

# FAQ'S Webcast - Interception & Monitoring Law - 16 May 2007



The JISC Legal Interception & Monitoring Law Webcast took place on 16 May 2007. We have compiled on this page a selection of questions together with our responses based on the questions which were asked live by viewers during the Webcast. If you have a query on the use of Information Technology by the FE or HE sector then please use our Enquiry Form online.

**20 June 2007**

---

## FAQ'S Webcast

1. [Would a blanket acceptable use policy which prohibits personal communications through the college network be enough to permit lawful monitoring of all email and Internet use if users breach the policy?](#)
2. [Is it acceptable to incorporate a clause within the IT Policy that states that users are obliged to nominate a colleague to have proxy access to their email account in order that messages can be checked during periods of absence?](#)
3. [Where does an institution stand when a user has shared his or her mailbox? Can it gain access to the original account via the third party?](#)
4. [With regards to obtaining consent from the sender and or receiver of emails to access their accounts, is verbal permission sufficient or does consent have to be in writing?](#)
5. [Can I still gain access to a staff/student email account if it has proved impossible to contact the sender or recipient of the emails?](#)
6. [Is it necessary to get a new member of staff to agree to sign to the terms and conditions of the IT policy or can consent be assumed when they take the post?](#)
7. [Can an institution monitor lawfully to guard against spam?](#)
8. [Is making archives classed as monitoring?](#)
9. [Should the police disclose details of the statutory powers that they are exercising with regards to monitoring?](#)
10. [It is accepted that interception of bulletin board postings could be illegal. However, could this right be offset against the needs of the service provider to ensure that there is no breach of copyright or libellous content? What if users were alumni?](#)
11. [Is there a recognised amount, say in percentage terms, that is considered as reasonable private use? And, what is reasonable in terms of private disk space? What could an institution do if these terms were breached?](#)
12. [What would be the position if a request for management information exposed operational staff to personal data?](#)
13. [Would it be lawful to use an automated recording service for the purpose of monitoring specified telephone lines for security reasons?](#)
14. [A member of staff accidentally sends confidential mail to a student who has the same name as the intended recipient \(member of staff\). The sender](#)

- [requests that the information be deleted. Can this be done and what guidelines should I follow?](#)
15. [Can a head of department make an FOI request to his employer, the institution, to trace personal data of an employee who has asked an anonymous question?](#)
  16. [Do the same monitoring rules apply to CCTV?](#)
  17. [Whilst investigating inappropriate use of emails you often discover an inappropriate circulated email, chain letter etc. How far down the line should one go for investigative purposes?](#)
  18. [Do the provisions of the Terrorism Act have any impact on this area of law?](#)
  19. [Can we covertly monitor students' online activity?](#)
  20. [Is it legal to use a program \(such as Imperata\) to monitor what students are doing? Further, if they use the internet inappropriately and I close it down, is this legal?](#)

**1. Would a blanket acceptable use policy which prohibits personal communications through the college network be enough to permit lawful monitoring of all email and Internet use if users breach the policy?**

No, an acceptable use policy does not over-ride the law in relation to monitoring. All monitoring must be carried out in accordance with the law. The employer must take every reasonable step to advise the sender and the recipient to the email that their communications are subject to monitoring. Difficulties may arise with regards to strict enforcement policy terms.. If a policy prohibits personal communications where is the line to be drawn? For example, employees may have built up personal relationships with an external party and communications between them may involve a personal element. Further is it practical, desirable or reasonable to inform in advance every external sender about the terms of your policy? For further details please refer to the 'Your Questions Answered' and the 'Panel Discussion' (3.34-3.45) sessions available on our webcast at 1hr 28 min and 40 sec and 1hr 45mins and 22 sec - [Interception and Monitoring Law Webcast](#).

**2. Is it acceptable to incorporate a clause within the IT Policy that states that users are obliged to nominate a colleague to have proxy access to their email account in order that messages can be checked during periods of absence?**

This is a matter of consent and how consent is achieved. The Information Commissioner has published detailed guidance in Part 4 of the Employment Practices Data Protection Code, on consent which states 'for consent to be relied upon it must be given freely'. This document can be accessed online at - <http://www.ico.gov.uk/>.

While it is acceptable to incorporate such a clause as a matter of policy it may again raise concerns with regards to distinguishing between private and business communications. For example, would a communication from an HR Department on the subject of 'sick days' or 'grievance' be regarded as business or personal? Further, would it be more appropriate for management to access the account rather a colleague? A clear policy with regard to what happens during absence is

considered acceptable and indeed desirable. It is a matter for the college to agree the best internal approach. Again the Information Commissioner offers detailed guidance on accessing communications during periods of absence. The Employment Practices Code Part 3 can be accessed at - [http://www.ico.gov.uk/for\\_organisations/topic\\_specific\\_guides/employment.aspx](http://www.ico.gov.uk/for_organisations/topic_specific_guides/employment.aspx).

**3. Where does an institution stand when a user has shared his or her mailbox? Can it gain access to the original account via the third party?**

The short answer is no, not simply as a matter of course. Once again the institution should seek permission to access an email account from both the sender and the recipient of the email. The general terms and conditions of monitoring apply. Institutions should look at the Employment Practices Data Protection Code, Part 3 which relates to monitoring at work issued by the Information Commissioner. It aims to strike a balance between the rights of employees and the needs of employers. This should be read in line with the Data Protection Act 1998 and The Regulation of Investigatory Powers Act 2000. To access the Code please refer to the Information Commissioner's website at - [http://www.ico.gov.uk/for\\_organisations/topic\\_specific\\_guides/employment.aspx](http://www.ico.gov.uk/for_organisations/topic_specific_guides/employment.aspx).

**4. With regards to obtaining consent from the sender and or receiver of emails to access their accounts, is verbal permission sufficient or does consent have to be in writing?**

A verbal agreement is as valid as a written one in this instance. However, the existence of it and its exact terms are far more difficult to establish than that of a written agreement. This may be of relevance in a dispute with an employee. It is worth noting that an agreement in writing can be substantiated by producing the documentation. Therefore, it is best wherever possible to obtain written consent.

**5. Can I still gain access to a staff/student email account if it has proved impossible to contact the sender or recipient of the emails?**

Any monitoring must be done in accordance with the law. The Information Commissioner provides detailed guidance on how to balance the rights of the individual with the employer's business needs. For full details please refer to the Employment Practices Code on the Information Commissioners website at - [http://www.ico.gov.uk/for\\_organisations/topic\\_specific\\_guides/employment.aspx](http://www.ico.gov.uk/for_organisations/topic_specific_guides/employment.aspx). Further information is also available on the JISC Legal website at – [Inappropriate Use of Computers](#).

It is suggested in this document that if you conclude that an account must be accessed that you seek permission from a Senior Officer, a log/audit is maintained on what is accessed and access is made for specific clear purpose.

**6. Is it necessary to get a new member of staff to agree to sign to the terms and conditions of the IT policy or can consent be assumed when they take the post?**

It is important that the terms and conditions of any IT Policy are clearly communicated to employees at the outset. The institution's rules and standards must be made known and understood by employees. To minimise the risk of future conflict, best practice suggests that if an employee accepts a job offer which includes adherence to the IT Policy then the policy terms should be made available to the prospective employee prior to acceptance of the post.

**7. Can an institution monitor lawfully to guard against spam?**

Yes. An institution can lawfully monitor system traffic to ensure the effective performance of its network. This would include the elimination of spam. For further information please refer to the 'FAQ' session of our webcast (2.40-2.55) available at 48 min - [Interception and Monitoring Law Webcast](#).

**8. Is making archives classed as monitoring?**

Archiving material may often have data protection implications. For further details on this please refer to 'Your Questions Answered' (3.25-3.35) session of our webcast at 1hr 33 min and 19 sec - [Interception and Monitoring Law Webcast](#).

**9. Should the police disclose details of the statutory powers that they are exercising with regards to monitoring?**

Yes. For a full response to this please refer to the FAQ (2.40-2.55) and Accessing Hard Drives (3.05-3.20) sessions of our webcast available at 54 min and 39 sec and 1hr 7 min and 50 sec - [Interception and Monitoring Law Webcast](#).

**10. It is accepted that interception of bulletin board postings could be illegal. However, could this right be offset against the needs of the service provider to ensure that there is no breach of copyright or libellous content? What if users were alumni?**

For a detailed discussion on this please refer to the 'FAQ' (2.40-2.55) session of our webcast at 51 min - [Interception and Monitoring Law Webcast](#).

For detailed coverage on third party content please refer to the publication entitled '[FE/HE Institutions Liability for Third Party Provided Content](#)' available on the JISC

Legal website. If alumni are permitted to use your systems this use should be subject to adherence to the acceptable use policy.

**11. Is there a recognised amount, say in percentage terms, that is considered as reasonable private use? And, what is reasonable in terms of private disk space? What could an institution do if these terms were breached?**

The legislation does not set out in percentage terms, or indeed otherwise, an acceptable level of private disk space. Private use terms are for individual institutions to decide. For more details please go to the 'FAQ' (2.40-2.55) and 'Your Questions Answered' (3.25-3.35) sessions available on our webcast at 57 min and 1hr 29 min and 30 sec - [Interception and Monitoring Law Webcast](#).

**12. What would be the position if a request for management information exposed operations I staff to personal data?**

In the course of employment some staff routinely handle personal data as part of their role and such data should be handled in accordance with the college data protection policy and the eight data protection principles set out in the Data Protection Act 1998. Please refer to the JISC Legal [Data Protection](#) web pages.

**13. Would it be lawful to use an automated recording service for the purpose of monitoring specified telephone lines for security reasons?**

Not necessarily. The case of Halford v UK 1997 IRLR 471 highlights the potential consequences employers might face if they do not monitor lawfully. In this case, the pursuer alleged that her employer had tapped her private telephone line. It was held that her employer had given no prior warning that her line would be intercepted. On this basis it was found to be in breach of Article 8 of the European Convention on Human Rights (ECHR). The same monitoring rules apply to email and Internet use as to telephone calls. For general guidance on the interception and monitoring of communications please refer to the 'Overview of the Law' (2.05-2.15) session of our webcast available at - [Interception and Monitoring Law Webcast](#).

**14. A member of staff accidentally sends confidential mail to a student who has the same name as the intended recipient (member of staff). The sender requests that the information be deleted. Can this be done and what guidelines should I follow?**

Pragmatically, the best way forward may be to approach the student directly to resolve the issue. However, if it is necessary to access the student account then this

must be done lawfully and in accordance with the institution's monitoring and data protection policies.

**15. Can a head of department make an FOI request to his employer, the institution, to trace personal data of an employee who has asked an anonymous question?**

Anyone may make a valid FOI request to a public authority. The public authority must release the information unless it is exempt from release under the legislation. One of the exemptions relates to personal information. If the information requested concerns a third party and disclosure would breach one of the data protection principles then subject to application of the public interest test the information in many of circumstances would not be released. For more information please refer to Personal Information (section 40) Awareness Guidance 1 on the ICO website at - [http://www.ico.gov.uk/what\\_we\\_cover/freedom\\_of\\_information/guidance.aspx](http://www.ico.gov.uk/what_we_cover/freedom_of_information/guidance.aspx).

**16. Do the same monitoring rules apply to CCTV?**

For comprehensive guidance on this topic refer to the ICO website at - [http://www.ico.gov.uk/for\\_organisations/topic\\_specific\\_guides/cctv.aspx](http://www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspx). These pages include a Good Practice Note, Checklist and a Code of Practice relating specifically to CCTV.

**17. Whilst investigating inappropriate use of emails you often discover an inappropriate circulated email, chain letter etc. How far down the line should one go for investigative purposes?**

Circulating chain letters and emails does not necessarily breach any laws per se. Any monitoring and investigation of such emails must be carried out within the law.

**18. Do the provisions of the Terrorism Act have any impact on this area of law?**

Yes. There are specific monitoring powers afforded to the police and other security bodies. For basic information on terrorism laws please refer to the Home Office website at - <http://www.homeoffice.gov.uk/security/terrorism-and-the-law/?view=Standard>. Further information is also available on the JISC Legal website at – [JISC Legal Terrorism](#).

## **19. Can we covertly monitor students' online activity?**

The Employment Practices Data Protection Code published by the Information Commissioner states that 'covert monitoring should not normally be considered'. Further as far as we are aware there is no evidence to suggest that students should be considered differently in this regard. Covert monitoring of behaviour can only be justified in very limited circumstance such as suspicion of criminal activity. Third party organisations such as the police can carry out covert monitoring in limited circumstances with appropriate authorisation. Authorisation (usually in the form of a warrant) will only be granted in certain circumstances such as in the interests of national security or for the purpose of preventing or detecting crime or of preventing disorder. The authorisation must be necessary and proportionate to what is to be achieved by it. It also must specify a description of the direct surveillance and it has to be carried out in the circumstances described in the authorisation and for the purposes described in the authorisation.

For full details please refer to the 'Panel Discussion' (3.35-3.45) session of our webcast available at 1hr 43 min and 15 sec - [Interception and Monitoring Law Webcast](#).

Further reading on this topic can be accessed at - <http://news.zdnet.co.uk/itmanagement/0,1000000308,2108075,00.htm> and - <http://www.out-law.com/page-445>.

Finally, the Employment Practices Data Protection Code can be accessed at - <http://www.ico.gov.uk/>.

## **20. Is it legal to use a program (such as Imperata) to monitor what students are doing? Further, if they use the internet inappropriately and I close it down, is this legal?**

If a college uses software to monitor student online activity then the student should be made aware that this is taking place. For example, the institution may wish to make reference to this in their acceptable use policy. For further discussion on this please refer to 'Your Questions Answered' (3.25-3.35) session available on our webcast at 1hr 25 min - [Interception and Monitoring Law Webcast](#).

**20 June 2007**

---

For a digest of IT Law relevant to FE and HE, subscribe to [JISC-LEGAL-NEWS](#).

---