**Here are some key aspects to consider when communicating via email in a school setting:**

* Refer to your school Data Protection / Email Policy if you have one.
* All work-related emails should be written using a school email address.
* Consider the working hours / email window of your recipient. You should have no expectation of receiving a response to your messages outside of their normal working hours.
* Emails should be written in the same professional tone as any other form of school communication.
* Consider who needs to see your message. Avoid using ‘Reply all’.
* Whatever you write in an email about any living person, they have a right to see.
* School email accounts must not be used to send personal emails.
* Only use abbreviations if you are sure the recipient will understand their meaning.
* The sending of abusive, threatening, discriminatory or other offensive email may be considered a criminal act.
* Bear in mind that emails may be submitted as evidence in legal proceedings.
* Email attachments should be opened with care unless you have absolute confidence in its origin as this is one of the most likely points of introducing a virus into a computer system.
* Staff should be aware that school email accounts may be accessed by other school staff for monitoring or management purposes.
* Do not forward any email containing a ‘sexting’ image of a child, even for investigation purposes.
* Always use your work email address to correspond with parents / carers to ensure that there is a full audit trail of such activity.
* Only Carbon Copy (CC) emails to those who need to consider or take action as a result of its content.
* Be careful when including a long email trail in a reply or forward; they can increase the risks of some recipients receiving information that was not intended for them.
* Regularly check if your email accounts have been compromised via a data breach and whether your passwords for those accounts have been exposed by visiting [Have I Been Pwned: Check if your email has been compromised in a data breach.](https://haveibeenpwned.com/) Changing your password is the most important thing to do if your account has been pwned. If you have reused your password on other accounts, you should also change the passwords for those accounts.
* Use strong passwords. The NCSC has some useful advice on [choosing a password using three random words](https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words). Make sure your domestic and work passwords are different.
* Password protect or encrypt attachments with sensitive information and phone the addressee or text the password separately.

You are responsible for the security of the information you are sending, and therefore you must assess its sensitivity and whether email is a secure enough method of communication. Ensuring the security of emails is crucial to protect sensitive information and maintain the privacy of staff, pupils, and stakeholders.