

Monitoring Internet Use

Does your college monitor staff or student (“users”) emails or their use of the Internet?

If the answer is yes then you should ensure that such monitoring is lawful or, the college could fall foul of the law.



The long-awaited revised Part 3 of the Employment Practices Data Protection Code (the Code) has finally been published by the Information Commissioner. Part 3 deals with the sensitive issue of monitoring in the workplace and is available at <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>. It covers mainly systematic or routine monitoring, but also occasional monitoring of users. The Code gives numerous examples of what it will apply to. These include randomly opening up individual users' emails, listening to their voicemails or monitoring their use of the internet.

Can your College monitor?

Before you can consider how to apply the Code to your monitoring activities, it is important to consider first whether or not the monitoring is permitted within the wider legal framework. “Live” monitoring, including the interception of phone calls or emails before they have been opened or “listening in” on users is subject to regulation from a number of sources.

Primarily, under the Regulation of Investigatory Powers Act 2000 (RIPA), a college must have either lawful authority or consent of the recipient and the sender, to intercept a communication in the course of transmission. This includes accessing communications such as voicemail and emails.

However, the Lawful Business Practice Regulations permit exceptions to RIPA by allowing monitoring for specific reasons, including:

- Operational purposes, e.g. to secure effective operation of their telecommunications systems, to protect against viruses or to forward emails to their correct destination;
- Routine access to business communications, e.g. to check voicemail systems when users are on holiday or sick; and
- Prevention or detection of crime.

Be aware that the Human Rights Act 1998 gives the users the right to respect for their private life and correspondence. Interference is permissible only if it can be justified as necessary for and proportionate to a legitimate aim. It can be a fine balancing act!

The Code compliments and reinforces the wider legal framework in relation to the monitoring of “recorded” information, such as CCTV footage, voice messages or e-mails. It explains how the Data Protection Act 1988 (DPA) protects a user’s right to privacy whilst also endeavouring to balance that protection against the needs of colleges to monitor. The Code details various areas of good practice to be followed which include:

1. Managing Data Protection

The Code encourages the establishment of a data protection “culture”. Colleges should appoint a person with the responsibility for compliance with the DPA, and mechanisms should be in place so that correct procedures are followed.

Anyone who has responsibility for processing information about users should understand their responsibilities. Make users aware of the possibility of criminal liabilities should they knowingly or recklessly disclose personal data in breach of the colleges’ policies and procedures. Serious breaches of the data protection rules should constitute a disciplinary offence.

2. The General Approach to Monitoring

The Human Rights Act gives users a legitimate expectation that their personal lives are private and they are entitled to a degree of privacy at work. Most monitoring will be intrusive, therefore colleges must make users aware of its nature and why it is taking place. One of the most valuable lessons to learn from the Code is the importance of carrying out an impact assessment to ensure that any monitoring is necessary.

As with all personal information, information collected via monitoring can only be used for the purpose for which it was collected. Where unexpected information is revealed, the college should disregard it unless it is “clearly in the user’s interest or reveals activity that no reasonable person could be expected to ignore”, e.g. criminal activity, gross misconduct or breaches of health and safety rules.

Keep to a minimum those persons that are granted access to personal information obtained through monitoring. Such information must be kept confidential and adequate security put in place to protect it. However, users must be allowed to have access to, and make representations about, information held about them obtained via monitoring which may have an adverse impact on them.

3. Monitoring Electronic Communications

Colleges wishing to monitor electronic communications must have a policy in place and ensure that it is communicated to users. The policy should cover:

- the circumstances in which users can or cannot use the colleges' equipment for private use;
- any restrictions that apply to private use and the penalties for breach of the policy; and
- the purposes and method of any monitoring.

Individuals who make or receive calls or emails from or to the college must be made aware that monitoring is taking place and the reasons for it. Individuals should be given the benefit of the doubt. They may visit web-sites unwittingly or by mistake. Personal e-mails should only be opened in exceptional circumstances (e.g. where harassment or criminal activity is suspected).

4. Covert Monitoring

Covert monitoring is only justified in cases involving suspected criminal activities or malpractice or the apprehension or prosecution of offenders. Senior management should be required to authorise any covert monitoring, and should note that justification is rare, so use only in exceptional circumstances. The recommendation provided within the Code is that covert monitoring is limited to circumstances in which the Police would be interested, and where openness would prejudice the investigation.

What to do now?

Whilst the Code is only guidance issued by the Information Commissioner and not legally binding, compliance will protect a college against challenges that they are not complying with the DPA. Breach of the DPA can be a criminal offence. The courts are also adopting a robust approach to evidence obtained in breach of the DPA. Evidence obtained in breach may be thrown out, or the Court may admit the evidence in the interests of justice, but show its dissatisfaction through an order for costs.

It is important that colleges take this opportunity to review any monitoring that is currently taking place and assess its impact on its users. Going forward, colleges need to create a culture of communication and compliance within their organisation.

Five Fundamentals

1. Notify the Information Commissioner of the way in which you collect and use data;
2. Understand that users have a reasonable expectation of privacy;
3. Communicate - need to tell users monitoring is taking place;
4. Be proportionate - carry out impact assessments for all monitoring; and
5. Be prepared - have policies in place and get your users on board.

An impact assessment should address the following:

1. Identify clearly the purpose(s) behind the monitoring arrangement and the benefits it is likely to deliver;
2. Identify any likely adverse impact of the monitoring arrangement;
3. Consider alternatives to monitoring or different ways in which it might be carried out;
4. Take into account the obligations that arise from monitoring; and
5. Judge whether monitoring is justified.

The JISC Legal Information Service runs a helpdesk for Further Education Colleges where you can email or telephone for information on the legal issues you have to tackle in your work.

Telephone - 0141 548 4939
email - jlis@strath.ac.uk
web: www.jisc.ac.uk/legal

Eversheds is a leading law firm in the education sector and has the largest education team in the UK. They offer an online Knowledge Bank dedicated to senior managers in Further and Higher Education Colleges providing a full range of information, services and news. Their website can be accessed at - www.eversheds.com. For further information please contact John Boardman at johnboardman@eversheds.com or John Skelton at johnskelton@eversheds.com.

