E-MAIL & INTERNET POLICY

PURPOSE

The purpose of this policy is to ensure that employees of the Chester Diocesan Board of Finance (DBF) understand the way in which Electronic mail (email) and the Internet should be used in the organisation. It aims to ensure that email and the Internet is used effectively for its intended purpose without infringing legal requirements or creating unnecessary risk.

SCOPE

All employees of the DBF including temporary staff, volunteers, contractors and clergy working in / for Church House are subject to this policy. Failure to comply may lead to disciplinary action, including dismissal. At the same time, your conduct and/or action(s) may be unlawful or illegal and you may be personally liable.

GENERAL STATEMENT

To maximise the benefits of its computer resources and minimise potential liabilities, the DBF has adopted this policy. Staff using computers must use these resources responsibly, professionally, ethically and lawfully.

You are given access to our computer network and Internet to assist you in performing your job. You should not have an expectation of privacy in anything you create, store, send, or receive on the computer system. The computer system, network and your computer belong to the DBF and have been provided for business purposes. Without prior notice, the DBF may review any material created, stored, sent, or received on its network or through the Internet or any other computer network.

You should never consider your electronic communications to be either private or secure. Email may be stored indefinitely on any number of computers, including that of the recipient. Copies of your messages may be forwarded to others either electronically or on paper. In addition, email sent to nonexistent or incorrect usernames may be delivered to persons that you never intended.

PROBIHITED ACTIVITIES

Use of computer resources for any of the following activities is strictly prohibited:

- Sending, receiving, downloading, displaying, printing, or otherwise disseminating material that is sexually explicit, profane, obscene, harassing, embarrassing, intimidating, fraudulent, racially offensive, defamatory, or otherwise unlawful
- Knowingly disseminating or storing solicitations, destructive programs (that is, viruses or self-replicating code) or any other unauthorized material
- Wasting computer resources by, among other things, spending excessive amounts of time on the Internet, downloading or playing games during working hours, engaging in non-business online chat groups during working hours, printing unreasonable amounts of personal documents, or otherwise creating unnecessary network traffic
- Using or copying software in violation of a licence agreement or copyright
- Violating any British, European, or international law
- Using DBF equipment in connection with personal business activity or other paid employment.

EMAIL and INTERNET USE POLICY

Email provides an excellent means of communicating with other staff, other Church bodies, outside individuals, bodies and businesses. Use of email, both internally and externally over the Internet, however, must be tempered with common sense and good judgment.

To maximize the benefits of this medium and minimise potential liabilities the DBF has created the following policy and guidelines. Please keep in mind that these guidelines are not intended to discourage your use of email in performing your job. Rather, they are intended to ensure that email is used responsibly and with discretion.

All work related e-mail correspondence must be sent from the work e-mail account. Employees are not permitted to use personal e-mail accounts for work purposes.

THINK before sending a message. - Staff should endeavour to make each electronic communication truthful and accurate. You should use the same care in drafting email and other electronic documents as you would for any other written communication. Please keep in mind that anything created or stored on the computer system may, and likely will, be reviewed by others. Before sending a message, ask yourself the following question: Would I want a judge or jury to see this message?

Be aware – When sending a personal e-mail or accessing the Internet for personal purposes you are using an address that identifies you as an employee of the DBF.

Inappropriate material. - Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by email. If you encounter this kind of material, you should report it to your line manager.

Data Protection implications. - There are Data Protection implications in the electronic transfer of information and files containing personal information. Email is a quick and convenient way to transfer data, but it is governed by the Data Protection Act in exactly the same way as other computer files. Apply the same qualitative judgment to sending information by email as you would do by any other means of communication. Always use the BCC distribution field when e-mailing a group that are not within the organisation unless you have the express permission of the group to share their e-mail addresses with each other.
Altering attribution information. - Staff must not alter the "From:" line or other attribution-of-origin information in email communications. Anonymous or pseudonymous electronic communications are forbidden. Staff must identify themselves honestly and accurately when sending email or otherwise communicating by email.

Monitoring of computer usage. - The DBF has the right to monitor any and all aspects of its computer system, including, but not limited to, monitoring sites visited by staff on the Internet, monitoring chat groups and news-groups, reviewing material downloaded or uploaded by users to the Internet, and reviewing email sent and received by users. This includes information sent and received via DBF smartphones.

Our connections to the Internet. - To ensure security and avoid the spread of viruses, staff accessing the Internet through a computer attached to the network must do so through the installed system which uses our approved virus scanning software. This is there for the protection of the network against viruses and unauthorised hacking. Staff accessing the network from outside Church House must ensure that their virus protection is up to date.

Virus detection. - Files received from unknown sources, including memory sticks or other storage devices brought from home; files downloaded from the Internet, Newsgroups, bulletin boards, or other online services; files attached to email; and files provided by customers or vendors, may contain dangerous computer viruses that could damage the DBF's computer network. Staff should never open attachments from unknown sources. If you suspect that a virus has been introduced onto the network, notify the Head of Finance immediately. Staff need to be aware that if a file is copied to a laptop from a memory stick or other memory device whilst working offline, they should not access this file once connected to the network or going online until their virus checker has updated itself and is up to date.

Use of encryption software. - Staff may not install or use encryption software on any computer, unless it is approved and installed by the Head of Finance.

Email footers. - You may, on occasion, receive email with disclaimers/ footers attached. It is the policy of the DBF to add a standard footer of this type to our emails. The approved wording is added automatically to external emails and is:

Chester Diocesan Board of Finance. Company number 7826. Registered Charity 248968.
Registered Office: Church House, 5500 Daresbury Park, Daresbury, Warrington WA4 4GE.

Disclaimer of liability for use of Internet. - The DBF is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains billions of pages of information. Although the Diocese operates internet filtering technology, users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material and no filter can be entirely effective. Users should not give their DBF email address to commercial organizations unless this is for work purposes. A very high proportion of email traffic is now *spam* – unwanted unsolicited advertising material often of an offensive nature, using email addresses harvested from commercial organisations and websites. The DBF email system blocks most of the spam sent to the DBF email addresses. However, not all spam can be blocked as the senders are constantly varying their techniques to avoid the blocking. Users accessing the Internet do so at their own risk.

Accessing inappropriate Internet sites. - Staff working for the DBF have a duty to conduct themselves whilst at work in a manner that is appropriate to the culture, aims and objectives of their employer. Deliberate accessing of offensive, pornographic or other inappropriate web-sites for personal gratification using the DBF's equipment and Internet address is not in keeping with the nature of the employer. Visiting such web-sites leaves a trail that the site owners can trace back to the DBF and the resulting publicity could be highly embarrassing for the Church. Such activities are likely to be considered as gross misconduct.

There are occasions when some staff may, in the course of their work for the Church, require to access otherwise undesirable web-sites. In such cases, the staff involved must clear this in advance with their Head of Department or the Diocesan Secretary and inform the Head of Finance prior to accessing these sites. However, you may, nonetheless, encounter inappropriate or sexually explicit material while browsing on the Internet. If you do, immediately disconnect from the site and inform the Head of Finance.

Illegal copying. - Staff may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licences that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not agree to a licence or download any material for which a registration fee is charged.

Email Systems. – DBF staff should only use email addresses/accounts operated by DBF in the form "@chester.anglican.org" for DBF business purposes. No other email accounts or similar communications mediums should be set up by staff for DBF business purposes without the prior specific approval of the Diocesan Secretary. If any member of staff becomes aware of the use of unauthorized email systems they should report it to the Head of Finance. All other accounts, for example Facebook or Twitter, must be set up in the name of the DBF and will be monitored by the Communications department.

Installation of Software. - Staff may not install any software on a desktop or laptop computer belonging to the diocese unless prior permission has been given by the Head of Finance.

Amendments and revisions

This policy may be amended or revised from time to time as the need arises. Staff will be notified of all amendments and revisions.

Violations of this policy will be taken seriously and may result in disciplinary action, including disconnection from the email/Internet system and, in serious or repeated cases, possible termination of employment.