Title: Authorisations procedure and guidance document for requests made under the University's Investigation of Computer Use Policy
Version: 1.1
Date: August 2015

1. Introduction

Authorising access to the personal data of a University member of staff or student without their consent must always involve a consideration of the privacy implications for the individual concerned and any third party who might also be identifiable. Decisions taken must consider whether the request is fair and proportionate in relation to the individual, taking into account the wider aims of the request.

The University's Investigation of Computer Use Policy outlines the circumstances in which it is permissible for the University to access the IT accounts, communications and other data of its members. The policy states:

"Decisions to access the IT accounts, communications and other data of members will be taken by an independent person in order to ensure that such requests are free of bias and are not malicious. Investigations of this kind are sensitive and time-consuming. Decisions to undertake such investigations will therefore be made at an appropriately senior level by a member of the University Secretary's Office who will also determine the scale of the work to be undertaken."

The Director of Legal Services will usually consider such requests and this document is intended to set out the procedure and some of the issues that should be taken into account when assessing a request.

2. Scope

This procedure covers requests for authorisation in relation to the following types of information:

- Emails and mailstores
- Electronic filestores
- Telephone usage
- Telephone call recording
- UCard access logs
- CCTV images
- Covert CCTV installation
- Contact directory opt outs
- Out of office messages
- External requests

As technology continues to evolve, there are likely to be further additions to those types of information listed above.

3. Compliance

In considering whether to authorise such requests, the following pieces of legislation must be considered and complied with:

- Data Protection Act
- Human Rights Act
- Regulation of Investigatory Powers Act (RIPA)
- Lawful Business Practice Regulations

4. Procedure

Such requests will usually be received by either IT Services or Security Services who control the systems containing such information. Members of staff receiving such requests must be aware of this procedure and must have authorisation from the Secretary's Office prior to taking any action that could have an impact upon the privacy of members of staff or students. Requests should be forwarded to the Information Rights Officer (email: data-protection@bristol.ac.uk) in the first instance who will ensure there is enough information contained in the request to allow the Director of Legal Services to make an informed decision.

If authorisation is granted, that authorisation will remain valid for ten working days from the date of authorisation. After that period, a separate request for authorisation must be made.

5. Notification to individuals

In the interests of transparency and natural justice, when authorising a request it should be considered whether the individual(s) concerned should be notified of the access. This should take into account fairness to the individual weighted against any potential prejudice that could be caused to an ongoing investigation. Snapshots can be taken of mailstores and filestores, therefore preserving any evidence prior to a search being undertaken. Protection of whistleblowers must also be considered.

6. Emails and mailstores

The University does allow some personal use of email, so any authorisation to access emails must be careful not to unnecessarily impinge on individuals' privacy rights.

Requests for access to emails or mailstores are usually made for one of two reasons:

- Internal investigations; or
- Business continuity

In the case of an internal investigation, it must be determined that there is a genuine reason to believe that there may be information held within an email account that is pertinent to the investigation and that the request is not a "fishing" expedition. This could be information that provides evidence of an individual's guilt or innocence in relation to a particular matter. If a search is to be authorised, the parameters must be as narrow as possible (including timescale, to/from addresses and search terms) to ensure the user's privacy is protected as far as possible. Any relevant

emails retrieved must be treated as “strictly confidential” and access limited to only those individuals who have a genuine need to see them.

There may be a need to authorise such a request for business continuity where a member of staff is away from the University for a prolonged period at short notice. It is always preferable that access be granted with the knowledge and consent of the individual, where possible. Gmail only allows ‘all or nothing’ access to email accounts, which makes it difficult to ensure staff privacy can be protected when considering allowing access. If specific emails are required, a search may need to be conducted by IT Services.

7. Electronic filestores

Such requests are likely to be for business continuity purposes and scope should be narrowed as far as possible to be able to locate specific documents

- Can specific filenames be identified?
- If not, search terms or file formats?

Usual procedure is that a member of zonal IT Services staff will accompany a member of school/divisional staff to attempt to locate files, ensuring there is no undue invasion of privacy i.e. not accessing any folders or files that are clearly personal.

8. Telephone usage

Unusually high telephone bills may cause concern about excessive use or misuse of telephone services (whether landline or mobile) provided by the University. Authorising the interrogation of an itemised bill may be appropriate in such circumstances, for the relevant time period.

9. Telephone call recording

Given that recording of telephone conversations will constitute “monitoring”, there must be a legitimate reason to authorise the recording of telephone calls, in line with the Lawful Business Practice Regulations. In most circumstances, callers should be notified that their calls will be recorded and the purposes for which the recordings might be used.

10. UCard access logs

UCard access logs show when members of staff (and students) enter and sometimes exit University buildings. These logs may be of use when investigating misconduct or an incident that has occurred in a University building. The University has a duty of care to its staff under health and safety legislation and UCard logs may also be used to ensure lone working procedures are being adhered to, as allowed for in the UCard Privacy Policy.

11. CCTV images

Authorisation may be required to allow access to CCTV images for the investigation of alleged misconduct or criminal activity. CCTV images may also be used to “establish the existence of facts relevant to the business of the University” – this might include evidence in relation to an insurance claim, for example. This also covers the installation of any standalone cameras, separate from

Security managed CCTV cameras, where a CCTV Impact Assessment Form (available from Secretary's Office) must be signed off by the Director of Legal Services.

12. Covert CCTV installation

Covert CCTV cameras can cause a high level of intrusion of privacy to individuals so the authorisation of their use must be considered very carefully and there must be sufficient grounds for their use – it will usually be in relation to suspected criminal activity or serious misconduct. The CCTV Impact Assessment Form (referred to in the CCTV Code of Practice) must be completed and signed off by the Director of Legal Services prior to installation. Any such authorisation must only be for a limited time period and subject to regular review.

13. Contact directory opt outs

Staff contact details are "public" under the University's data classifications and are available via the staff contact directory. If a member of staff wishes to opt out of the contact directory, they must make a request to the University Secretary (decision may be delegated) setting out why they do not want their contact details publicly available. The Director of Legal Services can then make a decision as to whether the reason put forward is legitimate.

14. Out of office messages

Such messages should be activated by members of staff where possible. In cases where this is not possible (e.g. due to sudden staff illness or death), an appropriate message must be authorised by the Secretary's Office. This includes modifications to existing out of office messages, for example amending the content or extending the period.

15. External requests

Any such requests received from external agencies (such as the police or security bodies) should be forwarded on to the Secretary's Office to ensure they are dealt with in accordance with the law.

For requests that relate to a criminal investigation, the University must receive a section 29 Data Protection form prior to disclosure. There may be "blue light" circumstances where information is required urgently and delay would prejudice an investigation or put individuals at risk. In such circumstances, a section 29 form must be obtained retrospectively.

Any RIPA notices received should be directed to the Secretary's Office for advice.