ADMINISTRATIVE PROCEDURE 146

Standardized E-mail Signature Block & Best Practice for Corporate E-mail

General Administration

December 2024

Purpose/Background

Rocky View Schools (RVS) employees have a responsibility to ensure e-mail sent via the jurisdiction's corporate account, Outlook Exchange, exemplifies a professional, uniformed approach consistent with RVS' brand.

Procedures

Signature block

1. Effective April 1, 2019, RVS employees shall use a standardized e-mail signature block. These standards only apply for the jurisdiction's corporate email account, Outlook Exchange, not its instructional email accounts, Google Gmail.

2. All RVS employees shall use one of the following templates to create a standardized e-mail signature block:

   For school staff:

   First Name Last Name, professional credentials (optional) (11 pt Calibri Bold)
   Title (10 pt Calibri), School Name (10 pt Calibri)
   Rocky View Schools (10 pt Calibri)
   Ph: xxx.xxx.xxxx (10 pt Calibri) – this will be the general school phone number
   www.changetoyourschoolurl.ca (10 pt Calibri)

   For Education Centre staff:

   First Name Last Name, professional credentials (optional) (11 pt Calibri Bold)
   Title (10 pt Calibri) (10 pt Calibri)
   Rocky View Schools (10 pt Calibri)
   O: xxx.xxx.xxxx (10 pt Calibri, if applicable)
   C: xxx.xxx.xxxx (10 pt Calibri, optional)
   www.rockyview.ab.ca (10 pt Calibri)

   Please note:
   - Logos, images, mottos, tag lines and/or quotes **are not to be included** in the signature block.
   - Updates must be made on both the Outlook Client (desktop) and Outlook Online (web) and across all mobile devices (e.g. iPad, phone, etc.)

E-Mail Best Practices

Below are best practices to promote and support the use of e-mail:

3. Subject lines

Subject lines are critical for locating e-mails and should describe the content of the e-mail.

4.1 Avoid subject lines such as:

- Hello
- Question for you
- Education

4.2 Use specifics

- Locally Developed Course: Liver Studies?
- Procedures for Non-Standard Items
- OH&S Audit – Next Steps

Attachments to internal staff

By sending attachments via e-mail, the attached file automatically becomes a duplicate version of the original file. The recipient(s) can then make changes and edits to the attached version, thus creating confusion and ultimately resulting in the possibility of the incorrect file being used.

3.1 Upload/create the document in SharePoint or common drive and share the link. This will ensure that only one copy of a document is being edited and previous versions can be restored, if necessary.

3.2 By sending a link versus an attachment, the sender eliminates the risk of file size preventing an e-mail from making it to the recipient.

4. Use of blind carbon copy (Bcc)

Bcc refers to the practice of sending an e-mail to multiple recipients in such a way that conceals individual addresses from the list of recipients. This can be accomplished by:

Addressing a message to oneself to avoid spam filters from misfiling the message → Enter detailed subject line (refer to Subject line section) → Add recipients to the Bcc field

4.1 E-mails sent using Bcc protect group names/individual identities and protect recipients from e-mail address mining.

4.2 Bcc e-mails should not be forwarded unless a request to do so is included in the text and a circulation list is included (e.g., please forward to relevant staff, circulated to all principals).

5. Use of Importance settings

Importance settings can help recipients prioritize their e-mail messages. If applicable, apply the setting that reflects the priority of the message in the context of the jurisdiction.

5.1 High Importance (red exclamation mark) – Read immediately.

5.2 No selection or Low Importance (blue downward arrow) – Read within 24 hours.

6. Responsible use of technology

Responsible use of digital technologies requires that users both protect and respect the jurisdiction.

6.1 Staff should never click on links in an e-mail until the sender is verified.

6.2 Best practice is to visit the sender's website to verify legitimacy of an e-mail. Phishing attempts can appear legitimate and entice the user to click on e-mail links.

6.3 When an e-mail containing a suspicious link is received and verified as spam, mark the e-mail as "junk" then delete from the junk folder. Do not attempt to click on the link.

7. Disclaimer

The jurisdiction may automatically append a disclaimer to all outbound corporate e-mail. The intent is to inform any recipient that the message is for the addressee(s) only and may contain information that is privileged, confidential or exempt from disclosure. The disclaimer asks unintended recipients to immediately notify the sender and delete this e-mail message and any attachments.

Reference(s):
AP140 – Responsible Use of Technology