

EMAIL POLICY

Policy

This policy outlines Railway Road Medical Centre's approach to the use of email communication. Email is generally not considered a secure method of communication unless it is transmitted via a government database, or is password-protected or encrypted. Appropriate precautions must be taken to protect the privacy and confidentiality of all information sent or received via email.

Guidelines

Email is commonly used for communication between staff, patients, healthcare providers, and third parties. All parties must understand the potential risks to privacy and confidentiality when using unsecured email.

All employees of Railway Road Medical Centre are required to uphold the principles of integrity, professionalism, privacy, confidentiality, and impartiality when sending or receiving emails.

To ensure compliance, staff must adhere to the following procedures:

- If an email is received that does not request information or action, it should be forwarded to the appropriate Practice Team member or Principal GP for review and information.
- Before sending any information, staff must first receive an email from the requesting party to verify the accuracy of the email address. This email must clearly outline the information being requested and include explicit consent from the patient, healthcare provider, or third party authorising the release of information to that email address.
- Once the email address and consent have been verified, a copy of the received email must be saved and recorded in the patient's file under "Correspondence In," clearly labelled as "Consent Obtained."
- The requested information may then be sent by replying directly to the verified email (using the "Reply" function) to ensure it is sent only to the authorised address.
- A copy of all outgoing correspondence must be saved and recorded in the patient's file under "Correspondence Out."