

Interception & Monitoring Law Webcast Transcript - JISC Legal



The JISC Legal Interception & Monitoring Law Webcast took place on **16 May 2007**. Below is a transcript of the Webcast for information purposes.

Please note: this guidance has been prepared by JISC Legal for information purposes only and is not, nor is intended to be, legal advice. This information is not intended to constitute, and receipt of it does not constitute, a contract for legal advice or the establishment of a solicitor-client relationship.

22 June 2007

Table of Contents

- [1. Introduction with Jason Campbell](#)
- [2. An Overview of the Law with William Malcolm from Pinsent Masons Solicitors](#)
- [3. Legally Monitoring Your Network by Julia Hörnle from the Centre for Commercial Legal Studies](#)
- [4. Intercepting Communications with Jason Campbell](#)
- [5. Some Frequently Asked Questions... Answered with the JISC Legal team](#)
- [6. Accessing Staff & Student Network and Hard Drives with William Malcolm](#)
- [7. Scenarios with the JISC Legal team](#)
- [7. Scenarios with the JISC Legal team](#)
- [8. Your Questions Answered with Betty Willder, William Malcolm and Julia Hörnle](#)
- [9. Panel Discussion - with Jason Campbell, William Malcolm and Julia Hörnle](#)

1. Introduction with Jason Campbell

Chair: Good afternoon and welcome to this webcast from JISC Legal from the University of Strathclyde in Glasgow . Today, we're going to be dealing with interception and monitoring law a particularly topical subject. Now, if you've tuned in expecting to get Sevilla versus Espanola I'm afraid you might be disappointed. The football is taking place here tonight, and in fact you may hear from outside some chants of Espanola because we seem to have half of their support outside our building, and so please ignore the car horns. Any great cheering it's because of the great job we're doing of course here at JISC Legal.

Okay, this afternoon, what are we going to be looking at? Interception and Monitoring Law. And to give you a run down of how the programme's going to go. At 5 past 2 we're going to give you an overview of the entire area of law to set the scene. After that, at 2.15 we'll look at legally monitoring your network and that will be followed by me looking at intercepting communications within your university or college network.

At 2.40 the JISC Legal team will give you some frequently asked questions, and hopefully the answers that go along with them. We know then that you will probably be gasping for a coffee and so we will give you a ten minute break to run off and boil the kettle. And then we will go in half past 3 to accessing network and IT hard drives. At 3.20 we will look at some common scenarios that come up in our experience, and again give you an analysis of the law pertaining to those. At 3.25 we'll deal with your questions and we will give you the opportunity to ask questions as the webcast goes on and we'll answer them live here in the studio. At 3.35 we'll have a panel discussion looking at the wider issues involved in interception and monitoring within UK further education and higher education.

If you are not aware of what JISC Legal does, if I may say a few words? JISC Legal's mission is to stop legal issues becoming a barrier to the use of technology in colleges and universities in the United Kingdom . And to that end we do several activities. First of all we hold events and indeed you are participating in one at the moment, but more traditionally as well you will find us doing regional workshops throughout the country, often in cooperation with regional support centres, but we also hold national events too. We also have an enquiry service, and if you go to the JISC Legal website, www.jisclegal.ac.uk you will find a button there for enquiries with contact details and an enquiries form. We aim to reply to your enquiries within three working days.

We have guidance published on our website. Again, it's all relevant and all contextual and all practical, because we know that you want to know what to do yourself, not really an academic analysis of the law. And finally we offer a newsletter, which again is available from our website. It's free, it comes once a month by email, and hopefully again we will keep you up to date on what's relevant in the law.

So, back to interception and monitoring law, what are the objectives of it this afternoon? Well, first of all it's awareness. Hopefully many of you will be in institutions that are already complying with the law, sometimes by accident, sometimes by design, but we want to make sure that you understand what the legal duties are, what the legal possibilities are, and so you can have confidence in taking action. And secondly we will hopefully give you an understanding of the law so you can apply it. Thirdly we will ask you to reflect on your institution's practices, to maybe ask if you've got the right policies in place, to ask if you are sure whose permission needs to be given for interception and monitoring to take place.

Throughout this webcast we're going to refer a little bit differently to monitoring and interception. Monitoring we're going to use primarily to mean the general looking at what goes on. For example for SPAM monitoring, you will understand. Interception will mean interception of communications. That's looking at specific communications, or specific user's attempt. Now of course there's a fuzzy line in between those two concepts of monitoring and interception, but, if you bear in mind when you are using monitoring and interception that's the definition that we're going for.

Of course there's a lot to take in an hour and three quarters this afternoon and so this recording will be available in a streaming version and also in a bite-sized downloadable version after the event.

Well, we want you to interact. This is the reason that we're doing it live. Hopefully you will notice on your screen, if you are using the embedded player or back on the website you will find a button that submits your questions. Hopefully somewhere down by my feet on your screen. We want you to put in the questions that matter to you, and we will try and deal with them as we go through. We won't mention your name, we won't mention your institution, so please be candid when asking them, and we hopefully then will meet your needs in delivering this webcast.

For the moment what I'd like you to do is actually press that button, submit your questions and say hello to us. Type in your first name, perhaps your institution for us, and say hello, just to try it out. It shouldn't interrupt your webcast. To get you to interact also, at the end of today's webcast we'd ask you to fill in the evaluation form, which there is a link to down there as well. Why would you want to fill in our evaluation form? Well, we have the answer, if you'll excuse me, we have one here, one pristine Play Station Portable and there will be a prize draw for those from UK further and higher education who submit the evaluation prize, and one lucky person will be the winner of this Play Station Portable. I do believe it can be used for educational purposes as well as playing games and watching videos and such. Good luck.

That brings me to the end of the introduction and it's time now to introduce two speakers that we have with us in the studio today. First of all we have William Malcolm. He's an Associate Solicitor with Pinsent Masons who do an awful lot of work in technology law and in particular you may have seen their Outlaw site. For information you should go to www.pinsentmasons.com. William is an associate solicitor and is an expert on privacy and data protection law. He's also working with us to write a publication on model policies on access to email and user IT accounts, and that should be available shortly to accompany this webcast.

With that I will hand over to William. We've also got Julia with us in the studio, and I will introduce her once William's finished. With that, it's over to William.

[Back to top](#)

2. An Overview of the Law with William Malcolm from Pinsent Masons Solicitors

William Malcolm: Okay, thanks very much for that introduction. So a lot to take in, in relation to today's topic, and really the first segment I've been asked to give you an overview of the law that applies in this area. Now, you will be relieved to hear, particularly if you haven't had the benefit of a coffee as yet that I'm not going to give you a blow-by-blow account of each section of the principle pieces of legislation. What this section is really designed to do is to allow you to navigate your way through often quite contradictory or apparently contradictory pieces of legislation so that we've got an overall picture of what the requirements are placed upon you as colleges and universities when you monitor, or indeed intercept. So, with that in mind, I'd be asking you if you've got any specific burning issues about the interpretation of any of the pieces of legislation. Things that are on your mind that I

don't cover, because we're only looking at this in general terms, now is the time to submit those questions. And we can look at that later in the session when we do the question and answer session.

So moving on then to an overview of the relevant law. Coming up on the screen now hopefully should be four bullet points on a slide and this really sets out in the UK terms the four main pieces of legislation that impact on this area. Now, why this area is often so confusing is because there is no single piece of law that looks at what you should be doing in this area. Effectively we've got different pieces of legislation designed for different purposes, most of them flowing from European legal requirements and most of them quite general, and all of these pieces of legislation have something to say about how you monitor and intercept the communications of staff and students.

Let's run through them. We've got the Regulation of Investigatory Powers Act 2000. We've got the Telecommunications (Lawful Business Practice) Interception of Communications) Regulations 2000. A snappy title. I will be referring to them as the Lawful Business Practice Regulations. We've got the Data Protection Act 1998, which is something many of you will have at least a passing knowledge of. And we've got the Human Rights Act 1998.

Now, I mentioned at the start that these pieces of legislation are designed to do very different things. Let's just try and keep in our heads what they're designed to do as we walk our way through this, because sometimes knowing what a piece of legislation is for actually helps you get to the right answer even before you've looked at the specific part of the act in question.

The Regulation of Investigatory Powers Act really exists in the UK to put monitoring on, for our purposes, monitoring on electronic communications network on a statutory footing. Well, what do we mean by that? What it means is that the act gives lawful authority to those who want to intercept communications on electronic networks, and it does that in a variety of ways. It gives the police lawful authority to intercept if they've got the appropriate warrant or they've got the appropriate reason. But it also sets out all of the circumstances in which it's appropriate to intercept communications on networks.

One of the things that I will be looking at when I talk about it in a bit more detail is the flow-through from that to the Lawful Business Practice Regulations.

What about the Data Protection Act? Well, it's a kind of broad piece of legislation which of course relates to the processing of all personal data, so that's really anything which identifies and relates to a living individual, whether that's a member of staff, a student or a third party mentioned in an email or communication that a member of staff or student receive.

And then finally we've got the Human Rights Act which of course applies to all public authorities, including universities and FE colleges, and really is designed to protect the fundamental rights and freedoms of individuals. And of course the relevant part here we'll be looking at is the Right to Privacy.

So a little bit more on RIPA then. What does RIPA do? Well, it forbids the interception of communications on electronic networks. Now I'm using that term effectively as a bit of a catch-all for the purposes of today's presentation.

What is an interception? Well, we'll be hearing a little bit more about that later, but for our current purposes an interception effectively relates to accessing a communication on an email on a network. Say you had an email sitting in someone's inbox unopened. Looking at that email would be classed as an interception. Similarly, if that email had been opened and filed in someone's personal filing folders down the side in Outlook Express, then that would also probably be classed as an interception, to access that communication in that way. So it's looking at a specific communication generally with a specific purpose in mind. Now of course interception is allowed with the consent of both parties to the communication, and where it's connected with the operation of the servers, but more generally the Lawful Business Practice Regulations set out the situations in which it's appropriate for businesses and universities and colleges to intercept communications. And these regulations provide the lawful authority that you need in order to carry out any interception activities, but only in defined circumstances. They apply to business communications, or communications related to the conduct of your business only and exceptionally to ascertain whether a communication is a business or personal communication.

Now, what's important here is that these regulations give you the authority to effectively intercept or monitor, or whatever way you want to phrase it, communications that are related to the business. Not personal communications. So a communication sent from a member of staff's email account to say his wife, or sent to a member of staff's family would not be. You would not have authority to intercept that by virtue of these regulations. So it's important to distinguish between communications which are private, and communications which relate to the operation of the business. These regulations will give you, by and large, the power to intercept relating to business communications.

The Data Protection Act sets out some comprehensive information with respect to monitoring, and all monitoring has to be fair, it has to be lawful, and it has to be proportionate. So when you monitor you've got to monitor taking account of the people's rights under the Data Protection Act.

And finally we talked at the outset about the Human Rights Act, an important piece of legislation which really incorporates the convention of human rights into UK law, and sets out the importance of giving people effectively some respect on their private life. The relevant part of the human rights convention for those purposes being the Convention of Human Rights Article 8.

So what does all this mean? Well, really what it comes down to is that you can monitor as long as it's lawful, proportionate and people are aware that the monitoring is taking place, and provided that you are monitoring communications relating to the business, and you are not interfering in people's private communications or the operation of their private life. And that's a fairly general statement which we'll investigate and drill into and look at with respect to scenarios as the presentation goes on this afternoon.

If you are looking for further guidance on this then the information commissioner which is the UK data regulator for the Data Protection Act, has set down some quite detailed guidance with respect to monitoring of employees, and this guidance, although it's aimed at employees, or monitoring of employees, there's some good practice hints and tips in there which are relevant if you monitor employees or students. So some common sense effectively bite-size information and you can get that from the Information Commissioner's website.

So how do you decide? One of the important things about monitoring, if we talk about respecting people's privacy, we talk about transparency, we talk about openness and all of the principles that flow from these complex pieces of legislation, is working out the impact that your monitoring will have on people's private lives, working out whether it's appropriate, and above all working out whether it's justified in the circumstances.

Now, the next speaker will talk in more detail about impact assessments and how you conduct an impact assessment. All I am going to say is that, before you do any monitoring work out what's the purpose of doing it? What are the real benefits of doing it? What's the adverse impact on the people we're monitoring? And considering different ways of achieving the same objective.

So how do we go about being open about monitoring and interception? Well, it's very important to have a communications policy and to notify others, where possible, about your monitoring and interception activities both internally and externally. Now, internal monitoring you cover by having a communications policy, sometimes referred to as an authorised use policy or an IT systems policy, and it should set out all users of the IT equipment within your university or college, what monitoring will take place and what interception will take place. Whether that's at a system level, whether that's to monitor for inappropriate material, whether that's to monitor general compliance with university college rules and procedures. And then externally, well there's lots of opportunities. Recorded messages and call scripts, terms and conditions for services, websites, email notices which are compulsorily printed on the bottom of most of our emails let people know, if they're replying to that email, what's going to happen, that the internal communication will be monitored.

So in a nutshell then, the key to all of this is monitoring is permitted within sensible limits and that you've got to develop a clear policy which is based on evidence that the monitoring is required and that the monitoring will be effective. Develop that clear policy and communicate it to staff and students alike in as many places as possible. You could incorporate it into the terms and conditions of staff, you can publish it on intranets, and you can let students know at matriculation effectively what the impact of the IT policy is.

Don't do it covertly. Let people know, be open and respect people's private life. And if you do those things, overall you will discover that these very four complex pieces of legislation by and large won't come back to bite you.

Now, I realise that's a very kind of general overview of a very, very complicated area, but hopefully it will give you some grasp of the concepts which inform the case studies and the things that we're looking at this afternoon.

That's all I have in this first section, and I'll hand back to our chair.

Chair: Thank you very much William, that was a very clear and concise overview of the issues that are involved there.

It's a very topical issue here because you may have seen last month the case of Coplands which was about Carmarthenshire College, and the facts go back a very long way. In fact prior to the current legislation. But it was an example of a personal assistant whose email and telephone use was being monitored, and unfortunately the UK government and the college came out on the wrong end of that case, and it brings to light certainly the topicality of the subject.

If I could next introduce Julia Hörnle from the Centre for Commercial Law Studies, based at the Queen Mary and Westfield. She's been researching and teaching the legal issues relating to the internet and e-commerce for some eight years now, and she is about to publish a book on internet dispute resolution later this year, unless it's been published already?

Julia Hörnle : Not quite yet.

Chair : Not quite yet. Without further ado I will hand over to Julia to take you through legally monitoring your network.

[Back to top](#)

3. Legally Monitoring Your Network by Julia Hörnle from the Centre for Commercial Legal Studies

Julia Hörnle : Hello, good afternoon. I think as has been obvious from William's presentation there are many different pieces of law and legislation which overlap and which make this area extremely complex in practice, and what my task is this afternoon is really to give you a very practical overview what these pieces of law mean in practice. Monitoring can obviously be justified. While the Data Protection Act and Regulation of Investigatory Powers Act do provide for criminal and civil liability for unlawful monitoring and interception, on the other hand the law also clearly provides that monitoring is lawful in certain circumstances. So where is the line between lawful and unlawful monitoring?

Well, there are basically two different methods to make monitoring lawful. The first one and perhaps the obvious one is consent. But the issue here is that under the Human Rights Act and the interpretations of the Data Protection Legislation, consent has to be voluntarily and freely given. Now, in the Employment Law relationship, such as between college and staff, and of course also in the student / college relationship, there is at least a question mark how voluntary consent is. So therefore in a way it may be safer not to rely on consent, but to rely on legitimate business

reasons for monitoring, because that is the second element which makes monitoring lawful.

Essentially it's a proportionality test. What does that mean? Well, first of all it means that colleges have to identify a legitimate business reason why they have to monitor data or e-communications. Secondly, they have to assess the positive benefits of the monitoring activity. In other words, is the monitoring actually effective? Does it achieve any benefits? And that has to be weighed against the negative impacts on the students, or the negative impacts on the privacy of staff. So this is what we mean by proportionality test.

I will go into more detail on this and obviously it's very, very fact-specific, so it's especially in this area I think where if you send us emails about your specific questions, your specific factual scenarios where our advice could be very helpful.

Now the Lawful Business Practice Regulations which William has also referred to actually contain a whole list of what could be a legitimate business objective in monitoring email or other e-communications. It's kind of difficult to think of a business objective which is not covered in the regulations, so I think this is probably not very difficult to establish. I will very briefly go through these.

The first one is, it is legitimate to monitor in order to establish facts. So for example, an employee or a member of staff had an accident, it's necessary to check which emails are related to the business, which emails need urgent answering, therefore it has to be established which of these emails relate to the business. So that's the type of thing which is envisaged here.

Secondly, clearly where colleges have to comply with regulation, or self-regulation, or proper standards, then again monitoring can be justified. For example, checking that members of staff or students don't misuse the facilities for sending out SPAM.

Then quality assurance and training is another issue clearly, for example monitoring staff's use of a web teaching platform to ensure the quality of the teaching could fall under this heading.

Another legitimate reason is interests of national security and also the prevention and detection of crime. So clearly if there is a reasonable suspicion that some terrorist activities are taking place on college servers that could be another legitimate reason to monitor.

Then also the purpose of investigating unauthorised use is clearly a legitimate business reason. For example, excessive use of e-communication facilities. Then finally clearly ensuring the effective operation of the system would be another legitimate business reason, such as guarding against viruses, guarding against external attacks. But it's very important to remember that it is not sufficient just to have a legitimate reason. The actual monitoring also has to be necessary. It has to be proportionate in relation to that business objective. So basically, before a particular type of monitoring is implemented the question has to be asked 'Is this monitoring effective to achieve the legitimate business objective? What are the real benefits of the monitoring?' Secondly, one has to ask oneself whether there is a less

intrusive form of monitoring which effectively fulfils the same purpose. In other words, is this type of monitoring really necessary?

So basically in weighing up the benefits and the negative effects of the monitoring, the following considerations have to be taken into account.

First of all, both students and staff, to a certain extent, have a legitimate expectation that they have some degree of privacy even in the work place or even in the context of college activities.

Secondly, it is recommended that staff and students should mark personal emails as such or personal communications as such. Either by saying they are private or from the context. And if an email, or a folder on a network space for example, is marked as private, then it's contents should not be monitored unless it is really, really necessary. For example if there is a suspicion of illegal activity or if there is a case of harassment going on.

Also, it has to be kept in mind that not all monitoring is equally intrusive. For example, if one uses automatic monitoring by the use of some type of software, this could be less intrusive than having a physical person actually looking at email or email headings. Clearly if the content or aspects of the content are not seen by human eyes that is less intrusive. Clearly occasional forms of monitoring, spot checks are also less intrusive than the systematic monitoring of all e-communications.

Generally speaking, content monitoring is also more invasive than the monitoring of traffic data. Now what is content as opposed to traffic data? Traffic data would be, for example, in an email the recipient and the sender. In a website communication it would be the URL rather than the content of the website. But it has to be kept in mind that clearly even traffic data contains some degree of content because clearly a URL might reveal the type of content which is available on that website. So for example the URL www.poka.com would give an indication that this is an online gambling site.

Furthermore, instead of monitoring traffic data or content data it might be less intrusive to actually look at file sizes, bandwidth, file extensions. So for example jpeg files would indicate that there is possibly an image which then could indicate some sort of illegal or unauthorised activity going on, depending on the context of course. So, if a system administrator is concerned, for example, about many images being shared by students or network space being used up by images and there is no reason for that, then that could be an indication that something unauthorised is going on.

Finally, I think it's also probably less intrusive to prevent any system abuse than monitoring for it. So for example, if it is possible to block URLs then this might be a better way to prevent system abuse rather than monitoring for it.

And then as William has already pointed out, but I think this is very worth repeating, is that covert monitoring will only be justified in the most exceptional cases. So, in other words, staff and students should be told about the monitoring. They should be

told that monitoring takes place, what type of monitoring takes place, and so basically, how and when and what.

Finally, it is also important to keep into account the interests and rights of third parties, not only the recipient of an email is affected in terms of data protection legislation for example, but also the sender. Or if a member of staff stores all their family photographs on a server for example, which I guess would be some form of unauthorised use, clearly the privacy of the family members would also be affected.

Then in this context it's also important to reduce the reasonable expectations of privacy which a member of staff or a student has, by clear notifications that monitoring is taking place, for example another method would be to use a non-personal email address, such as admissions@college.ac.uk, because that would kind of indicate to the world at large that this is not a personal email address but primarily a work email address.

In the slides on the examples again, that shows the kind of legitimate reasons for which monitoring could be justified. I think in the amount of time I have I don't have the time to go through them, so I will just go through them.

I want to conclude by just very briefly listing other legal obligations, apart from monitoring, which have to be taken into account. The main point here again is that an Acceptable Use Policy should clearly outline what type of use is permissible and what isn't. In particular the type and amount of personal use which is allowed. The policy should also, as I've said before, and as Williams said before, the type of monitoring which is actually carried out. This will, as I said, diminish the legitimate expectations of privacy. Furthermore, the policy should be easily accessible. I had actually had a look at our policy and it took me quite a while, it was sort of dug deep in the pages of the computer services, so guys, if you are listening out here that's no personal criticism here but I think staff have to be made aware that such a policy exists. This could take place for example when people are trained. When students or staff are given their email addresses and they're given their passwords, I think at this point it would be very useful to be pointed out that there is an acceptable use policy and what it contains, and also about monitoring.

Furthermore, of course the general obligations regarding personal data applies, so data collection must not be excessive and the personal data must not be kept longer than necessary. This means, for example, that logs have to be destroyed when they're no longer needed for the purposes of monitoring. Also, it's very important that data which is found as a result of monitoring is only used for the purpose for which monitoring is carried out, and for the purpose for which subjects have been informed. So for example, if the college is monitoring in order to prevent SPAM from being sent from college servers and a result of that monitoring it is found out that the member of staff is actually sending pornography or receiving pornography, well, in that case, that couldn't immediately lead to disciplinary action because the monitoring was only carried out for the purpose of discovering SPAM. Clearly, that could be then a reason for carrying out further monitoring and also clearly telling staff that there is monitoring for that reason.

The final point actually I should not forget is subject access request, clearly to the extent that monitoring uncovers personal data, the people whose data this is have right to ask the college what type of data is covered, and so monitoring software has to be compliant with this requirement.

I think I've covered monitoring now as much as I could in the short space allocated, so it's over to Jason to introduce the next session.

Chair: Thank you very much Julia and I know that speaking for 10 minutes as a legal academic is somewhat short in terms of this, that's the cliché that when you ask a law lecturer to speak for 10 minutes they speak for an hour, and if you ask a lawyer to speak for 10 minutes they bill you for an hour. Anyhow, moving on from there.

In about five minutes time we'll go over to some frequently asked questions, but until then I'm briefly going to deal with the subject of interception of communications directly.

[Back to top](#)

4. Intercepting Communications with Jason Campbell

First of all I think it's useful to remind ourselves why we would want to intercept communications, or indeed monitor at all. The typical scenarios we're looking at is first of all, as we all do, we're looking for viruses, trojans, malware of all sorts. Okay, that tends to be about automated processes. Sometimes we're looking for inappropriate content as well coming through, to stop that coming up on our college and university servers.

We're looking at inappropriate use of facilities. Sometimes students, and dare I say, staff, sometimes consider the internet access at work to be a free-for-all and apparently their own personal facility, and of course that can't be allowed in certain circumstances.

There's also a question of where a member of staff is absent, gaining access to their working communications, whether that be documents or communications with the outside world. The business of the college or university has to continue so we may need to get in to see what's going on there.

Of course more contentiously there are discipline questions that come up, whereby staff would like to see what's been going on from a student account or perhaps even a staff account, in order to verify facts with regards to a disciplinary procedure. And finally I suppose one that does come up is the tidying up after a person leaves an institution. It's quite rare I think, I'm told by IT persons that I know, that a person leaving an institution clears out the network drive, clears out all the communications, and sometimes IT staff are left with the situation what to do with it, especially if it's taking up a fair bit of room on a network drive.

These issues, these sorts of scenarios are compounded by the fact that there is sometimes a culture of people considering their email communications at work to be

a semi-personal facility as well and that's where the contentious elements can come up. There have been a few cases in recent times concerning the Regulation of Investigatory Powers Act, one regarded email diversion where someone re-configured an email server to send particular emails, a copy of them, to another person for mal purposes, shall we say? That ended up with a £20,000 fine, and so it can be quite a serious matter. A further case involved unauthorised voice-mail access and again that has lead to a prison sentence in fact. So, getting it wrong is not the question. If we're looking out for situations where people are just not complying and going outside their job in fact, and what we don't want to see is IT staff looking at accounts because they can. That is certainly not a lawful purpose, or indeed because it could be fun to do so.

There are also duties under the Data Protection Act and for example in a case under the Data Protection Act a Police Support, a Civilian Support Officer was found to have looked at the police records in order to find out details about her ex-husband, and that unfortunately was deemed to be criminal offence. Therefore purposes have to be related to the business of the institution.

Very briefly then, what is a communication defining it? Well, here we're talking about private networks. That is we're not talking about a public communications network, we're talking about information and passing it onto our college and university networks, and through the JANET network, which is probably a private network in itself. You may come across a different situation if you are running a public network, but that's not going to apply in almost all of our cases. The legislation is the Regulation of Investigatory Powers Act of 2000. There's a Scottish version which deals with the authority to conduct covert surveillance but it doesn't really concern us too much. The RIPA 2000, the UK Act will pretty much do for all of us, whichever of the jurisdictions in the UK we're in. Already the speakers before, Julia and William, have referred to the telecommunications regulations and those specify the purposes under which the interception can be done.

Moving on, there's also the Computer Misuse Act, and it's worthwhile pointing out here that going into a system without authorisation or for an unauthorised purpose can be a criminal offence under the Computer Misuse Act of 1990 also.

When it comes down to employment practices and dealing with employees for example disciplinary matters or investigating employment malpractice, then the Employment Practices Code and the supplementary guidance which is available from the UK Information Commissioner, provides valuable guidance in this area.

Going back to that question of what is interception. It's access to another person's communications without the consent of the sender and receiver. It must be in the course of transmission. Admittedly, that is a phrase that's not been defined by the courts. But take a cautious approach if you are accessing someone's email then you are really looking at an interception of communications there.

The important thing to realise is that without the authorisation of the controller of your local system, which means the College Principle, the University Principle, or someone with their delegated authority, then you could be committing a criminal offence by intercepting communications.

So, if you are intercepting communications you must make sure that you have the permission of such a person, and that permission is recorded. Even if you have the person's permission, that's not sufficient to avoid all legal problems.

Having the permission will stop it being a criminal offence. However, there may be civil liability, that is, you may be sued for compensation if you are not complying with the lawful business practices that Julia outlined.

With regards to interception, these tend to be purposes connected with the provision of the service, the provision of the telecommunication service, so that for example that might be re-addressing wrongly-addressed email or checking subject lines in emails for viruses for example.

Other interceptions may be allowed for the establishment of facts, again Julia eluded to ascertaining compliance with regulatory procedures or practices, ascertaining and demonstrating standards. Detecting unauthorised use, preventing or detecting crime in the interests of national security, though one might say that that's best left to the police, and indeed the authorities, the government authorities that deal with it and rather than becoming an amateur police force, it's best being left to the professionals in terms of that, and ensuring the effective operation of the system.

The interception must be made solely for the purpose of the monitoring or for the particular purpose that is lawful and a record of communications relevant to the systems controllers business must be made. In particular circumstances where, for example, calls to help lines may not be recorded. It's certainly not for private purposes of uses or for a bit of a laugh that communications can be intercepted.

With that I think it's time to get over to the nitty-gritty of what questions that you've been asking. If you remember, you can put questions to us now, please press that question button, fill it in, remember there's a PlayStation Portable available in the prize draw for evaluation, so bear that in mind. We'll give you a few frequently asked questions and then we'll give you a coffee break after that. Here's over to the frequently asked questions.

[Back to top](#)

5. Some Frequently Asked Questions... Answered with the JISC Legal team

FAQs:

Question 1: There seems to be a lot of legislation that applies to surveillance. The Data Protection Act 1998, The Regulation of Investigatory Powers Act 2000 known as RIPA, the Human Rights Act 1998 and the Telecommunications Lawful Business Practice Interception of Communications Regulations 2000. Why is this so complicated in a legal sense?

Answer: It is true that the legislation relating to interception and monitoring is complicated in the legal sense. The main reason for this is because the legislations

are interrelated to each other. A good example to illustrate this interrelationship is the situation concerning management of email communications at institutions. If on the one hand interception and monitoring of emails is permissible under the Lawful Business Regulations 2000 on the other such interceptions may raise questions relating to privacy and the Data Protection Act. Also, in situations where bullying or harassment of an individual is done by a fellow staff member, it is possible that the institution may be held liable for breach of the Human Rights Act. In such a case email communications can form part of the evidence in any legal action and would be available to the complainant by relying on the Data Protection Act.

Question 2: As part of maintaining the IT of the college it is sometimes necessary to get into user accounts. Is this legal?

Answer: The short answer is yes, with the consent of those individual users whose accounts are being accessed. Without express consent firstly what should be looked at is why it is necessary for some individual to access and view the contents of another user account. This access is considered processing in terms of the Data Protection Act. The purpose behind the processing should then be examined. If the processing arises because of bad systems, or general snooping, then this could be a breach of the Data Protection Act.

If the processing is in the legitimate interests of the college then it is likely to be justifiable in terms of data protection. However, the general requirement the data is processed fairly and lawfully must also be satisfied. It is accepted that those who maintain the IT infrastructure are likely to come across and process stored personal information of individuals. As stated previously, in these circumstances the Data Protection Act regime applies to the information. Anyone who has responsibility for accessing and processing information about users should understand the consequent responsibilities.

Each college is obliged to make staff and those with such access aware of their responsibilities. Serious breaches of the Data Protection rules are likely to constitute a disciplinary offence. It should also be remembered that there is the possibility of criminal liability should an individual knowingly or recklessly disclose personal data without lawful authority.

In summary, where such access to the content of user accounts is likely to be on an ongoing basis, consent to the processing should be obtained from those involved.

Question 3 : Many of our staff are not always in the office every day. Is it okay for one of the technical staff to log in and check for emails marked 'important' when the staff member is not in the office? Is this different for students?

Answer: As previously mentioned, where the content of emails is being viewed it is permissible usually only with the consent of the individuals concerned. Processing which includes opening and reading of private personal data installed emails by an institution without the consent of the individual could possibly breach data protection principles. Guidance issued by the Information Commissioner, the Employment Practices Code at Section 3.2 deals directly with this. It says 'Monitoring electronic communications' and I quote from there - 'where possible avoid opening emails,

especially ones that clearly show they are private or personal. Ensure that email monitoring is confined to address or headings unless it is essential for a valid and defined reason to examine content. Encourage workers to mark any personal emails as such, and encourage them to tell those who write to them to do the same. If workers are allowed to access personal email accounts from the workplace such email should only be monitored in exceptional circumstances. For some key staff clearly it is preferable to have a situation where important business emails are identified by the use of a role-based email address where the addressee email is something like headmaster@college.ac.uk or renewals@college.ac.uk. In that case the likelihood of personal information being processed is reduced.

With regard to students, it is hard to envisage when it will be necessary for an institution to keep track of important emails in an individual's absence without their consent.

Question 4: In what circumstances can a college search and look at staff and student communications and personal disk space?

Answer: A college can intercept communications to protect against computer viruses, to monitor how staff deal with customers, and to ensure workers are not using the internet to access offensive material. Briefly RIPA allows colleges and universities to carry out interceptions without the consent of the sender or the receiver of the communication in certain circumstances including for purposes connected with the provision of the service. A possible example might be re-addressing wrongly-addressed email, or checking subject lines in emails for viruses, and the monitoring of system traffic to ensure effective performance. A possible example might be finding out the source to cut down on SPAM. The Lawful Business Regulations permit interception in a number of circumstances, including to establish the existence of facts, to investigate or detect unauthorised use of a communication system, to prevent or detect crime, or in the interests of national security. Also to ensure the effective operation of the system.

Monitoring, but not recording, is also permissible in the following cases. To ascertain whether communication is business or personal and to protect or support help line staff. There are also additional conditions being the interception must be made solely for the purposes of monitoring or, where appropriate, keeping a record of communications relevant to the system's controller's business. That is relevant to the business of an FE or HE establishment. Every effort must have been made to inform users that this monitoring and recording is likely to take place.

If the proposed interception by your educational establishment does not fall within one of these accepted categories, then consent of all parties must be obtained prior to any interception taking place.

With regard to personal disc space, if what is being looked at is the content of private communications then the Data Protection Rules referred to before apply to searching the user's personal disc space.

Many of the same rules apply to student communications and personal disc space, however the legal relationship with the student is different than with employees and is examined in some detail elsewhere in this webcast.

Question 5 : Is it legal for IT staff to intercept or monitor communications or postings by students or staff in forums or bulletin boards?

Answer: The interception and monitoring of communications for postings by students or staff in forums or bulletin boards is regulated by the RIPA and the Lawful Business Regulations. Part 1 of the RIPA makes it an offence for a person to intentionally, and without lawful authority, intercept any communication on a private telecommunications system in the course of its transmission. Bulletin boards operated by institutions fall within the definition of a private communications network. Therefore, interception of communications made by staff or students on a bulletin board operated by an institution is illegal. However, section 3 of the Lawful Business Regulations provides some exceptions where it will be legitimate for the IT staff to intercept communications made by staff or students in a bulletin board.

As mentioned before, it permits the interception without consent to investigate or detect unauthorised use of the communication system, to prevent or detect crime, to safeguard national security or to ensure the effective operation of the system.

It is also worth noting here that every effort must be made in such situations to inform the users that monitoring and recording of their communications may be made.

The same rules apply to postings or communications made by staff or students over the institution's local area network to a private bulletin board available on the internet.

Question 6 : What is the legal position with regard to log files? The filtering software we use generates records of attempts by individual 'loggers on' to access barred websites. Is this monitoring legal?

Answer: Any comprehensive programme of logging will capture information about the activities of individual users. In some cases this has the potential to intrude on the privacy of those individuals. Users and system administrators must be clear that the primary purpose of log files is to provide a better service to legitimate users by providing computers and networks that are fit for their intended purpose and which work as reliably as possible.

Human Rights Law states that everyone has the right to respect for his private and family life, his home and his correspondence. All users and administrators are required to respect this. Most log files contain personal data so are subject to the provisions of the Data Protection Act. Users must be informed what information will be recorded and what it may be used for. Of course, there is nothing to prevent the anonymous use of the information generated by log files for the purposes of analysis or research where the information is truly anonymous.

Detailed useful information with regard to log files is available on the JANET UKERNA Website in a document called Guidance Note on Log Files at www.ja.net. Send us an email at JISC Legal if you have any difficulty locating this, or any other of the documents or information referred to. Our email address is info@jisclegal.ac.uk.

Question 7 : What is the legal position with regard to a public authority, for example the police, requesting information that is stored in a student or staff PC for purposes of law enforcement?

Answer: Part 1, Chapter 2 of RIPA empowers certain public authorities, like the police, to serve a notice in writing to a service provider requesting the disclosure of the communications data of persons for specified purposes. The police can therefore ask college or universities to disclose to them certain communications data to safeguard national security, to prevent or detect a crime or disorder in the interest of the economic well being of the UK and in the interest of public safety and for protecting public health.

Also, Section 29 (1) and (2) of the Data Protection Act which deals with crime and taxation creates an exception by which personal data that is processed for the purpose of prevention or detection of crime and for the apprehension or prosecution of offenders are exempt from the first data protection principle, dealing with fair and lawful processing of personal data.

This exemption can be applied if the police need some information to prevent or detect crime, or catch or prosecute a suspect.

It should however be kept in mind that it is up to you to decide whether to release the personal information. If you are satisfied that the information is going to be used for such purposes and that withholding the information would significantly harm any attempt by the police to prevent a crime or catch a suspect then you can disclose this information.

For more information you may read the Good Practice Note "Data Protection Good Practice Note - Releasing Information to Prevent or Detect Crime", that's published by the Information Commissioner's Office.

Question 8: What's wrong with IT staff checking that students and staff who would abuse the system are prevented from doing so? Surely we should be anticipating and preventing such abuse?

Answer: It is certainly lawful for operational staff to protect computer systems from abuse. In fact, in terms of data protection there is a positive obligation on the institution to secure the personal data of individuals from unauthorised access, misuse, or modification. It is only where the rights of an individual are infringed does the law step in and set limits in order to protect those rights.

Question 9: It says in our policy that reasonable personal use is permitted of the IT facilities? What is reasonable personal use in this context?

Answer: There is no hard and fast definition for what is recognised as reasonable and personal use of an institution's IT facilities. Reasonable personal use may vary from institution to institution. In general, use of the IT facilities of an institution would be considered reasonable if such use does not have an adverse impact on the IT resources of the institution and does not cause any damage or difficulty to the institution's computers or to its networks.

Some examples of actions that will be considered beyond the scope of reasonable personal use might include the installation of inappropriate software, use of an institution's IT facilities for private financial gain, or for any commercial purposes, and use in such a manner that it adversely affects the performance of official duties of the staff or that of any other member of staff.

Question 10: What purpose does an Acceptable Use Policy fulfil and what terms should it contain?

Answer : An Acceptable Use Policy is a document that sets out a framework of rules governing what users of an institution's computer systems and its IT network can and cannot do. Institutions need an acceptable use IT policy to ensure that users of its IT and communications systems work within a set of framework of information and security rules. This helps to ensure the safety, security, integrity and performance of an institution's IT network. It helps to minimise the liability of an institution from a potential legal action that might arise from any unauthorised use. They help to ensure compliance with the relevant law and may help to demonstrate effective and appropriate use of publicly funded resources.

The Acceptable Use Policy in its broader sense should cover what is treated as acceptable and unacceptable use of IT systems, terms relating to compliance with the policy and the sanctions that may apply in the case of non-compliance with the policy. The policy may therefore involve rules relating to the interception, monitoring and use of the IT systems and facilities. This can comprise the institution's intranet, use of the internet, emails, electronic bulletin boards, computers, and even chat or messaging software. You'll hear more about policies throughout this webcast.

Chair: Well, you've been going for an hour and we've bombarded you. It's about time for a coffee I think. Remember, get your questions in, there's still time. But for now it's a five minute break and we'll be back with more after that.

(Short break)

Chair: Welcome back, I hope you've got your coffee and you are enjoying it. Well, I'm pleased to be able to say that we've filled our server capacity in fact for this webcast, so well done for getting connected yourself. If you've got any colleagues that haven't been able to connect, well they're probably looking over your shoulder, but otherwise they can get hold of the webcast later on as a downloadable file, or indeed as a streamed version. A reminder that we appreciate your feedback in helping us improve for the future. This PlayStation Portable could be yours if you stick in the evaluation form to us after you've seen today's presentation.

Well moving on, we've had an overview, we've had monitoring, we've had intercepting communications and we've had frequently asked questions. For the rest of this afternoon's session, we're going to be looking at the practicalities of accessing network and hard drives, and what's the legal situation. We're going to look at some common scenarios, we're going to deal with your questions, and again we've got time still for you to put in a question to us using the form on the website. And then we'll be looking at a panel discussion on the wider issues.

So coming back, well William gave us an overview beforehand. He's now going to deal with the nitty-gritty of accessing network and hard drives, so it's over to William.

[Back to top](#)

6. Accessing Staff & Student Network and Hard Drives with William Malcolm

William: Thank you very much again for that introduction. Well, we're getting now to the point where some of the practical issues that you base on a day-to-day basis begin to get flushed out and there can probably be no greater example of that than a situation where a member of staff is on holiday and you need to get access to their account to continue with a piece of work. Someone leaves the organisation and you need to find copies of information that's backed up. It's alleged that a student has acted inappropriately and you need to check an email account, or you need to check an IT account to see whether that's the case, or someone from the police walks into reception area and asks for a copy of information from a student's IT account. And these are the issues that we're going to try and walk you through over the course of the next 15 minutes or so.

I've split this part of the webcast into two sections. What do you do if a third party **out with** your organisation requests information from the IT account or from the hard drive of a member of staff or a student? And then what do you do with regard to your own access and monitoring arrangements?

Turning to the access by the police and other third parties. Well, we heard in question 7 there, when we were looking just before the coffee break, that the police have powers under the Regulation of Investigatory Powers to require information of organisations. We also heard that the police have got a wide range of statutory powers under which they can require information. And that's certainly the case. But when you are faced with a question as to whether or not you should disclose information to the police or any third parties, the key provisions you should be concerned with are Sections 29 and Section 35 of the Data Protection Act. Now, within your university and college if data protection is not your area, then get a hold of the person who is responsible. Get a hold of your Data Protection Officer, get a hold of your Data Protection Manager and ask them for a view before you disclose information to the police. Don't just assume that the police are entitled to what they're asking for. It's often the case that the police are asking you to do them a favour by disclosing information. The Data Protection Act really splits up into two important sections, and what we're going to look at is the key considerations relevant to what you would do when you are asked by the police or someone else for access to information.

Well, the key issue is whether you are obliged to disclose, or whether you are being asked to volunteer to make a disclosure.

If the police are saying to you "we have statutory powers to compel you to disclose this information" or "we have a court order" then you are obliged to disclose. And in that situation you will get comfort from the Data Protection Act under Section 35 which I will talk about in a second.

If, however, the position is that you are being asked to volunteer to disclose, then you need to perform a little assessment under Section 29 of the Data Protection Act, which I will talk about in a second.

So, what do you do? You confirm the recipient's identity. Who can disclose the information within your organisation? Have you got the power or do you need to speak to someone else? What about the security relating to the disclosure? There's no point in getting all the information that the third party wants and then putting it in a bog standard envelope and posting it through the mail if that's not a secure means of the transmission. And then there's all the issues to do with whether to refuse to disclose, and what the consequences of that are.

So what do you do? A police officer walks into the building and requests information under Section 29 of the Data Protection Act. The first thing to note is that the police officer is not entitled to the information under Section 29 of the Data Protection Act. What Section 29 does is give you, as the university or college, the authority to disclose if you are satisfied that not to disclose would prejudice the prevention and detection of crime. So in essence, if a police officer asks for information, if they haven't served a court order or exercised another statutory power, such as a power under RIPA, they're asking you to do them a favour. They're asking you to help them out. And as a responsible organisation you would want to do that in most cases, but, you would want to perform that assessment to see whether the disclosure is necessary for the prevention and detection of crime. You wouldn't just make an assumption that you can make the disclosure because the police are asking for the information.

So what do you do when the police or a third party asks for information? You establish whether or not that you are required to disclose. And if you are required to disclose you are given all the comfort you need by the Data Protection Act under Section 35, which basically provides 'any disclosures required under an enactment by an order of court, or by any rule of law don't breach the Data Protection Act', so you are asked for information by a third party, what do you work out? Am I being asked to do this as a favour? Am I being asked to volunteer? In which case you look at Section 29 'Necessary for the prevention and detection of crime' - make the disclosure. Are you being asked to compel disclosure? In which case, no problem, 'here's the information, here's what you need', and you are given comfort by Section 35.

And of course remember that if you don't feel comfortable interpreting these sections or making those decisions contact your Data Protection Manager within your organisation and they will be able to help you with that assessment.

So that's the situation with respect to disclosures to third parties. But what about access to accounts on an ongoing basis? Internal access. What happens when there's just a member of staff wanting to access another member of staff's account, or you've got concerns because a student hasn't appeared in university or college for five or six days and you want to just check and see if they're okay by looking at their email account for example? What happens in these run-of-the-mill situations? Well, I think what we tried to do in the first part of today's session was spell out the importance of having a Communications Policy which tells staff and students what they can expect with respect to monitoring. So where you end up is that a member of staff's employment contract, a student's terms and conditions of use, all of the documents which staff and students are given tell them what monitoring to expect, and that expectation exists.

What I'm going to say now pre-supposes to a certain extent that your organisation has got that right. Now, if it hasn't got it right, all is not lost, but it does mean that you are going to have to give a little bit more consideration as to whether or not there are risks attached to the access in question.

So, some key concepts about access within your organisation. If you haven't already done so, appoint some authorised people, or find out who in your organisation are the people who are authorised to grant access to IT accounts or IT services. Have a closed user group of people who are appropriately trained and who understand all of the issues involved. That may be the IT department, but just because they control access to the systems doesn't necessarily mean that it has to be them. It could be anyone within the organisation, indeed anyone with the appropriate responsibility and training. And you could nominate one individual within a department. So our first top tip is, have authorised persons. Have people who are responsible for making the decision as to whether or not a disclosure should be made.

We've covered the importance of a Communications Policy, so I'm not going to dwell on that, that's the second bullet point on the slide. The next thing that I'd want to cover off is the concept of reasonable suspicion or purpose. It's not good just to say "we want to be able to access accounts". You must have a reason, and that reason could include a wide variety of things. Or, if it's because you suspect wrong-doing, you must have a reasonable suspicion of that wrong doing, and ultimately we would kind of encourage you to look at access on a case-by-case basis and say "actually what's the reason for this access and do I have a reasonable suspicion of wrong-doing?" And if you do have a reasonable suspicion of wrong-doing then the position is that you should only use the information you are gathering for the purpose you are collecting it. You don't go in there and say "well I've got this information now and I'm going to use it for 10, 20, 30 purposes". You limit what you are going in for, and the next thing is that you only access specific information. You don't just allow someone access to the whole IT account, the authorised person allows someone within your organisation to access the portion of the information that they need access to for the reason the access has been granted.

Another thing that we would encourage you to do is get consent if that is possible. So if you can't get consent then you obviously need to go to the authorised person and the authorised person will work out with you whether or not the individuals have been appropriately notified through the communications policy that such an

interception was likely. And if that's not the case they can work out the risks with you, but we would certainly encourage you to get consent if possible, and even if consent is withheld never be covert. You should always let people know if you are monitoring or intercepting communications on their network. The only situation in which you shouldn't let people know if that's the case is that to do so would tip those individuals off that a crime is being committed. So generally you would want to let people know, you want to be upfront and you would want to be open.

I'm turning to the next slide with the final two points I'd like to make, allow individual access to the material. If you are accusing someone of something, of committing a crime, breaching policy, show them what you have. You may have accessed the information lawfully, you may have accessed it in accordance with the communications policy, but ultimately, if we're about being open and transparent why shouldn't they have a copy of what you have, unless of course to pass that on would be unlawful, such as in the case of pornography, so that they can defend themselves and put their case to you. And lastly, and this is a big one, leave crime to the police. If you suspect a student or a member of staff has committed a criminal offence then don't go off on an investigation of your own without consulting the police. The police have proper powers to investigate crime. You, as an organisation, don't have those powers. So if you suspect that a crime has been committed then you should allow that investigation to be conducted by the police in an open and transparent manner.

One final point I would mention is the importance of evidence. If you access information on IT accounts then don't just, even if your access is held to be unlawful, a tribunal or a court might still render it admissible. So all is not lost. Do what you can to be open. Do what you can to be transparent, do what you can to comply with the rules, but if you access information which shows wrong-doing, then ultimately a tribunal may decide that the person's wrong doing has a higher weight than your unlawful access.

I hope that's given you a snapshot. I know you will have questions on many specific issues that you face on a daily basis, and we will look forward to chatting those through with you later on.

I'll hand back to the chair.

Chair: Thank you very much William, that's very useful. Some very practical information there. Well, next we're going to go on and we're going to look at some scenarios that typically come up, and following that there will be your questions, and thank you ever so much for those of you who have already put in questions. It allows us to deal with the real issues that matter to you and I'm pleased to say that we've received many questions and we're going to distil those down and hopefully give you the answers after the next section.

7. Scenarios with the JISC Legal team

The next section that we're going onto just now is dealing then with certain typical scenarios.

Case Study 1: A college principal has just received by email a sample of obscene materials which his IT manager says a member of staff has been downloading from the internet onto college computers. What should he do?

Answer: As with any other incident response, the first aim is to limit the damage cause by the incident. Clearly the college principal has to be very careful and one of the first difficulties is that someone has to make a decision whether the material involved is illegal or not. If it is obviously illegal, such as child pornography images, then the police should be involved as soon as possible. A local police liaison officer should be able to provide guidance on appropriate actions to take once illegal materials are discovered on college computers. The situation is also likely to be a breach of college disciplinary rules and has to be handled, as would any other breach of discipline.

Where the materials are not illegal and if the institution has a clear Acceptable Use Policy which sets the limits on what is permitted for staff use of the college information systems, and an inter-related disciplinary procedure, then the email which the college principal has received should trigger this disciplinary investigation procedure. It should be remembered that what the college is really doing is allowing individuals to use the IT facilities so long as they remain within the terms and conditions of acceptable use, which the college specifies.

Just like any other college facility, the privilege can be withdrawn if abused.

Ensuring that the Acceptable Use Policy terms and conditions are clear to all users is essential. If these procedures are not already in place at your institution, then you should take steps to get them in place as soon as possible. It is important that the Acceptable Use Policy is enforceable, otherwise the institution may be held to have treated a member of staff or a student unfairly when taking disciplinary action.

Collecting Evidence: One important question to be asked and answered though is how the IT manager has come across the materials in the first place. Was it by monitoring individuals? Was this done lawfully?

The outcome of such an investigation may in the extreme result in the dismissal of an employee and may form the basis of a subsequent action for unfair dismissal. Such action is likely too be vigorously contested. In that event there is the risk that evidence gathered by IT staff during an investigation will be held inadmissible if it were gathered in an unlawful way.

Evidence could also be discredited if presented inappropriately. The authenticity of email messages and the validity of logging records are particularly likely to be challenged. Often college and university IT departments are unaware of these issues. While they may receive guidance from the police investigating a serious crime this will not be so for minor offences or for civil actions. Consequently, there is a risk that what may seem a cast iron case will flounder when contested for example in an employment appeals hearing. IT staff are increasingly likely to be called upon to investigate and gather evidence when there is an allegation of improper conduct. This has to be carried out in compliance with the Data Protection Act, the Regulation of Investigatory Powers Act and the Human Rights Act. It is essential that staff

understand their responsibilities and the limits of their authority. Documented procedures making clear what staff are authorised to do and what they are not must be provided.

For users, every institution should have an Acceptable Use Policy. To be enforceable the Acceptable Use Policy must be properly incorporated into the student contract or into an employee terms and conditions, and additionally, reasonable steps must be taken to communicate its contents and any sanctions that might be imposed.

Case Study 2: What if the individual involved was a student rather than a member of staff?

Answer: The response by the college should be similar. The same tests will be applied to the evidence to be used. Acceptable use by students must be enforced in the same way as for members of staff.

In summary: If the college has robust transparent procedures in place to handle such incidents, then dealing with finding obscene materials on college computers should present few difficulties which cannot be managed. However, being caught without such procedures could cause the college many problems.

Further Guidance: You should refer to the document "Inappropriate Use of Computers for Technical Investigation Process", which is a document describing an investigation process agreed by the Higher Education Information Directors Scotland Members. It is available on the JISC Legal website.

Further useful guidance is available in the document "Legal Risks and Liabilities for IT Services in FE and HE" by Christine Cooper, again, on the JISC Legal website.

Chair: Well, hopefully that's given you some answers to the typical scenarios that might come up. Your questions have been coming in all afternoon. We've compiled them together, and I have with me now Betty Wilder from the JISC Legal Team along with her studio guests, Julia and William, who are going to attempt to answer some of those questions.

[Back to top](#)

8. Your Questions Answered with Betty Willder, William Malcolm and Julia Hörnle

Betty: Right, I think that we'll just head straight on with this as we have had many questions, so press straight on with number one.

Julia, maybe if you would start with this one?

Q: As a teacher I use software to watch what students are doing and sometimes to amend their work located in the student's space on the VLE. Is this acceptable?

Julia: I think one of the purposes allowed under the Lawful Business Practices Regulations is quality assurance, and that obviously applies to the college like it applies to any other organisation. So as long as students are made aware of the type of monitoring that is taking place, and the kind of monitoring is not excessive, such a type of monitoring would be justified.

Betty : Right, and following on from that, William.

Q: Next step. If they're using the internet inappropriately I would close this down on them by taking control of their computer, am I infringing any laws by doing this?

William: Well, one of the key issues is by which means did you come by the information that they were accessing inappropriate material? Most universities and colleges will monitor internet use at a system level, and monitor for inappropriate content, and then those system read-outs are flagged up for further investigation. And if that's covered in the communication policy that's entirely appropriate. So once you have that information, you obviously investigate, and yes, it may be appropriate to close off an IT account pending an investigation if, for example, pornography was being accessed and that was putting rest of the university or college at risk by having offensive or unlawful or illegal in fact material on it's servers, so it's legitimate to close it off for an investigation, but as in all things there will be a disciplinary process, the student or member of staff concerned would get to put their side of the story forward, and it could be that the IT Policy, the IT access is restored after that. But it is certainly legitimate to close down access while an investigation is being conducted and make it clear to the student or member of staff that that's what is happening.

Betty : As a follow on to that William, could they close down inappropriate emails before the students have actually sent them?

William : Well again, the key question here is how did they come by this information? Certainly the content of communications should not be intercepted without the system flagging that perhaps there is some inappropriate material there, perhaps a flesh tone detector, a piece of software to indicate that a particular attachment is perhaps of a sexual nature. You could have an attachment which is particularly large, which indicates theft of confidential information. And if that's flagged for investigation then that could be stopped by the university or college in question. But one should be aware that it's not appropriate to simply access all outgoing communications of students on the basis that they might do something wrong. There must be an appropriate monitoring policy in place which flags the issues for further investigation.

Betty: Thank you. Right, the next one Julia I think. Now, it's been suggested that staff be allowed to use personal web mail, for example G-mail, for personal email. Where do we stand if inappropriate material is circulated on this within the organisation? And as it's external we cannot monitor it, where would we stand?

Julia: I think the first point that is that it's perhaps impossible to prohibit all personal use so it is kind of important to make clear to all staff what is personal allowed use, and what sort of use is not allowed, and I think the place to state that is the Acceptable Use Policy. Just to state that certain content is inappropriate is not

enough because it's not clear as to what is inappropriate content. So the first step really is in the Use Policy to really define what is appropriate and what is inappropriate content. And that then will kind of inform staff what they can post and what they can't post.

Betty: Thank you. William, the next question is,

Q: If we were allowed to allow staff personal disc space would it be appropriate to clearly define the size limit on this, and if it's exceeded what powers would we have? Either shut it down or stop further upload?

William: Well it's entirely appropriate for a university to allow an academic or a student space for personal material. It's also appropriate that that is monitored at a system level in line with the established Communications Policy. Obviously there wouldn't be any routine access to that portion of the disc space without an exception report being sent back, but whilst university staff, and university students may have a legitimate expectation to use their email or actually equipment for personal use, they really shouldn't have an expectation that they get to clog up the server with say I-tunes or MP3 tracks or particularly large graphic files. It's perfectly legitimate for a university to give a limit and simply to notify a student or member of staff that if that limit is exceeded then they will have X number of days to delete the content, or a portion will be deleted for them. I think that's entirely legitimate. You will allow some personal use. If people want more space they should buy their own PC.

Betty: Thank you. The next one. I'll just leave this one open.

Q : We have regulations for use of our IT services which are published on our website, which again is what you've been saying both of you that each organisation should have. This states that email is regarded as confidential and no one will look at it unless we are investigating misuse. In that case we will tell the user that we are doing so. Does that therefore make it illegal for someone to look at another person's email if that person is, for example, off sick?

William: I can certainly happily take that if you wish. Basically again there are technical processes in most software packages now, particularly Outlook, where people can set up effectively user groups to allow for access when people are off sick, so it would be clear to members of staff that that was going to happen. Now, obviously that's the cart before the horse, so to avoid the problem do it now. But in the event that you haven't avoided the problem and you end up in this situation, then my view would be that it is legitimate to access things on an individual's IT account which are work-related, taking care not to access personal material, taking care not to access any material which is marked 'personal' and again checking that such access is communicated to staff in the Authorised Use Policy.

Betty: So what you are saying is tell the staff in advance what the expectation is in these situations?

William : Yes, and if you haven't done that, whilst someone wouldn't want to trouble someone if they were particularly ill, you could always phone them on their mobile and ask "do you mind if I access your account?" apart from the fact that that gives

you consent, you know, a little cooperation and a little kind of sensitivity to someone's personal space goes a long way in resolving any practical difficulties.

Julia: I think just to add really, which goes along the same tune is that it all depends on the legitimate expectations of privacy and also on necessity. So, if the person has still access to his or her emails or he or she can be contacted very easily, then it may be difficult to argue that there is a real necessity to look at their email and so I think it depends on the circumstances unfortunately.

William: That's an excellent point.

Betty: Thank you very much. That in fact for the viewers that was the most prevalent question today, was accessing email in an employee's absence.

Finally, email archiving. Again, I will leave this one open so fire away.

Q: How does email archiving of all business emails relate to monitoring? Is it classed as monitoring only if the archive is examined by a person based on a legitimate reasonable concern, or is making the archive itself that is classed as monitoring?

Julia: I think probably it's just literally making a copy without identifying the recipient or the sender or any type of data is probably not monitoring. However, if the archiving process was some kind of checking of content, even if that's done on an automated basis, then I think it might well fall within the ambit of monitoring, but then that monitoring might not be unlawful.

William: Yes, just very quickly to add to that. Of course any retention of personal information in that way subject to the Data Protection Act, it must be fair and lawful and you can't keep it for longer than you need it for your legitimate purpose. So the question is not so much whether it's monitoring, but is it personal data? And if it is, it's subject to the eight Data Protection Principles in the same way that all personal data is.

Betty : Thank you. Now, next one.

Q: Would it be fair to say that if a public authority allows the private non-business related use of a system then monitoring cannot take place?

Again, this is to reinforce what you've already said, but, again, a question for William?

William: Again, you cannot monitor or effectively access or intercept private communications, but it's always appropriate to monitor at a system level, i.e. against a defined set of rules in line with the Communications Policy to check against misuse. So, don't access the content, but by all means have a set of rules that are applied from an IT standpoint, so you can check on appropriate use and behaviour.

Julia: I guess the question, because it refers to a public authority, must have the Human Rights Act in mind?

William : Absolutely.

Julia : But clearly obviously under Article 8 of the European Convention, monitoring can be justified, so the sort of proportionality test applies nevertheless.

Betty : Right, thank you, and quite a technical one here, or it is for me anyway, so here goes (laughs).

Q: We are considering using a centralised audit trail database and enquiry system which will contain one or two months-worth of security gate information, network log-in etc., and PCs used, potentially websites visited, so that the university secretary can respond to police enquiries without recourse to the IT technicians to investigate. The concern from the IT technicians is that they might be the ones who have to give evidence in enquiries, and potentially go to court. Is this a legally acceptable solution to this aspect of monitoring for police, external access purposes?

William : I'm happy to start off if you wish. I think there is a number of questions contained in that problem. It's for the university to frame the appropriate management policy with respect to who accesses the communications. Clearly if you have software that retains all information you have to check that that's appropriate in terms of the principles in the Data Protection Act. Are you retaining it for longer than you need it for your business purpose? And you also have to be aware that you are potentially retaining quite a lot of information that may become accessible under the Freedom of Information Act, so in an attempt to help the police you may be shooting yourself in the foot somewhat by opening yourself up to foyer requests. But ultimately it's for the university to set the appropriate governance structure, and if that is that the university Chancellor or Principal or whoever has those access rights, then that's a matter for the university. Will the IT staff have to go to court? Well, they may well have to do, but unfortunately that's just the nature of the beast (laughs).

Julia: Yes I don't have anything to add really.

Betty: And finally, the next question was in fact on deceased persons.

Q: Can we, if we are in the unfortunate situation where one of our students has died, can we access his email account in those circumstances? Thinking of data protection.

Julia: Well, the first easy bit of the answer is that personal data has to refer to a living person, so the Data Protection Act wouldn't apply. As to Article 8 of the Human Rights Commission, I think that still applies, but I'm not 100% sure, I must admit.

William: Of course data on the dead remains confidential and remains effective. Confidentiality doesn't die with death although the protection afforded in the Data Protection Act do. I'm not sure about the convention point. I'd need to check. But I think that on a kind of practical level don't forget that all the rules we've been talking about, about network monitoring apply to networks and not to people, so you've got to kind of bear in mind that those still apply. I think that provided that you handle it practically and sensitively you shouldn't come across too many issues.

Betty: And I think we're perhaps getting towards the final question here.

Q: What will happen to an institution if they monitor their students or their staff illegally and they get caught doing so or the student or the member of staff raises a stink on this, what happens?

Julia: Well again there are obvious various pieces of legislation applicable and it depends a little under which piece of legislation we are sort of looking at enforcement action. The Information Commissioner might actually take enforcement under the Data Protection Act. The Data Protection Act provides for civil compensation and also some criminal liability, and obviously the Regulation of Investigatory Powers Act also provides for civil and criminal liability. Having said that, criminal liability does not apply if it is within the control of a private network.

William: Yes, I go along with that. The big risk is that if it's on a public network, it's deemed to be a public network, and you end up in a position where your interception amounts to a criminal offence. That would be a bit problem for you and for senior university staff. So that's the nightmare scenario. And going along with that you've got data protection issues, the individual can sue you under the Data Protection Act if your unlawful activity gave rise to a loss, if they can demonstrate that loss was linked to the breach in court they can sue you for damages, and more people are doing that. And ultimately you've got the one thing in all this that no one wants which is bad PR, bad publicity, and having to explain to a senior member of your organisation why it happened and why there's not a policy in place.

Betty : I think that I'm afraid it's all that we have time for in this section. We have had many more questions, but unfortunately we can't at this stage get through them all. Thank you both very much.

William : Thanks for you questions.

[Back to top](#)

9. Panel Discussion - with Jason Campbell, William Malcolm and Julia Hörnle

Chair: Thank you very much Betty. Thank you William and Julia. We're going to round up with me taking Betty's seat here and giving a few general questions which haven't yet been answered. If you've got a question, a specific question that hasn't been answered so far then please do feel free to use our enquiry service. Information is available on our website www.jisclegal.ac.uk. And so to finish off then I'm going to request Betty with the panel and we're going to deal with some general questions. I don't know if you've been able to hear the noise of the Spanish celebrations that are going on in George Square just down the road as we go on, but hopefully you've enjoyed some background music. Incidental music, for copyright purposes I hasten to add.

Just to finish off, just some general questions. First of all, should staff and students be treated differently? Talking about the legal situation.

William: To be honest it's one of these questions that inevitably they will be treated differently, but does the legal regime that applies to both of them in term of data protection and networks differ greatly? Not particularly. You know, the same law applies but there might be some differences in treatment. One which springs to mind is that staff have terms and conditions of employment, whereas students have a contract with the university for education services. So perhaps the terms and conditions that are put into the respective contracts vis a vis monitoring and use, might be slightly different. But the law is the same the impact may be slightly different. But by and large I think it's sensible to approach staff as you would approach students and vice versa.

Chair: Right thank you. Is there any difference between read and unread emails in terms of monitoring and interception?

Julia: If the question refers to the type of data you discover between read and unread data I could see a difference there, but I think in principle there is probably no difference in the way you treat the application of the law to that data.

Chair: Thank you. There may be certain circumstances where an institution would wish to engage in covert surveillance and obviously this is going to be controversial, so situations like contentious situations, if someone's suspected of stealing for example, or engaging in fraud, or something along those lines. Could you clarify what sort of circumstances is it legal to conduct covert surveillance?

William : I take it that, I know that some people differ on their point of view on this. I take a fairly strict view, as I said during one of my presentations earlier. I think that investigation of crime is a matter for the police. If you have reasonable cause to suspect criminal activity it is not your role, as a university, to go off on a covert investigation of your own. Your role is as a responsible public authority inform the police and have them conduct a lawful responsible investigation, and my very strong advice is leave it to the experts. If you don't have enough to point the finger or you are not sure about calling the police, then perhaps a little bit of monitoring in line with the Communications Police to establish a probable cause or fact for contacting the police is permissible, but I just wouldn't go into the territory of conducting your own investigation into a crime.

Julia : I kind of agree that covert monitoring should only be carried out in very, very, exceptional circumstances and certainly there has to be some very concrete moment of suspicion, either concerning illegal activities, but perhaps more difficult if there is a claim say for sexual harassment. In those circumstances, I think it might be more difficult to draw the line when covert monitoring is allowed, because clearly if there is an harassment claim the university might, or the college might be liable under employment law as well, so I think it's slightly wider perhaps than just illegal activities, but I think there has to be a concrete suspicion of serious misconduct or criminal activity.

Chair: Okay thank you. I think with all the institutions have on their plate there's always a temptation to think 'well just tell all staff and students that they may use the facilities for nothing but the institution's purposes for their studies, or research, or

their administration'. What legal status would that have and would that change this at all?

Julia: I think two points come to mind. First of all there is sometimes a blurred line between what our private and what our work purpose is. So for example, especially in the area of research where I think sometimes research requires a sort of wider attitude, and what you actually find you use in research etc, you might not use all the stuff for example your access on the internet. So I think that's a blurred line, or, you know, if I update myself on the news every morning, is that my private use or is that the background information on which I conduct my legal research? So there is a blurring between the private and the work use, or the student use.

The other issue here is I think that it is fairly clear from the case law of the European Court of Human Rights that even in a workplace scenario, there is a core or privacy expected and you can't destroy that legitimate expectations of employees even at the workplace. So simply saying 'you are not allowed to use e-communications for private uses' unfortunately will not do the trick.

Chair: Okay thank you very much there. Let's say an institution as well wants to simplify matters by adopting a policy that says in as many words 'We can monitor anything, we can intercept anything on our network', is that going to hold under the law?

William: I don't think that you will be surprised to hear that the answer to that question is no. We talked earlier about the importance of purpose. Purpose is all important when you look at the Data Protection Act. Why am I doing something? And it's important that you've gone through that privacy impact assessment that we talked about earlier. Worked out why you are doing something, what the impact on the individual is and worked out how the information will be used. And it's impossible to see how you could have done that properly or sufficiently if you just say 'we'll monitor everything and anything' I think you run a serious risk that your collection of information is in breach of the Data Protection Act, particularly the first principle of the Data Protection Act and that you are requiring that you are collecting information which is effectively far beyond what you need for your legitimate purpose. So I think such a move would be pretty dangerous.

Chair: Well, thank you very much. I think that brings us to the point that in the next few weeks we're going to be unveiling our model policy on this subject, and hopefully that will help you. If you haven't already got a policy on this maybe it's time to re-visit your institution's policy to make sure that you have a reasonable and sensible and legal policy in place. This also maybe time to look at the procedures to make sure that IT staff that are asked to look into people's IT accounts understand the duties, the Data Protection duties that are involved in the privacy respect that's required by law, in order to have the confidence that's what's going on is right.

Well, it comes to me to wind up. First of all could I say a big thank you to our guests in the studio, William from Pinsent Masons and Julia from the Centre for Commercial Legal Studies. Hopefully they've answered your questions there, and please do continue to ask questions via our website.

Could I say a big thank you to all the audio-visual staff and technical staff here at the University of Strathclyde to make this sort of event possible. It's been fairly easy for us and allowed us just to concentrate on the law. May I also say a big thanks to the rest of the JISC Legal Team for putting this all together, and especially to John Kelly who has been the one responsible for putting it all into place. I will remind you that the evaluation form is available. We value what you think, whether it's good or bad, and unfortunately JISC Legal staff are not eligible for winning this Play Station Portable, so it's going to be one of you if you are from the UK further or higher education sectors. So please do put in your form, your evaluation form. Click on the button below this, or go back to the webcast front page and you will find the evaluation form there. Let us know, and we will let you know who wins the Play Station Portable.

With that, that ends our one and three quarter hours that we've had on this subject. We hope that we've informed you somewhat and made you aware of the various issues that are involved and gave you some practical contextual information that you can use at your institution. If you have any further suggestions for work that JISC Legal can do to help you, please do get in touch with us.

With that, and with the Spanish fans still going in the background, I'll say goodbye.

[Back to top](#)

Ends

22 June 2007