BISHOPS' CONFERENCE OF SCOTLAND

EMAIL RETENTION AND USAGE POLICY

Table of Contents

Document Control

Title	Email Retention and Usage Policy
Prepared by	Donna Maguire
Approved By	Mgr Hugh Bradley
Date of Approval	10/05/18
Version Number	1.6
Review Frequency	5 years
Next Review Date	2023

Status Control

Version	***Date***	***Status***	***Prepared by***	***Reason for Amendment***
1.6	10/05/18	draft	DMM	

EMAIL RETENTION AND USAGE POLICY

1 INTRODUCTION

Email messages sent or received during BCOS business are corporate/business records, and therefore must be managed as records. All email messages are the property of BCOS; when you leave the employment of the BCOS you may not take any e-mails, calendar appointments or contacts with you. The BCOS must ensure that all evidential emails are retained with accordance to the Retention Schedule.

The new GDPR regulations require us to manage our emails correctly. They also require us to be able to locate all relevant records and information that has been requested or to be able to confirm that records have been deleted appropriately. The regulations also state that we must not retain personal data for any longer than is necessary, so we cannot permanently hold onto any emails, sent and received, if they contain information about individuals, unless we can show a valid business or legal reason to do so. They must be removed from being accessible through the email system and archived in the appropriate associated project folder.

This policy and associated guidance is intended to help employees to determine whether, and for how long, to retain information that is sent or received by email. It also sets out rules on when, and for what purpose, you should use your BCOS email account.

2 SCOPE OF THIS POLICY

This Policy applies to all emails, sent and received, by BCOS staff during BCOS business, on any device being used, whether supplied by BCOS or from any other source and used by the employee (commonly referred to as BYOD = Bring Your Own Device). This is irrespective of wherever you are, whether in or out of the office, at home, on mobile phones/tablets, in hotel business centres, Internet cafes, etc.

Related BCOS Policies and Guidance documents are as follows:

- Basic Guide to Data Protection
- Data Protection Policy
- Information Audit Guide
- Data Retention and Disposal Schedule
- Data Breach Policy
- Computer Usage Policy

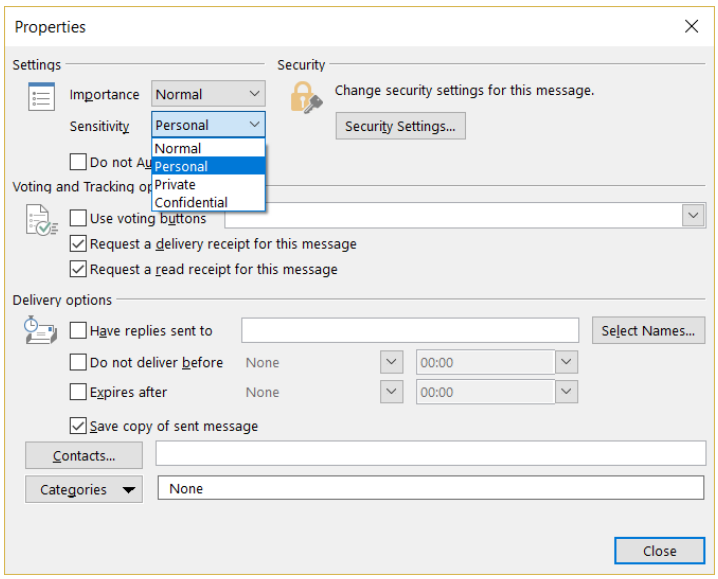
3 THE POLICY

3.1 Usage of BCOS Email

Users are encouraged to keep business and personal email accounts separate. In accordance with BCOS Computer Usage Policy you can access your personal email account using BCOS equipment and via BCOS networks provided it does not interfere with your work. All personal emails should be clearly marked as being Personal/Private.

Reasonable personal use of your BCOS email account is allowed if it does not impact on your work. Tag these messages as 'Personal' using the inbuilt Sensitivity option within your Email Properties.

e.g. in Outlook via the Properties -> Sensitivity settings



3.2 Cautionary advice

Be aware that anything you write in an email relating to BCOS business may be subject to disclosure under the GDPR, if involved in a Subject Access request. Email messages can and are used as evidence in legal proceedings. Therefore, even though an email has been sent as "Personal", there can be no expectation of personal privacy, as any email you send or receive using your BCOS email account is owned by BCOS.

You should not:

- use your BCOS email address to sign up for personal accounts on websites such as Amazon, eBay, Facebook, Twitter, PayPal, etc
- send BCOS business to your home email account
- set up Auto-forwarding to email accounts outside BCOS.

3.3 People with multiple roles within the BCOS

It is often the case that people will have more than one position with an agency/office. Some may also be working for several agencies/offices at the same time. It is important that emails are managed correctly in these situations. As you will receive an email account for each role, it is your responsibility to manage these accounts accordingly. Ensuring that the correct email is sent to and from the correct account is crucial. If a Subject Data Access Request is made, then all email accounts may need to be searched to comply.

3.4 Remote access

It is possible to connect to your BCOS account remotely, via Microsoft portal: https://login.microsoftonline.com. From here you can pick up your email and you will have full access to Office 365 and One drive. For full details contact IT support.

BCOS Computer Usage Policy offers the following advice:

- Be careful when using the 'Reply All' function (which sends a copy of your response to all recipients listed in the 'To:' address of any received email message) i.e. communication within a group. Ensure that you send messages or attachments only to intended recipients.
- Consider carefully before sending via email any sensitive or confidential subject matter that should be discussed privately and in person, as this may inadvertently fall into the wrong hands.
- Do not use email for unnecessary communication, such as gossip or potentially critical remarks about others.
- Do not send large attachments, as some email systems are unable to accommodate them. There are other methods available.
- Do not print emails. This adds to the places needing to be searched for any data requests, requires secure disposal and increases environmental waste
- If you receive an unusual, unsolicited, suspicious email then ***do not open/click on it or any links within it.*** By hovering the mouse pointer over any links, you may discover the real address it will take you to.
- Never respond to spam or 'unsubscribe' to an unknown email.

3.5 Explicitly Prohibited Use

Users shall not use BCOS email to view, download, save, receive or send material related to or including any of the following:

- illegal activities
- offensive content of any kind, including inappropriate jokes, pornographic material
- content that promotes discrimination based on race, gender, national origin, age, marital status, sexual orientation, religion or disability
- threatening or violent behaviour
- gambling or wagering
- copyright violation
- leaking/theft of all types of information

- messages that misrepresent yourself or BCOS.

All illegal activity will be reported to the relevant authorities. The BCOS can be held legally responsible for communications made by its staff

3.6 Retention of Emails

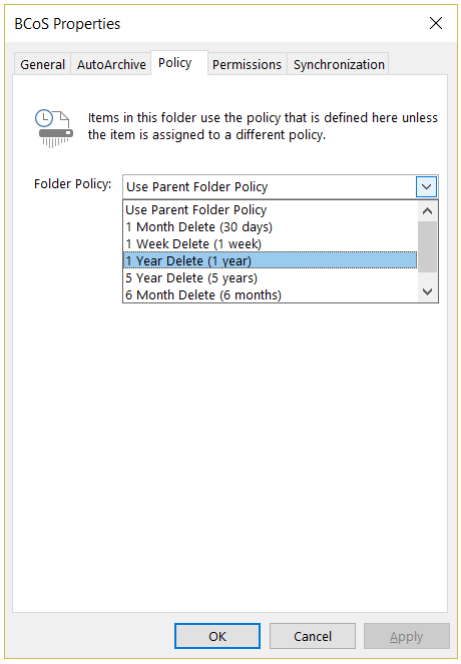
BCOS employees are responsible for managing their email records in the same way that they are responsible for managing other business records. Storage is available for email, but there is a limit. Notification will be sent if your usage is excessive. To prevent this, please ensure you are following the BCOS Data Retention Policy and remove/archive emails which are no longer currently required. If you then still require increased storage for business purposes, please contact IT Support.

How long an email should be retained is governed by the information contained within it, not by the medium on which it is stored. The BCOS Data Retention Schedule sets out classes of information, along with the recommended period for which they should be retained.

Do not use .pst files (Outlook 'personal folders') to archive emails. This is an older storage method that no longer meets BCOS standards. If you need to retain content from .pst files, please contact IT Support for assistance in converting the content out of .pst files into Office 365, where retention can be set appropriately. If .pst files are stored on your hard drive, then they may be lost if you leave BCOS or overlooked if they are requested under GDPR. IT Support may, from time to time, scan systems to determine if .pst files are still being used.

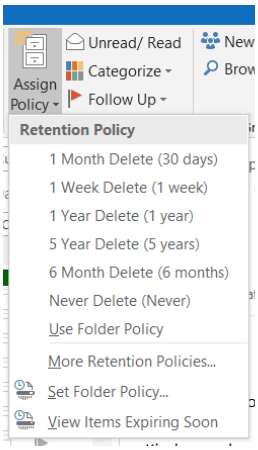
3.7 Data Retention on Email Folders

Retention Policies can be set on email folders within Outlook, including Outlook Online (part of Office 365). You should set folder policies to suit the Retention Schedule appropriate for the type of content, e.g. in Outlook, right-click folder name -> Properties -> Policy.



Move emails into the folders using Automatic Rules, Quick Steps or manually if appropriate – ask IT Support for assistance in configuring these if required.

Retention on individual emails can also be set via the "Assign Policy" menu item.



Outlook has "Archive" features, including "Auto-Archive" settings. These are **not** the same as moving email content into an official archive such as the Scottish Catholic Archives. You should NOT adjust these settings.

3.8 Saving and storing emails in other ways

Email messages can be saved outside the email system in appropriate folders i.e. a Project Folder on your shared network drive or your personal office network. Saving emails to. PDFs is done by printing your email 'to PDF', either by using the print to Microsoft PDF or Adobe PDF. These are accepted as the most stable and reliable form of saving, as they maintain their authenticity and are an accepted form of long term preservation for digital content. If you need to keep email for use in litigation, keep it in the email system so that its audit trail is available. These important emails should be kept in a Special Folder for this purpose.

3.9 Deleting email messages

You should set your Deleted Items folder to empty itself on closure of the Outlook application. The Deleted Items folder must not be used as a file store. Emails deleted from your Deleted Items folder will be stored centrally for 30 days after deletion, in case they need to be recovered. After this period, they will be permanently destroyed.

N.B. Emails in the inbox will be deleted after 6 months. If you wish to retain any email, you will have to move them into a folder or save them out of the email system e.g. as pdf. This will not be implemented until you have cleared your inbox of old emails.

3.10 Security

You should only use the Email programs and systems approved by BCOS: the most recent version of Microsoft Outlook, Outlook for Mac and Office 365 suite, including online versions in browser, and Microsoft apps for smartphones.

Email systems are not encrypted by default. BCOS cannot guarantee that any messages sent or received by email are secure or private. If sensitive information must be sent by electronic communications systems, encryption or similar technologies to protect the data should be used. Contact IT Support if this is needed.

Individual email account passwords must not be shared. If you suspect someone else knows your password, inform IT Support immediately. Systems used to access email, whether BCOS owned or owned by others i.e. systems using older versions of Window and Outlook etc., should not be used to send and receive email, unless you are using online portal versions. NO emails should be stored on IT equipment that is not up to date and fully compliant with BCOS IT Support. All equipment should be up-to-date with security updates, antivirus/anti-malware. Any attempt in bypassing security features could result in Disciplinary Procedures.

3.11 Monitoring of Emails

BCOS IT Support will monitor emails sent and received relating to BCOS business in accordance with the Regulation of Investigatory Powers Act 2000, GDPR and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Please be aware that personal IT equipment may require to be inspected by BCOS to comply with the above laws and regulations.