy, officers, consultants, contractors, volunteers, casual workers, agency workers, parishioners, and anyone who has access to our IT and communication systems. In this policy all these people are referred to as Diocesan Personnel.

1.3 Misuse of IT and communications systems can damage the Diocese and its reputation as well as causing harm and distress to any affected individuals. Breach of this Policy by Diocesan personnel may lead to sanctions being imposed which includes removal from role.

1.4 This Policy does not form part of any contract between Diocesan personnel and the Diocese and it may be amended at any time.

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.

2.2 All Diocesan personnel have a specific responsibility to ensure the fair application of this policy and are responsible for supporting colleagues and ensuring its success.

2.3 Head of Committees/Commission and Services and Parish Priests will seek support from an IT Specialist approved by the Diocese in dealing with requests for permission or assistance under any provisions of this policy and may specify certain standards of equipment or procedures to ensure security and compatibility.

3 EQUIPMENT SECURITY AND PASSWORDS

3.1 Diocesan personnel are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this Policy.

3.2 Diocesan personnel are responsible for the security of any computer device used by them. They should lock the device or log off when leaving it unattended or on leaving the office, to prevent unauthorised users accessing the system in their absence. Anyone who is not authorised to access the Diocesan network should not be allowed to use any device on it.

3.3 The Diocese buys in IT Support which will generally be responsible for making sure the software on each Diocesan device is kept up to date and that data on those devices are regularly backed up. Diocesan personnel are responsible for making sure that software is

updated and data backed up on any of their own devices used for Diocesan purposes - for further details please refer to our Bring Your Own Device Policy.

3.4 Passwords should be used on all IT equipment. This includes items that are taken out of the office

3.5 Passwords must be kept confidential. Usernames and passwords must not be shared. On cessation of being a member of Diocesan personnel (for any reason) all Diocesan IT equipment is to be returned to the relative Line Manager.

3.6 Diocesan personnel who have been issued with a laptop, tablet computer, smartphone or other mobile device, must ensure that it is always kept secure, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. Diocesan personnel should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

4 SYSTEMS AND DATA SECURITY

4.1 Diocesan personnel should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

4.2 Diocesan personnel must not download or install software onto Diocesan equipment from external sources without authorisation from Line Manager. This includes software programmes, instant messaging programmes, screensavers, photos, video clips and music files. Incoming files and data should, wherever possible be virus-checked. Non-Diocesan devices or equipment must not be attached to Diocesan systems without authorisation. This includes any USB flash drive, MP3 player, tablet, smartphone or other similar device, whether connected via the USB port, infra-red connection or in any other way.

4.3 Caution should be exercised when opening unsolicited emails from unknown sources or an email which appears suspicious (for example, if it contains a file whose name ends in .exe). The Diocese reserves the right to delete or block access to emails or attachments in the interests of security and the right not to transmit any email message.

4.4 No attempt should be made to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of a role.

4.5 When Diocesan equipment is used outside Diocesan premises every precaution must be taken to prevent importing viruses or compromising system security. The system contains information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

4.6 Smartphones need to have tracking enabled so they can be traced if lost or stolen. In addition, smartphones should be able to be deactivated remotely if lost or stolen. For further details please refer to our BYOD Policy.

5 EMAIL

5.1 Before sending an email, consideration should be given in deciding if it is the appropriate method for a particular communication. Correspondence with third parties by email should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals.

5.2 The sending of an abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate email is prohibited. Anyone who feels that they are being or have been harassed or bullied or is offended by material received from a member of Diocesan personnel via email should inform their line manager.

5.3 Diocesan personnel should take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. There is no control over where an email may be forwarded by the recipient. Avoid saying anything which would cause offence or embarrassment if it was forwarded to colleagues or third parties or found its way into the public domain. Data protection legislation gives everyone about whom the Diocese holds personal data the right to be to see all that personal data. This means that any comments made about a person in an email may be seen by that person.

5.4 Email messages are required to be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

5.5 In general, Diocesan personnel should not:

5.5.1 send, forward or read private emails at work which they would not want a third party to read;

5.5.2 send or forward chain mail, junk mail, cartoons, jokes or gossip;

5.5.3 contribute to system congestion by sending trivial messages, copying or forwarding emails to those who do not have a real need to receive them, or using "reply all" unnecessarily on an email with a large distribution list;

5.5.4 sell or advertise using Diocesan communication systems or broadcast messages about lost property, sponsorship or charitable appeals;

5.5.5 agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter;

5.5.6 download or email text, music or any other content on the internet which is subject to copyright protection, unless it is clear that the owner of such works allows this;

5.5.7 send messages from another person's email address (unless authorised) or under an assumed name;

5.5.8 send confidential messages via email or the internet or by other means of external communication which are known not to be secure.

5.6 When sending bulk distribution emails all addressees should be blind copied (bcc) so that other addressees cannot see who else has been sent the email.

5.7 If an email in received in error Diocesan personnel should inform the sender. Similarly, if an email is sent in error contact should be made with the recipients and Line Manager informed immediately.

5.8 Personal email accounts must not be used to send or receive emails which relate to Diocesan roles. Only use the email account we have provided for you.

6 USING THE INTERNET (APPLICABLE TO DIOCESAN MAINFRAME USERS)

6.1 Internet access is provided primarily for the purposes of the Diocese. Occasional personal use may be permitted as set out in paragraph 7.

6.2 When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in paragraph 9.1, such a marker could be a source of embarrassment to the visitor and the Diocese, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature.

6.3 Diocesan personnel should not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste or immoral. Even web content which is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that Diocesan software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this Policy.

6.4 Except as authorised in the proper performance of a Diocesan role, Diocesan personnel should not under any circumstances use Diocesan systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even in your own time.

6.5 If a search engine shows inappropriate material of any sort a record should be made of date, time, who made the search, search criteria and any witnesses.

7 PERSONAL USE OF OUR SYSTEMS (MAINFRAME USERS ONLY)

7.1 The Diocese permits the incidental use of the internet, email and telephone systems to send personal email, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must not be overused or abused. The Diocese may withdraw permission for it at any time or restrict access at its discretion.

7.2 Personal use must meet the following conditions:

7.2.1 use must be minimal, for Diocesan personnel based at Lancaster this must take place substantially out of normal working hours.

7.2.2 personal emails should be labelled “personal” in the subject header;

7.2.3 use must not interfere with the work of the Diocese or with the exercise of the role of Diocesan personnel.

7.2.4 use must not commit the Diocese to any marginal costs; and

7.2.5 use must comply with this Policy (see in particular paragraph 5 and paragraph 6) and other Diocesan policies.

7.3 Diocesan personnel should be aware that personal use of the systems may be monitored (see paragraph 8) and, where breaches of this policy are found, action may be taken under the

[Disciplinary Policy (see paragraph 9). The Diocese reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it is considered that personal use is be excessive.

8 MONITORING

8.1 A CCTV system monitors the exterior of the curial offices at Balmoral Road Lancaster, 24 hours a day as well as a number of other locations within the Diocese. This data is recorded.

8.2 The Diocese reserves the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the Diocese, including for the following purposes (this list is not exhaustive):

8.2.1 to monitor whether use of the email system or the internet is legitimate and in accordance with this Policy;

8.2.2 to find lost messages or to retrieve messages lost due to computer failure;

8.2.3 to assist in the investigation of alleged wrongdoing; and

8.2.4 to comply with any legal obligation.

9 PROHIBITED USE OF DIOCESAN 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. Misuse of the internet can in some circumstances be a criminal offence. It is not permitted to misuse Diocesan systems by participating in online gambling, forwarding chain letters, or by creating, viewing, accessing, transmitting or downloading any of the following material (this list is not exhaustive). Diocesan employees may face gross misconduct proceedings.

9.1.1 pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

9.1.2 offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our parishioners;

9.1.3 a false and defamatory statement about any person or organisation;

9.1.4 material which is discriminatory, offensive, derogatory or may cause offence or embarrassment to others;

9.1.5 confidential information about the Diocese, the work of the Diocese or any member of Diocesan personnel, or parishioners (except as authorised in the proper performance of your duties);

9.1.6 any other statement which is likely to create any criminal or civil liability (for the writer or the Diocese),

9.1.7 music or video files or other material in breach of copyright.

Any such action will be treated very seriously and an employee is likely to face summary dismissal.

9.2 For Diocesan personnel, where evidence of misuse is found, the Diocese may undertake a more detailed investigation in accordance with the Diocesan disciplinary procedure involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or others involved in the procedure. Such information may be handed to the police in connection with a criminal investigation.