**Ethical Issues and Email Accounts in the Professional Workspace.**

Modern businesses and enterprises depend on an electronic mailing system for communication within and with external parties. However, often there is confusion concerning the law on the usage of email, and many organisations lack policy concerning the use of email. An approach through a policy that defines acceptable and nonacceptable use of emails to employees in the workplace is essential to avoid ethical and legal challenges. An ethical electronic mail system defines clearly to employees the parameters of personal and professional email use of company resources.

Employees at times assume that the emails they exchange using the electronic mailing system are private; however, to protect the organisation against threats such as spam and malware coming through email, many organisations scan incoming and outgoing emails. It is ethical to inform employees that the company monitors emails and uses automated software solutions to check their emails. A medical research organisation employs me as an email system administrator. We often intercept emails that are classified as profanity. Some of the emails that get quarantined as profanity are false-positive since the employed algorithm would classify medical terms as profanity. This sometimes raises ethical questions regarding providing filtering software access to employee communication without consent from the system user. However, the employer has the right to monitor and filter emails exchanged using the organisation's resources and, moreover, if the organisation can demonstrate a legitimate business reason for doing so.

Companies must create policies regarding email use in the workplace. Ethical email providers disclose precisely what is allowed and what is prohibited. If the policy is vague, it may not protect employers. For example, if employers plan to monitor both company and personal emails, the policy should state that even personal accounts are subject to scrutiny. If the company allows limited private use, the policy should say when employees can do so only during breaks and lunch hours. If the policy is vague, employees could successfully challenge it in court.

The other challenge that I have noticed is that medical technologists often share lab results reports with personally identifiable data without encrypting the information. A patient can be harmed if unauthorised access is obtained to the patient's results.

This should be evaluated using the principle of beneficence since there is a need to balance the risk of sending data unencrypted versus benefiting the patient by providing access to results timeously.

As an electronic mail system and information technology security personnel for the organisation I work for, I have access to confidential data. Knowing individuals' and organisations' networks and systems provides me with a privilege that can be abused deliberately or inadvertently. Technical knowledge and skills are usually the focus of education and training for IT professionals and information security specialists. You learn how to perform tasks, but with little consideration of how those abilities can be misused. In most cases, IT professionals are not aware of ethical issues related to their jobs.

Most of the ethical issues IT professionals face in their profession are related to privacy. As an administrator of a mailing system, I should not access or read network users' emails because I can do so due to the privileges of being the administrator. Yet, there is a need to ensure that the company's sensitive data is protected and is not disclosed through email systems. It is ethical to inform network users through a policy if you are going to scan emails for data leakage protection before you can proceed.

The other ethical issue is with internet web proxy servers. Web browsing data of network users is still private, yet employers collect and store the browsing data through proxy servers. Although collecting and storing web browsing data may be ethically questionable concerning privacy, the employer still needs to filter traffic and stop accessing websites that may expose other employees to the content they find harmful.

**References:**

Buerck, J. P., Fisher, J. E. and Mathieu, R. G. (2011) 'Ethical dimensions of spam', *International Journal of Electronic Business*, 9(4), p. 350. doi: 10.1504/ijeb.2011.043255.