KENNESAW STATE UNIVERSITY

Email Best Practices

Effective email communication at Kennesaw State University enhances accessibility, readability, and security while fostering a sense of community and leaving a positive impression. By following these guidelines, you will enhance the quality of your messages, promote accessibility, and maintain data security.

Protect Your—and KSU's—Data

- Adhere to KSU's Data Management Guidelines.
- Never share confidential data via email. If a message must contain sensitive information, encrypt the attachment and share the password through a separate channel.
  Examples of confidential data: passwords, Social Security numbers, driver's-license numbers, bank-account details, credit/debit-card numbers, identifiable medical information, visa and passport numbers.

Define Your Purpose and Determine Audience

- **Define your purpose:** Begin by asking yourself what you are trying to achieve with your email. Are you informing, requesting, persuading, confirming, or reminding?
- **Determine your audience:** Determine the individual(s) or group you need to address. Consider their roles and responsibilities, as well as their relationship to you. Always tailor your message based on your audience.
- **Consider tone and style:** The purpose and audience will help you decide whether your email should be formal, casual, or neutral, and whether you need to provide a detailed explanation or a simple message.
- Use descriptive subject lines that summarize the content. E.g., "Science 1101: Our Group Project"
- Avoid vague language like "Important Update" or "Read This Now."

Begin with a Salutation

- Use an appropriate salutation.

  E.g., Dear Professor Jones, if you are emailing a professor, or Hi, Jane! If you are emailing a classmate.

Share Key Information Early in the Message

- Begin with a summary of the most important details, including dates if applicable.

  E.g., "Starting February 1, we will . . ."

- Ensure critical updates are immediately visible without scrolling.

Keep Content Concise and Scannable

- Use bullet points, numbered lists, or headings for easy readability.
- Limit each paragraph to 2–3 sentences.
- Use bold and highlights strategically
  E.g., You might put the main point of the message in bold font and/or highlight key dates or deadlines.
- Include links to additional resources rather than overloading the email with excessive details.

Use Descriptive Hyperlinks

- Use meaningful text that reflects the link destination
  E.g., View the event schedule.
- Avoid embedding URLs behind generic words like "here" or "click here."
- Avoid typing out long URLs and avoid including "https://" or "http://".

Use Inclusive and Professional Language

- Address all recipients respectfully, using gender-neutral language when appropriate (e.g., "they" instead of "he/she").
- Tailor the tone to your audience: formal for external communications, and conversational for internal emails.

Keep Attachments to a Minimum

- Share content via secure, campus-approved platforms such as OneDrive rather than large attachments. Learn more about sharing documents securely here: How to Determine Where to Store and Share Information
- When sharing attachments, include a brief description of the file's purpose.

Prioritize Accessibility

- Use clear fonts and ensure text is easy to read on all devices.
  - Suggested fonts for the body of emails: Aptos or Calibri
  - Suggested font size for the body of emails: 12
  - Suggested font color: Black (except for links, which should be underlined and in blue font.)
- Include alt text for images to accommodate people using screen readers.
- Avoid overly complex formatting or bright color schemes.

Standardize Email Signatures

- Follow KSU's standard format for email signatures.
- Avoid excessive links, quotes, or images in your signature.

Avoid Composing Messages That Look Suspicious

- Don't spoof addresses (e.g., using display names like "KSU Payroll Dept" from a personal Gmail).
- Steer clear of alarm-style language ("ACT NOW OR YOUR ACCOUNT WILL BE CLOSED!").

- Never request passwords, MFA codes, or personal data by reply.
- Limit exclamation points, emojis, and ALL-CAPS—they're common phishing flags.
- Ensure link text matches the real destination; mismatches look phishy.

Looks Suspicious	Looks Legit
Subject: URGENT—Verify your account immediately!!! **From:** "KSU IT Helpdesk john.doe@yahoo.com" **Body:** Click here http://tinyurl.com/abcd to avoid deactivation.	**Subject:** Action Needed – Two-Factor Setup by May 15 **From:** UITS Help Desk helpdesk@kennesaw.edu **Body:** Visit Duo Enrollment to complete the setup (link goes to a kennesaw.edu domain).

Review and Proofread Before Sending

- Check and double-check the recipient(s) and avoid using the "Reply All" option unless your message is intended for everyone in the list.
- Check for grammatical errors, broken links, and tone consistency.
- Confirm that all links and/or attachments are correct and appropriate for the intended audience.