Ely Diocesan Board of Finance

Acceptable Use IT Policy

Owner: Jon Green

Date: 16 May 2018
1 Overview
The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at The Ely Diocesan Board of Finance (EDBF) in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

The EDBF provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the company against damaging legal issues.

2 Scope
All employees, contractors, consultants, temporary and other workers at the EDBF, including all personnel affiliated with third parties, must adhere to this policy. This policy applies to information assets owned or leased by the EDBF, or to devices that connect to an EDBF network.

Any exceptions to this policy must be approved in advance by written application to the Ely Diocesan Data Controller.

3 Responsibilities
The EDBF is subject to the requirements of the General Data Protection Regulation and the Data Protection Act 2018 which take effect in May 2018. These pieces of legislation stipulate the obligations placed on the EDBF in processing data and the responsibilities owed to data subjects about whom information is processed in the conduct of the EDBF’s business.

The EDBF continually monitors the requirements placed on it and seeks, through system review and staff training, to engender in its staff the principles of best practice in Data Protection and responsible secure processing of data.

4 Policy Statement

4.1 General Requirements

4.1.1 You are responsible for exercising good judgment regarding appropriate use of EDBF resources in accordance with EDBF policies, standards, and guidelines. The EDBF resources may not be used for any unlawful or prohibited purpose.

4.1.2 For security, compliance, and maintenance purposes, authorised personnel may monitor and audit equipment, systems, and network traffic per the Audit Policy. Devices that interfere with other devices or users on the EDBF network may be disconnected.

EDBF prohibits actively blocking authorised audit scans. Firewalls and other blocking technologies must permit access to the scan sources.

4.2 System Accounts

4.2.1 You are responsible for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.
4.2.2 You must maintain system-level and user-level passwords in accordance with the Password Policy.

4.2.3 You must ensure through legal or technical means that proprietary information remains within the control of EDBF at all times.

Unauthorised conduct of any business that results in the storage of information on personal or non-EDBF controlled environments, including devices maintained by a third party with whom the EDBF does not have a contractual agreement, is prohibited.

This specifically prohibits the use of an unauthorised e-mail account that is not provided either by the EDBF, or its customers and partners, for company business.

4.3 Computing Assets

You are responsible for ensuring the protection of assigned EDBF assets. Laptops left at EDBF premises overnight should be secured or placed in a locked drawer or cabinet. Employees must report any theft of EDBF assets to the Diocesan Office IT support team onsite, or third party provider, as soon as they become aware.

4.3.1 All PCs, PDAs, laptops, and workstations must be secured with a screensaver with the automatic activation feature set to 10 minutes or less. You must always lock the screen or log off when the device is unattended.

4.3.2 Do not interfere with corporate device management or security system software, including, but not limited to, antivirus, Teamviewer, Complete IT management software.

4.4 Network Use

You are responsible for the security and appropriate use of the EDBF network resources under your control. Using EDBF resources for the following, or doing anything that could reasonably be expected to result in the following is strictly prohibited:

4.4.1 Causing a security breach to either the EDBF or other network, including, but not limited to, accessing data, servers, or accounts to which you are not authorised; circumventing user authentication on any device.

4.4.2 Causing a disruption of service to either the EDBF or other network, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.

4.4.3 Introducing honeypots, honeynets, or similar technology on the EDBF network.

4.4.4 Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software. See the Diocesan Copyright Policy for more information.

4.4.5 Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.

4.4.6 Use of the Internet or the EDBF network that violates the parameters defined within the
Diocesan Staff handbook and the EDBF policies relating to the use of a person’s own device.

4.4.7 Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers.

4.4.8 Port scanning or security scanning on a production network unless authorised in advanced by the Diocesan IT Manager.

4.5 Working from home

4.5.1 You are responsible for informing your line manager when you take work home.

4.5.2 If working on something at home and at work try to keep both sets of information up to date.

4.5.3 Home computers should have records removed once project/work records no longer needed at home.

4.5.4 Staff agree to take all reasonable steps to keep work taken home secure.

4.5.5 Staff must return all work-related material upon the completion/termination of their contract; and the EDBF should be informed if information has been passed to or been accessed or seen by any third party with no right to have access to that information.

4.5.6 Where permission has been given to permit direct access to EDBF servers and data files from home staff must confirm that devices comply with the EDBF policy for the use of personal devices.

4.6 Electronic Communications

At the commencement of your employment, you will be provided with email addresses and access to electronic mailboxes. These are intended to allow for the better performance of the duties set out in your contract of employment. All email accounts are intended to be for business purposes only. Please do not use them for personal reasons. The accounts will remain at all times the property of the EDBF. Email is a method of delivery of communication. It should not be treated as a document filing system. Where documents are sent as attachments, users should save any appropriate files into electronic case folders held in secure network files. Similarly, where a letter is communicated in the body of an email, users should save a copy of the text into the electronic working folder in a secure network file.

The following are strictly prohibited:

4.6.1 Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates The EDBF policies against harassment or the safeguarding of confidential or proprietary information.

4.6.2 Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.

4.6.3 Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.
4.6.4 Posting the same or similar non-business-related messages to large numbers of newsgroups (spam).

4.6.5 Use of an EDBF e-mail or IP address to engage in conduct that violates EDBF policies or guidelines. Posting to a public newsgroup, bulletin board, or listserv with an EDBF e-mail or IP address represents the EDBF to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

5 The Rights of Data Subjects
Under current United Kingdom legislation, unless there is a satisfactory reason demonstrated to the Regulator, all data subjects have the following rights in respect of their personal data held from time to time by the Ely Diocesan Board of Finance:

- The right to request a copy of personal data
- The right to request that the diocese corrects any personal data if it is found to be inaccurate
- The right to request personal data is erased where it is no longer necessary to retain such data;
- The right to withdraw your consent to the processing of data at any time
- The right to request that the data controller provide the data subject with his/her personal data and where possible, to transmit that data directly to another data controller - known as the right to data portability
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data, (where applicable)
- The right to lodge a complaint with the Information Commissioners Office.

6 References

7 Enforcement
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with The Ely Diocesan Board of Finance.

8 Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>honeypot, honeynet</td>
<td>Network decoys that serve to distract attackers from valuable machines on a network. The decoys provide an early warning for intrusion detection and detailed information on vulnerabilities.</td>
</tr>
<tr>
<td>Spam</td>
<td>Electronic junk mail or junk newsgroup postings. Messages that are unsolicited, unwanted, and irrelevant.</td>
</tr>
</tbody>
</table>