



**Introduction** Lifelong Healthcare provides email access to its employees where relevant and beneficial for their roles.

This email usage policy outlines the regulations governing email use within the organisation. It also sets out the expectations for staff behaviour when using email.

This policy should be read alongside other key policies. Users should also refer to the company's data protection and internet usage policies.

**Purpose of this Policy** Email is a standard communication tool in business. It is widely used and arguably as crucial as the telephone.

However, like any technology, email can present risks if used incorrectly or inappropriately.

This email policy:

- Reduces security and business risks faced by Lifelong Healthcare.
- Informs staff of permitted email usage.
- Ensures employees adhere to proper email etiquette.
- Assists the company in meeting its legal obligations regarding email use.

**Scope of the Policy** This policy applies to all staff, contractors, and volunteers at Lifelong Healthcare who use the organisation's email system.

It applies regardless of location, whether on company premises, while travelling for business, or working from home.

It covers the use of company email on any device, whether owned by the company or the employee.

**Authorised Users** Only individuals authorised to use email at Lifelong Healthcare may do so.

Authorisation is typically granted by an employee's line manager or the company's IT department when a new employee joins and is assigned login credentials for company systems.

Unauthorised use of the company's email system is strictly prohibited.

Employees who use company email without authorisation – or provide access to unauthorised individuals – may be subject to disciplinary action.

## Key Areas

**Email Security** Misuse of email can present security risks to the organisation. Users must not:

- Open email attachments from unknown sources, as they may contain viruses, Trojans, spyware, or other malware.
- Disable security or email scanning software, as these tools are essential for business security.
- Send confidential company data via email. The IT department can advise on secure alternatives.
- Access another user's company email account. If access is required (e.g., during an employee's absence), a request should be made to the line manager or IT department.

Users must always consider system and data security when using email. Guidance is available from line managers and the IT department as required.

Email is not inherently secure. Most emails sent over the internet are in plain text, making them vulnerable to interception. While such incidents are rare, email should be regarded as an open communication channel, unsuitable for confidential information.

**Inappropriate Email Content and Use** The company's email system must not be used to send or store inappropriate content or materials.

Employees must understand that viewing or distributing inappropriate content via email is unacceptable under any circumstances.

Users must not:

- Write or send emails that could be defamatory or create liability for the company.
- Create or distribute inappropriate content via email, including but not limited to pornography, racial or religious slurs, gender-specific remarks, content promoting criminal activities or terrorism, or material related to cults, gambling, and illicit drugs.
- Use email for any illegal or criminal activities.
- Send offensive or harassing emails.
- Send messages or material that could damage Lifelong Healthcare's reputation.

Any user who receives an email they consider inappropriate should report it to their line manager or supervisor.

**Copyright** Lifelong Healthcare respects and adheres to copyright law. Users may not use company email to share copyrighted software, media, or materials owned by third parties unless authorised.

Employees must not use the company's email system to engage in activities that may breach copyright laws.

Users should be aware that emails and attachments may be subject to copyright. Forwarding such emails may infringe copyright regulations.

**Contracts and Liability** Users must exercise caution when making commitments or agreeing to purchases via email.

An email may constitute a legally binding contract between Lifelong Healthcare and the recipient – even if the sender has not obtained prior authorisation within the company.

**Email Disclaimer** The standard company email template includes an email disclaimer. Users must not alter or remove this when sending messages.

**Email Marketing and Bulk Email** Lifelong Healthcare may use email for marketing to existing and potential clients.

Significant legislation governs bulk email and marketing communications.

All email campaigns must be authorised by the Practice Manager and executed using the company's designated email marketing tool.

Users must not send bulk emails via the standard business email system.

All enquiries regarding email marketing should be directed to the Practice Manager.

### **Email Best Practices**

**Email Etiquette** Email is a primary communication tool with clients, partners, and key stakeholders. Although relatively informal, employees must recognise that each email reflects the company's professional image.

Users must:

- Avoid forwarding chain emails or 'humorous' messages, as these clutter inboxes and may be inappropriate for the workplace.
- Use meaningful subject lines instead of leaving them blank or using vague terms like 'hello'.
- Use the 'important message' setting sparingly for genuinely critical emails.
- Refrain from requesting 'read receipts', as these can be intrusive and are not supported by all email services.
- Avoid using ALL CAPITAL LETTERS, as this may be perceived as impolite.
- Be selective with group emails, including only recipients who will find the content relevant and useful.
- Use 'CC' (carbon copy) sparingly; if someone truly needs to receive an email, they should be in the 'To' field.
- Use 'BCC' (blind carbon copy) for group messages when appropriate to maintain recipient privacy.

**Internal Email** is a useful internal communication tool, but it can be overused.

Before sending an internal email, users should consider:

- Would a face-to-face conversation or phone call be more effective?

- Is email the best method for document discussions? Tracking feedback and versions can be challenging via email.
- ‘Reply all’ is rarely necessary. Instead, reply to the sender and manually add other relevant recipients.

## **Policy Enforcement**

**Monitoring Email Use** The company email system is provided for legitimate business purposes.

Lifelong Healthcare reserves the right to monitor employee email usage. Any such monitoring will be conducted by authorised personnel.

Additionally, all emails sent or received through the company’s email system form part of official company records. The company may be legally compelled to disclose these records to law enforcement or other relevant authorities.

Employees must ensure that all business-related emails are accurate, appropriate, ethical, and lawful.

**Potential Sanctions** Knowingly violating this email use policy is a serious matter. Users who breach this policy may face disciplinary action, up to and including termination of employment.

Employees, contractors, and other users may also be held personally liable for violations.

Where appropriate, Lifelong Healthcare will involve the police or other law enforcement agencies in cases of serious breaches.

However, the company is unlikely to take formal action against employees who inadvertently fail to follow guidelines in good faith.