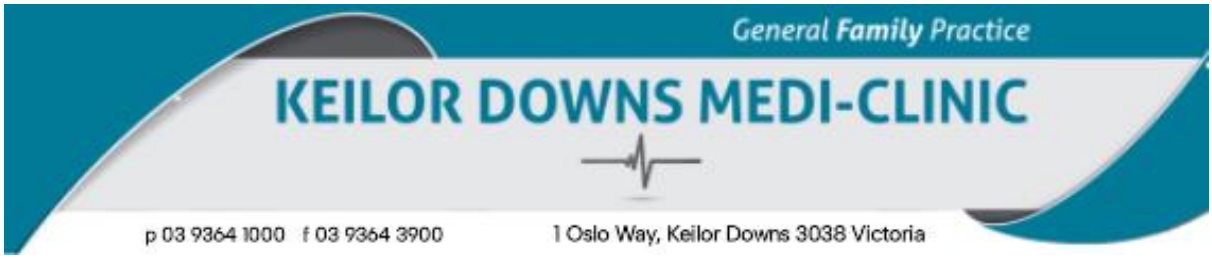

E-MAIL POLICY

Introduction

Keilor Downs Medi- Clinic makes email available to its employees where relevant and useful for their jobs.

This email use policy describes the rules governing email use at the company. It also sets out how staff members are expected to behave when using email.

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

Why this policy exists.

Email is a standard way to communicate in business. It's used widely and is arguably just as important as the telephone.

Like any technology, email can cause difficulties if used incorrectly or inappropriately.

This email policy:

- Reduces the security and business risks faced by Keilor Downs Medi- Clinic
- Let's staff know how they are permitted to use company email.
- Ensures employees follow good email etiquette.
- Helps the company satisfy its legal obligations regarding email use.

Policy scope

This policy applies all staff, contractors and volunteers at Keilor Downs Medi- Clinic who use the company email system.

It applies no matter where that email use takes place: on company premises, while travelling for business or while working from home.

It applies to use of company email on any device, no matter whether owned by the company or employee.

Authorised users

Only people who have been authorised to use email at Keilor Downs Medi- Clinic may do so.

Authorisation is usually provided by any employee's line manager or the company IT department. It is typically granted when a new employee joins the company and is assigned their login details for the company IT systems.

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

Employees who use the company email without authorisation – or who provide access to unauthorised people – may have disciplinary action taken against them.

Key areas

Email security.

Used inappropriately, email can be a source of security problems for the company. Users of the company email system must not:

- Open email attachments from unknown sources, in case they contain a virus, Trojan, spyware or other malware.
- Disable security or email scanning software. These tools are essential to protect the business from security problems.
- Send confidential company data via email. The IT department can advise on appropriate tools to use instead.
- Access another user's company email account. If they require access to a specific message (for instance, while an employee is off sick), they should approach their line manager or the IT department.

Staff members must always consider the security of the company's systems and data when using email. If required, help and guidance is available from line managers and the company IT department.

Users should note that email is not inherently secure. Most emails transmitted over the internet are sent in plain text. This means they are vulnerable to interception.

Although such interceptions are rare, it's best to regard email as an open communication system, not suitable for confidential messages and information.

Inappropriate email content and use

The company email system must not be used to send or store inappropriate content or materials.

It is important employees understand that viewing or distributing inappropriate content via email is not acceptable under any circumstances.

Users must not:

- Write or send emails that might be defamatory or incur liability for the company.
- Create or distribute any inappropriate content or material via email.

  inappropriate content includes pornography, racial or religious slurs, gender specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.

This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone based on race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

- Use email for any illegal or criminal activities.
- Send offensive or harassing emails to others.
- Send messages or material that could damage Keilor Downs Medi- Clinic's image or reputation.

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

Copyright

Keilor Downs Medi- Clinic respects and operates within copyright law. Users may not use company email to share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.

Employees must not use the company's email system to perform any tasks that may involve breach of copyright law.

Users should keep in mind that the copyright on letters, files and other documents attached to emails may be owned by the email sender, or by a third party. Forwarding such emails on to other people may breach this copyright.

Contracts and liability

Users must be careful about making commitments or agreeing to purchases via email.

An email message may form a legally-binding contract between Keilor Downs Medi Clinic and the recipient – even if the user has not obtained proper authorisation within the company.

Email disclaimer

The standard copy email template includes an email disclaimer. Users must not remove or change this when they send messages.

Email marketing and bulk email

Keilor Downs Medi Clinic may use email to market to existing and potential customers.

There is significant legislation covering bulk email and use or email for marketing.

All email campaigns must be authorised by the practice manager and implemented using the company's email marketing tool.

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

All questions about email marketing should be directed to the practice manager.

Email best practice

Email etiquette

Email is often used to communicate with customers, partners and other important contacts. Although a relatively informed medium, staff should be aware that each email they send does affect the company's image and reputation.

It's a good idea to follow rules and good email etiquette. Users must:

- Not forward on chain emails or 'humorous' messages. These clogs up people's in-boxes and some topics are not appropriate for the workplace.
- Always use a meaningful subject line rather than leaving it blank or using a single work like 'hello'.
- Only use the 'important message' setting sparingly, for messages that really are important.
- Never ask recipients to send a 'message read' receipt. Many people find these annoying and not all email services support them.
- Do Not use ALL CAPITAL LETTERS in messages or subject lines. This can be perceived as impolite.
- Be sparing with group messages, only adding recipients who will find the message genuinely relevant and useful.
- Use the 'CC' (carbon copy) field sparingly. If someone really needs to receive a message, they should be included in the 'to' field.
- Use the 'BCC' (blind carbon copy) field to send group messages where appropriate. It stops an email recipient seeing who else was on the email.

Internal email

Email is a valid way to communicate with colleagues. However, it tends to be overused for internal communication.

Users should keep these points in mind when emailing colleagues:

- Would the issue be better addressed via a face-to-face discussion or telephone call?

- Is email the best way to send a document out for discussion? Often, it becomes very hard to keep track of feedback and versions.
- It's rarely necessary to "reply all". Usually, it's better to reply and then manually add other people who need to see a message.

Policy enforcement

Monitoring email use

The company email system and software are provided for legitimate business use.

The company therefore reserves the right to monitor employee use of email.

Any such examination or monitoring will only be carried out by authorised staff.

Additionally, all emails sent or received through the company's email system are part of official Keilor Downs Medi Clinic records. The company can be legally compelled to show that information to law enforcement agencies or other parties.

Users should always ensure that the business information sent via email is accurate, appropriate, ethical, and legal.

Potential sanctions

Knowing breaching this email use policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment.

Employees, contractors and other users may also be held personally liable for violating this policy.

Where appropriate, the company will involve the police or other law enforcement agencies in relation to breaches of this policy.

However, the company is unlikely to take formal action if a user fails to adhere to the guidelines in the 'email best practice' section.