

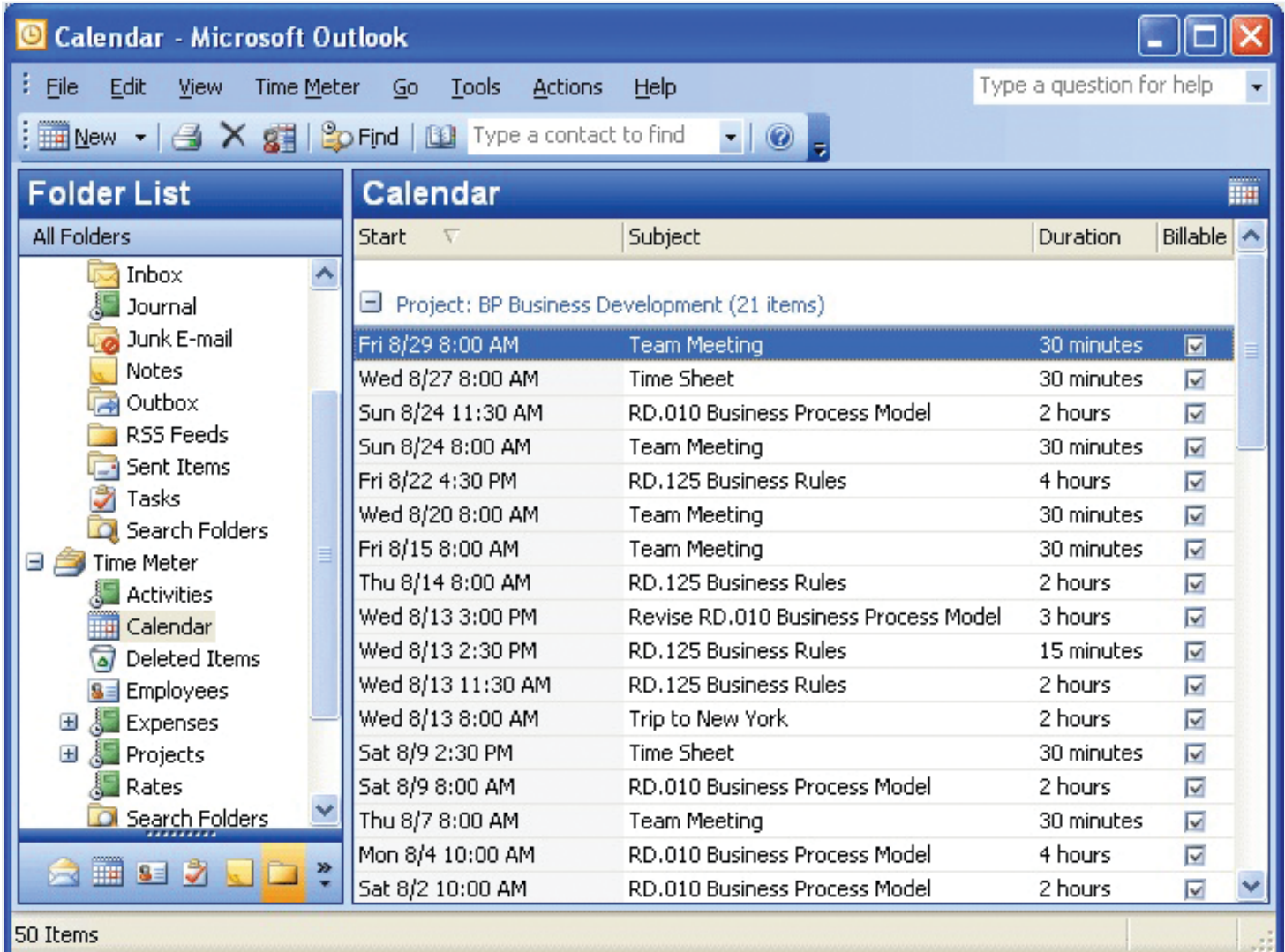
Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

Email Retention – Does Your Firm Have a Policy?

The benefits of email are a two edged sword as they can both improve a firm's effectiveness with enhanced collaboration, and can cause great embarrassment and financial loss in cases of litigation.

Roman Kepczyk • Mar. 22, 2012



The screenshot shows the Microsoft Outlook interface with the Calendar view selected. The 'Folder List' on the left shows various folders, with 'Calendar' highlighted. The main window displays a list of calendar items for a project named 'Project: BP Business Development (21 items)'. The list includes dates, times, subjects, durations, and billable status.

Start	Subject	Duration	Billable
Project: BP Business Development (21 items)			
Fri 8/29 8:00 AM	Team Meeting	30 minutes	<input checked="" type="checkbox"/>
Wed 8/27 8:00 AM	Time Sheet	30 minutes	<input checked="" type="checkbox"/>
Sun 8/24 11:30 AM	RD.010 Business Process Model	2 hours	<input checked="" type="checkbox"/>
Sun 8/24 8:00 AM	Team Meeting	30 minutes	<input checked="" type="checkbox"/>
Fri 8/22 4:30 PM	RD.125 Business Rules	4 hours	<input checked="" type="checkbox"/>
Wed 8/20 8:00 AM	Team Meeting	30 minutes	<input checked="" type="checkbox"/>
Fri 8/15 8:00 AM	Team Meeting	30 minutes	<input checked="" type="checkbox"/>
Thu 8/14 8:00 AM	RD.125 Business Rules	2 hours	<input checked="" type="checkbox"/>
Wed 8/13 3:00 PM	Revise RD.010 Business Process Model	3 hours	<input checked="" type="checkbox"/>
Wed 8/13 2:30 PM	RD.125 Business Rules	15 minutes	<input checked="" type="checkbox"/>
Wed 8/13 11:30 AM	RD.125 Business Rules	2 hours	<input checked="" type="checkbox"/>
Wed 8/13 8:00 AM	Trip to New York	2 hours	<input checked="" type="checkbox"/>
Sat 8/9 2:30 PM	Time Sheet	30 minutes	<input checked="" type="checkbox"/>
Sat 8/9 8:00 AM	RD.010 Business Process Model	2 hours	<input checked="" type="checkbox"/>
Thu 8/7 8:00 AM	Team Meeting	30 minutes	<input checked="" type="checkbox"/>
Mon 8/4 10:00 AM	RD.010 Business Process Model	4 hours	<input checked="" type="checkbox"/>
Sat 8/2 10:00 AM	RD.010 Business Process Model	2 hours	<input checked="" type="checkbox"/>

Email has become a critical business tool not only as one of the primary means of communicating with clients but also for documenting decisions and business information in client files. With today's smart phones, tablets and remote access services via the Internet, email is universally accessible and its extreme ease of use makes it the primary communication tool for just about everyone. Unfortunately, email's benefits are a two edged sword as they can both improve a firm's effectiveness with enhanced collaboration, and can cause great embarrassment and financial loss in cases of litigation.

While most firms are aware that they should have and adhere to an email retention policy, the vast majority do not do so until after they have been the victim of a lawsuit, since email is usually one of the primary pieces of evidence targeted by opposing counsel. Surprisingly, many firms often feel that since they have limited the size of their personnel's email accounts that they have already addressed the retention issue, which is definitely not the case. So what does a firm need to do to tackle the issue?

The solution is to develop an email retention policy that is easy for firm personnel to understand and is well documented. While this is admittedly a very difficult thing to do, it is the responsibility of the firm to put in place tools that allow the email retention policy to be consistently applied across the firm including the implementation of a document management or archival solution. Firms should work with their legal counsel to develop a policy specific to their State and areas of practice. There are specific rules for managing email regarding HIPAA compliance, SEC, investment management, and financial institution type work that the firm may have to comply with, so it is imperative that the firm's policy incorporate those rules along within the overall policy.

One of the first steps in creating a policy is to specifically identify what types of information employees are allowed to send via email. For instance, stating that sensitive, confidential documents should not be sent unless encrypted, or specifying that the firm's portal should be used for these documents instead, outlines boundaries for firm personnel. The policy should identify what constitutes acceptable business use for email and include specifications that prohibit inappropriate content or any item that could be deemed as harassment being sent in an email. The policy should also identify what would be construed as acceptable and unacceptable personal use of the firm's email accounts.

The policy should also specify how emails with an ongoing business purpose are to be archived and at what point any emails stored locally would be archived or erased. Some firms specify that email older than a certain age (we have seen the most common policies being between 30 and 180 days) will be automatically deleted. Firms without an archiving solution would also need to specify how files should be saved including the client folder, email file naming convention, and the disposition of email from their account.

The policy should also specify where email can be retained. Many firms utilize web-based email so that it can only be accessed by authorized personnel through a login process which the firm controls. The policy for these firms should consider disallowing saving emails personally and specifically prohibit email from being copied and stored locally on C:Drives (via a .PST file), as well as prohibiting copying emails to local storage media such as flash drives. If the firm allows email to be accessed or downloaded to personnel devices such as smart phones or tablets, the policy should state also clearly document the firm's rights to that information.

Many firms include within their policies that the employee agrees that any such local information is the property of the firm and is to be deleted upon termination, that they agree to adhere to the firm's retention policy across any and all devices, and that the firm retains the right to remotely wipe the device if it is misplaced, stolen or if the employee leaves the firm. In the event that this must be done, the IT team needs to be involved in "digital cleansing" of the device as simply deleting files does not always ensure they are actually gone.

The email retention policy should also outline the firm's right to review emails to ensure compliance with the policy, as well as consequences to the employee for not complying with them. These consequences are not to be taken lightly as the firm must adhere to the policy across the board or face it being thrown out in the event of litigation.

The IT department also must be involved in the creation of the policy as they will need to implement email archival tools and processes to enforce and manage it. The reality is that if the policy is too hard to comply with or the email tools too difficult to use, personnel will find a way to work around it, so this consideration needs to be incorporated. When policies mandate the destruction of old emails, the IT team will be involved to verify that procedures were properly completed and that the data on any backups has also been taken into account. IT personnel will also need to be included as a part of a litigation response team in the event that the firm anticipates

a law suit or regulatory inquiry, so they can immediately suspend the document destruction policy for a litigation hold and properly document which files are impacted. In this regard, the IT team will also be involved with managing a central archiving or document management solution for those firms that choose automated tools.

Once the policy is written and reviewed by the firm's legal counsel, it must be explained to firm personnel and verified that they understand how to apply it including any training on the firm's archival tools. This training should extend to any interns, part-time employees, or subcontractors and all firm personnel should be reminded annually. Please note it is generally accepted that if the firm leadership and personnel choose not to adhere to the firm's policies, most will agree that the firm should not implement it, so it is critical to get them onboard in the beginning.

Creating and implementing an email retention policy is not an easy process as evidenced by how few firms actually have one in place but if the firm works with the right providers, it can be done and it is usually less expensive before receiving a subpoena from an attorney.

Roman H. Kepczyk, CPA.CITP is Director of Consulting for Xcentric, LLC. and works exclusively with accounting firms to implement today's leading best practices and technologies. Roman is also author of "Quantum of Paperless: A Partner's Guide to Accounting Firm Optimization" which is available at Amazon.com

Article

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.

© 2023 Firmworks, LLC. All rights reserved

