The Uniting Church in Australia
QUEENSLAND SYNOD

Checklist

Email Scam Prevention

1. **Verify the Sender**
   - ☐ Check the actual email address, not just the display name.
   - ☐ Be cautious of small misspellings or unusual domains.
2. **Confirm Unusual Requests**
   - ☐ If someone asks for directories, contact lists, or financial help, verify by phone or in person before responding.
3. **Protect Sensitive Information**
   - ☐ Never send member directories, contact details, financial records, or login credentials without authorised approval.
   - ☐ Use password-protected files when sharing sensitive information.
4. **Slow Down Before Responding**
   - ☐ Scammers rely on urgency. Pause and review before clicking or replying.
5. **Look for Red Flags**
   - ☐ Poor spelling or grammar
   - ☐ Unexpected attachments
   - ☐ Links or messaging that don't match the sender's usual style or domain
   - ☐ Requests that feel out of character for the person
6. **Use Secure Practices**
   - ☐ Enable multifactor authentication on email accounts.
   - ☐ Keep antivirus and system updates current.
7. **Report Immediately**
   - ☐ If you suspect a scam, notify your ministry agent, Church Council, and your IT support immediately.
   - ☐ Do not engage further with the suspicious email.
8. **Build a Safety Culture**
   - ☐ Regularly remind staff and volunteers about impersonation risks.
   - ☐ Encourage everyone to ask, "Is this request expected and legitimate?"