Peterborough Diocesan Board of Finance

IT Acceptable Use Policy

Diocesan Board of Education Users

Policy Status

This IT Acceptable Use Policy explains what you may and may not do when you use the Diocesan Board of Finance's IT systems, and the consequences of not following the policy.

This policy has been agreed by Andrew Roberts Diocesan Secretary, in consultation with CoopSys the DBF IT Managed Service Provider. Changes to this policy are not permitted without the express permission and authority of Andrew Roberts, Diocesan Board of Finance, Diocesan Secretary.

Approval and review

Document Control

Date	Version	Status	Author	Reason for Change
15/08/2022	1.0	FINAL	Sue Ratcliffe	New Policy
25/11/2022	1.1	FINAL	Sue Ratcliffe	Email and Calendar p7 updated
14/12/2022	1.2	FINAL	Sue Ratcliffe	Bespoke for DBE Users

Supporting Documents

Document	Location
Data Protection Policy	G:\ Policies
DBE Staff Handbook	Ask PC for location

Contents

1. Document Purpose

This policy outlines your responsibilities as a *user of the DBF IT infrastructure*. It clarifies what you may and may not do when you use the Diocesan Board of Finance's IT systems, and the consequences of not following this policy.

2. Introduction

This policy outlines the responsibilities of all users of the Peterborough Diocesan Board of Finance (DBF) Information Technology (IT) in respect of use of, and access to, the DBF's physical and wireless IT network, the devices attached to it, and the security of the systems that can be accessed via those devices. This policy replaces all previous Acceptable Use and IT Policy Documents.

This policy applies to the following groups of people:

- Employees of the DBF
- Employees of organisations that pay for DBF IT Services (tariff payers) in this instance Diocesan Board of Education Staff
- Office Holders, Agency staff, consultants, contractors, and volunteers of the DBF or its tariff payers.

3. Guidance and Scope

The following guidance applies unless otherwise instructed by the Assistant Diocesan Secretary or the IT Managed Service Provider.

Failure to comply with this policy could result in disciplinary action in accordance with The Diocesan Board of Education Staff Handbook. [1] This includes dismissal for employees, and termination of contracts with contractors, consultants or agency staff.

[1] Or any handbook relevant to office holders.

Identity and access management

Do	Don't
✓ Notify servicedesk@coopsys.net of any new person starting in your team using the New Starter Form no less than 15 working days before their start date	X Share your password with anybody.
✓ Notify servicedesk@coopsys.net of any person leaving your team using the Leaver form as soon as the leaver's end date has been agreed.	X Ask for a colleague's password.
✓ Change your password immediately if you think an unauthorised person may have accessed your account. Notify servicedesk@coopsys.net and your line manager as soon as you are aware of any un authorised access.	X Attempt to access any system or network area you have not been authorised to access.
✓ Always apply strong passwords (i) to systems and devices.	X Do not use the same password or PIN across multiple devices / applications, or re use the same password /PIN across multiple devices/applications.
✓ Only access the DBF network from devices protected by anti-virus and firewall software.	
(i) The National Cyber Security Centre advises using three random words with numbers and symbols if you need to www.ncsc.gov.uk	

Software

Do	Don't
✓ Seek advice from servicedesk@coopsys.net **before** purchasing new software.	X Copy, modify or update software
	X Save files on your desk top
✓ Notify servicedesk@coopsys.net if you need an application or other software update.	X Install any software on any device connected to the DBF network without authorisation from Coopsys.

File Storage

Do	Don't
✓ Store all DBE data on the appropriate network drive or approved system.	X Save non DBE related files on any network drive of a DBE computer, laptop or tablet.
✓ Only use secure (encrypted) USB devices to transport data (not as an additional storage mechanism) if there is no other option available.	X Save files on your desk top. X Keep DBE data on removable (USB) devices for any longer than is necessary.
✓ Encrypted USB devices should be ordered from servicedesk@coopsys.net. All data saved to a removable device should be transferred to the network as soon as possible.	

Hardware

Do	Don't
✓ Keep IT equipment protected against accidental/malicious damage, loss, theft, including unauthorised access to data.	X Lone out or dispose of IT Equipment; in the case of disposal, without prior approval from the Director of Education[2]
✓ Report loss or theft of your IT equipment immediately to servicedesk@coopsys.net, and then to the police. Obtain a crime number and report immediately to sue.ratcliffe@peterborough-diocese.org.uk with the crime number.	X Remove audio-visual equipment e.g screens and/or projectors from any meeting rooms. X Disable security settings or features on your device. X Connect any non DBE devices to the DBF physical network.
✓ Be prepared to return/collect your device in person as required when security/maintenance updates are needed.	

[2] peter.cantley@peterborough-diocese.org.uk

✓ Return any devices to your line manager at the end of your employment.

Internet and Social Media

Do	Don't
✓ Let servicedesk@coopsys.net know if you have inadvertently accessed an inappropriate website. ✓ Let servicedesk@coopsys.net know if a website has been blocked inappropriately.	X Make excessive or inappropriate personal use of the internet. (personal use is permitted during lunch breaks) X Use the internet for 'streaming' unless for specific work purposes when this should be kept to a minimum. X Make inappropriate use of social media * - see section 4 *(*see the Social Networking Policy for advice)*

Email and Calendar

Do	Don't
✓ Keep your outlook calendar up to date with your whereabouts at all times. ✓ Allow full visibility of your calendar (see section 5 relating to the Bishop's Management Group.) ✓ Use the out of office function for all absences of one day or more with clear signposting for any matters needing attention in your absence. ✓ Mark any sensitive entries in your calendar as 'private'. ✓ Make sure emails are polite, professional and non-aggressive at all times. ✓ Delete emails that are sent to you in error and notify the sender. ✓ Mark email as 'confidential' where appropriate to avoid any liability	X Put confidential matters in your calendar without applying the appropriate privacy settings. X Attempt to email scanned documents to external recipients directly from a multi-function device (i.e shared scanner/printer) X Use work email for personal use X Open any emails or attachments that appear to be suspicious – report them to servicedesk@coopsys.net immediately. X Set up DBE emails on a personal device without first getting that personal device set up on 'in tune' (contact servicedesk@coopsys.net) to allow remote wiping in the event of loss. X Store critical business information solely within the email system. All business critical information should be stored in the appropriate network area.

arising out of a breach of privacy. ✓ Send all official and business related emails using the DBE email system. ✓ Password protect all sensitive email attachments and send all passwords by text. ✓ Remember, offers or contracts sent by email are as legally binding on the Board as those sent on paper hardcopy.	X access or attempt to access any personal/non DBE email accounts from your work device. (*Note: all personal devices must be on the most up to date operating system applicable to that device before use for work emails will be allowed)*

4. Inappropriate use of IT

Inappropriate use includes, but is not restricted to:

- Failure to observe this policy or the Data Protection Policy
- Any behaviour that could be considered to be bullying or harassment – all DBE employees deserve to be treated with dignity and respect (see also: Dignity at Work Policy)
- Hacking
- Any use that might bring the DBE into disrepute.
- Inappropriate use of social media (see: Social Networking Guidelines).
- Personal use of @Peterborough-diocese.org.uk email addresses
- Inappropriate use of email which includes, but is not limited to, the sending or forwarding of chain letters, junk mail, unsubstantiated warnings, circulars, or other trivial content.
- Without prior approval, wilfully receiving, viewing, downloading, storing, distributing or otherwise using with the aid of the DBF/DBE facilities, any material, whether business or personal, that is, or could be considered to be: defamatory; offensive or obscene; untrue or malicious; abusive; racist; homophobic; sexist or ageist; pornographic; gambling related; unauthorised copyright material.

5. Microsoft Outlook Calendar Protocol

The Calendar guidance in this policy applies to all staff/officer outlook calendars where the employer is the DBF/DBE; with the exception of the Bishop's Management Group calendars, which are covered by the document Access to Calendars, **and Emails March 2022** held by the Bishops' Office where all questions should be directed

Questions relating to DBE Staff Calendars should be directed to education@peterbrough-diocese.org.uk.

Calendars should be up to date and visible to all staff at all times.

Any calendar entries, which relate to meetings of a sensitive nature should be marked ‘Private’.

Any attachments saved in a calendar entry, if of a confidential nature, should be password protected.