

## 6.4.9 Email and Internet Usage Policy

### Purpose

The purpose of this policy is to ensure that email and internet systems are used appropriately, securely, and professionally, and that patient confidentiality, privacy, and data security are maintained at all times in accordance with applicable healthcare laws, regulations, and professional standards.

### Scope

This policy applies to all employees, contractors, students, and other authorized users of Riddell Country Practice electronic systems, including email, internet access, computers, mobile devices, and any other technology provided or approved by the practice.

### Acceptable Use

Email and internet access are provided primarily for business-related purposes, including:

- Patient care and clinical communication
- Practice administration and operations
- Professional education and research relevant to duties
- Communication with patients, providers, insurers, and regulators (as permitted)

Limited personal use may be allowed provided it:

- Does not interfere with work duties
- Does not consume excessive system resources
- Does not violate any part of this policy

### Patient Confidentiality and Privacy

- Patient-identifiable information must only be transmitted via approved, secure systems.
- Personal or health information must not be sent to unauthorized recipients.
- Staff must verify recipient details before sending emails containing sensitive information.
- Patient information must never be accessed, shared, or stored without a legitimate clinical or business reason.
- Email is not to be used for clinical advice unless specifically approved and appropriately secured.

### Prohibited Use

Users must not use practice email or internet systems to:

- Access, transmit, or store offensive, inappropriate, or illegal material
- Share confidential patient or business information without authorization
- Engage in harassment, discrimination, or unprofessional conduct
- Download unauthorized software or files
- Circumvent security controls or monitoring systems
- Use personal email accounts for official practice communications involving patient or business information
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy
- Stealing, using, or disclosing someone else's password without authorization
- Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers
- Passing off personal views as representing those of the organisation

### Professional Conduct

All electronic communications must:

- Be professional, respectful, and accurate
- Reflect the values and reputation of the practice
- Avoid informal language, slang, or humor that could be misinterpreted
- Be written with the understanding that emails may become part of the medical or legal record

### **Security and Passwords**

- Users must keep login credentials confidential and not share passwords
- Devices must be locked when unattended
- Suspected security breaches, phishing emails, or unauthorized access must be reported immediately
- Practice systems must not be accessed from unsecured or public networks unless approved safeguards are in place
- All sites and downloads may be monitored and/or blocked by RCP if they are deemed to be harmful and/or not productive to business
- The installation of software such as instant messaging technology is strictly prohibited

### **Monitoring and No Expectation of Privacy**

- The practice reserves the right to monitor, access, and audit email and internet usage to ensure compliance with this policy, legal obligations, and accreditation standards

### **Breaches and Disciplinary Action**

Failure to comply with this policy may result in:

- Disciplinary action up to and including termination
- Mandatory retraining
- Legal or regulatory reporting where required

If an employee is unsure about what constitutes acceptable internet and email usage, then he/she should ask his/her supervisor for further guidance and clarification.

All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with the policies and procedures mentioned above.

### **Policy Review**

This policy will be reviewed regularly and updated as necessary to remain compliant with legal, regulatory, and accreditation requirements.