Computer Usage Policy

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 you must observe when using these systems, the circumstances in which the Diocese may monitor your use, and the action the Diocese may take in respect of breaches of these standards.

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 of these people are referred to as Diocesan Personnel.

1.3 Misuse of IT and communications systems can damage the Diocese and our reputation as well as causing harm and distress to any affected individuals. Breach of this Policy by employees may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal or removal from your post.

1.4 This Policy does not form part of any contract between you and the Diocese and we may amend it 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 Chief Operating 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 The Chief Operating Officer will deal 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 You are responsible for the security of the equipment allocated to or used by you, and must not allow it to be used by anyone other than in accordance with this Policy.

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

3.3 The Chief Operating Officer 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. You are responsible for making sure that software is updated and data backed up on any of your own devices used for Diocesan purposes - for further details please refer to our BYOD Policy.

3.4 You should use passwords on all IT equipment, particularly items that you take out of the office. Passwords should be at least 8 characters long, contain numbers, lower and upper case letters and a symbol. Passwords must be changed every 3 months or when prompted.

3.5 You must keep your passwords confidential and must not use another person's username and password or make available or allow anyone else to log on using your username and password. When you cease to be a member of Diocesan personnel (for any reason) you must provide details of your passwords to your line manager and return any equipment, key fobs or cards.

3.6 Any passwords or passcodes to devices need to be provided to your line manager at the Diocese in case the Diocese needs to gain access to the device. These will be kept confidentially.

3.7 If you have been issued with a laptop, tablet computer, smartphone or other mobile device, you must ensure that it is kept secure at all times, 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. You 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 You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

4.2 You must not download or install software from external sources without authorisation from your line manager. This includes software programmes, instant messaging programmes, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked before they are downloaded. If in doubt, staff and volunteers should seek advice from a suitably qualified person. You must not attach any device or equipment to our systems without authorisation from your line manager. 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 We monitor all emails passing through our system for viruses. You should exercise particular caution 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). Seek advice from a suitably qualified person immediately if you suspect your computer may have a virus or if you have opened any suspicious email attachments or clicked on any suspicious links. We reserve the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message.

4.4 You should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your role.

4.5 You must be particularly vigilant if you use our IT equipment outside Diocesan premises and take such precautions as we may require from time to time against 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 If you have a smartphone this needs to have tracking enabled so it 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 Although email is a vital communication tool, you should always consider 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 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate emails. 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 or the Chief Operating Officer.

5.3 You 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. Remember that you have no control over where your 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. Remember that 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, you should not:

5.5.1 send, forward or read private emails at work which you 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 our 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; and/or

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 so that other addressees cannot see who else has been sent the email.

5.7 If you receive an email in error you should inform the sender. If you have sent an email in error contact your line manager.

5.8 Do not use your own personal email account to send or receive emails which relate to your role in the Diocese. Only use the email account we have provided for you.

5.9 We do not permit access to Dropbox on our computer systems at any time due to additional security risks.

6 USING THE INTERNET

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 You 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 our 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 your role, you should not under any circumstances use our 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.

7 PERSONAL USE OF OUR SYSTEMS

7.1 The Diocese permits the incidental use of our 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 and if you are an employee must take place substantially out of normal working hours (that is, during lunch hours, before 9 am or after 5.30 pm);

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 your role within the Diocese;

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 our other policies including our Data Protection Policy and Privacy Policy.

7.3 You should be aware that personal use of our systems may be monitored (see paragraph 8) and, where breaches of this Policy are found, action may be taken under the Disciplinary Procedure (see paragraph 9). We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.

8 MONITORING

8.1 Our systems enable us to monitor telephone, email, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our systems including the telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

8.2 CCTV systems may be in use to monitor the exterior of the Curial Offices as well as a number of other locations within the Diocese. This data is recorded.

8.3 We reserve 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):

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

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

8.3.3 to assist in the investigation of alleged wrongdoing; and

8.3.4 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 if you are an employee be dealt with under our Disciplinary Procedure. Misuse of the internet can in some circumstances be a criminal offence. In particular, it is not permitted, and if you are an employee it will usually amount to gross misconduct to misuse our 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):

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 you or the Diocese); and/or

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

Any such action will be treated very seriously and if you are an employee is likely to result in summary dismissal.

9.2 If you are an employee, where evidence of misuse is found, we may undertake a more detailed investigation in accordance with our 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 Disciplinary Procedure. If necessary such information may be handed to the police in connection with a criminal investigation.