Sheffield Hallam University

Monitoring Policy

Issuing Authority	Governance and Planning Services
Effective from	1 October 2015
Planned Review Date	1 June 2017
Version	V 2015.2
Enquiries to	Helen Williamson, Information Governance Officer Governance and Planning Services, SRD ☎3361 Email: h.williamson@shu.ac.uk or foi@shu.ac.uk

Monitoring Policy

Purpose of the policy

The Data Protection Act 1998 does not prohibit monitoring, but any monitoring of staff or students needs to be carried out in accordance with the Act. Since monitoring has the capacity to intrude or interfere in the private lives of individuals, it must be justified. Monitoring is recognised as sometimes being a necessary part of the employment relationship. Monitoring is also a necessary part of crime or fraud detection and ensuring that the University estate, facilities, telecommunications and IT systems are used appropriately. Any benefits to the University of monitoring staff or students must be weighed up against any possible adverse impact on them.

This policy sets out the University's approach to monitoring staff and students, the responsibilities of managers with respect to that monitoring and the individual rights of staff and students.

Core principles

- Staff and students have legitimate expectations of reasonable privacy within the University
- Intrusion into the private lives of staff or students is not normally justified unless the University is at risk
- The University should have a clear idea of the benefits that monitoring will bring and must be able to justify these against any adverse impact on staff or students
- Staff and students need to be made aware of the nature, extent and reasons for any monitoring which is likely to take place
- Staff and students are expected to abide by the current policies and procedures in place and take responsibility for their own conduct
- Specific monitoring may be carried out in line with statutory requirements, eg monitoring of the Joint Academic Network IT system (JANET).

Definitions

Monitoring
Activity which sets out to 'collect information about staff or students by keeping them under some form of observation' and 'goes beyond one individual simply watching another and involves the manual recording or any automated processing of personal information'.

Systematic monitoring
Where all staff or students, or groups of staff or students are monitored as a matter of routine. An example might be to establish patterns of use or demand for a service. This may or may not identify individuals.

Occasional monitoring
Short term measure in response to a particular problem or need. This does not include occasional access to records which contain information on individuals but which were not collected primarily to keep a watch on their performance or conduct.

Covert monitoring
Monitoring which is 'carried out in a manner calculated to ensure those subject to it are unaware it is taking place'.

What is not covered by this policy

- Audit – auditors monitor systems rather than individuals
- Equal opportunities monitoring.

This is not an exhaustive list.

Authority for monitoring

Unauthorised monitoring is not permitted. Attempts by any member of staff to implement unauthorised monitoring will be in breach of this policy and may result in disciplinary action. The following is a list of those members of staff, in addition to the Vice Chancellor, who may authorise monitoring, together with their areas of responsibility

- Director of Human Resources – any matters relating to staff
- University Secretary – any matters relating to students
- Head of Security – any security matters, eg CCTV
- Director of Finance – any financial matters, eg suspected fraud
- Chief Information Officer – any IT matters, eg Internet and e-mail use
- Director of Estates and Facilities – any matters relating to the use of the University estate and its facilities, including telecommunications systems

They may also designate a nominee to authorise monitoring.

What may be monitored and why?

Some examples of monitoring activity are

- Routine use of CCTV to check that health and safety rules are being complied with or to assist in the prevention of crime eg theft
- Keeping recordings of telephone calls that come into the University for training purposes or for dealing with complaints
- Examining website logs to ensure that staff or students are not visiting inappropriate sites
- Randomly checking or using software to check if staff or students are sending or receiving inappropriate e-mails
- Checking telephone logs to detect misuse of telecommunications
- Checking for SPAM e-mails

- Examining the contents of computer hard disks to check for any unlicensed software or to see if updates are needed.

This is not an exhaustive list. See supporting documentation for examples of some of the types of monitoring conducted in the University, its purpose, how it is carried out, on whose authority and who it affects. Sometimes, monitoring may be carried out, but the data collected is only viewed retrospectively to investigate an incident.

How monitoring information will be used

Any monitoring information that is collected in relation to a student or member of staff may be used in a disciplinary investigation, for example where there is inappropriate use of the internet or e-mail. Monitoring information may be used for training purposes, for example telephone training. Information collected may also be passed to relevant authorities if there are any criminal proceedings to which it relates. It will also be used to plan and deliver IT and telecommunications services.

Impact assessments

The Monitoring at Work Code (see section 15) suggests that in all but the most minor cases, an 'impact assessment' is carried out to decide if and how to use monitoring. This involves measuring the benefits monitoring may bring, any adverse impact on individuals, whether comparable benefits can be obtained with a lesser impact, and the techniques available for carrying out monitoring. A decision will be made as to whether the monitoring is a proportionate response to the problem it seeks to address.

Criteria for decision to monitor

The consequences of monitoring must be considered in terms of any potentially adverse impact on staff or students

- What intrusion will there be into the private lives of staff or students, eg interference with their private telephone calls or e-mails
- To what extent will staff or students be aware that they are being monitored
- What impact, if any, will there be on the relationship of mutual trust and confidence between the staff or students and the University.
- What impact will there be on relationships with unions
- Whether information that is confidential will be seen by those who do not have a legitimate business need to know.

Alternatives to monitoring should be considered

- Can established or new methods of supervision, training or clear communication deliver acceptable results
- Can investigations be carried out on specific incidents, rather than monitoring continually

- Can monitoring be limited to those staff or students about whom complaints have been received or who may be suspected of wrong doing
- Can monitoring be automated
- Can high risk areas be targeted
- Can audits or spot checks be carried out instead

The decision as to whether the current or proposed method of monitoring is justified involves

- Establishing the benefits of the method of monitoring
- Considering any alternative method of monitoring
- Weighing benefits against adverse impact
- Ensuring that any intrusion is no more than absolutely necessary
- Taking into account the results of consultation with staff or students or their representatives, eg trade unions, student union.

Retention of information

- Impact assessment documentation should be kept for six years after the monitoring has ended.
- Personal data collected during the monitoring process should only be retained for as long as is necessary to fulfil the purposes of monitoring set out in the impact assessment.
- Personal data collected for monitoring purposes should be kept securely and destroyed once it is no longer needed, in accordance with the University's document retention schedule

Security of information

Personal data collected in the course of monitoring activities will be processed fairly and lawfully in accordance with the Data Protection Act 1998, eg it will be:

- adequate, relevant and not excessive
- used for the purpose(s) stated in the impact assessment only and not used for any other purposes
- accessible only to appropriate staff on a need to know basis - this will be decided by the designated authority in question
- treated confidentially
- stored securely
- not kept for longer than necessary and will be securely destroyed once the issue(s) in question have been resolved.

Informing staff and students of monitoring activities

Staff and students are notified of the nature of any monitoring that is taking place. Relevant policies in relation to monitoring are available via the intranet, from your manager or Faculty office, or from the University Secretary's office or the Human Resources Directorate.

If any changes are made in regard to monitoring, staff and students will be notified. The exception to this is covert monitoring activity, eg for crime detection, which is allowed for by the Regulation of Investigatory Powers Act 2000 and successor legislation.

Managers with responsibility for authorising monitoring are required to record the authorisation with reasons. An annual report on the policy, while not revealing personal details, will be published outlining the nature and extent of the monitoring that has taken place during the year.

Individual rights

The Data Protection Act 1998 confers on individuals various rights including the right to find out what information a Data Controller holds about them – the right of subject access. Personal data collected or kept by the University for the purposes of monitoring will be made available if a subject access request is made, unless an exemption applies.

Information can also be obtained from the Information Commissioner's Office which enforces the Data Protection Act https://ico.org.uk/.

Further Guidance for Staff

Data Protection
IT Regulations
Anti-Corruption Policy

Relevant Legislation, Codes and Regulations

- Data Protection Act 1998 sets out the responsibilities of organisations processing personal data and the rights of individuals with respect to the use of their personal data.
- Employment Practices Data Protection Code Part 3: Monitoring at Work sets out good practice with regard to monitoring of staff.
- Regulation of Investigatory Powers Act 2000 sets out the circumstances in which communications can lawfully be intercepted without consent, eg investigating or detecting unauthorised use of a communications system, preventing or detecting crime, ensuring the effective operation of the system.
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 sets out the circumstances in which telecommunications can be lawfully monitored.
- Human Rights Act 1998 confers on all individuals a number of fundamental rights and freedoms, including 'the right to respect for private and family life, home and correspondence' (Article 8).

Supporting Documentation for the University Monitoring Policy

Examples of some of the types of monitoring conducted in the University, its purpose, how it is carried out, on whose authority and who it affects.

Category of monitoring	Type of monitoring	Purpose	By whom	Affecting whom	On whose authority
Occasional/ covert (signage alerts people to CCTV use)	CCTV	Prevention of crime	Security	Cameras are directed at areas rather than at individuals, but may be focused on individuals where there is suspicious behaviour. May include staff, students, visitors, contractors, members of the public.	Head of Security
Occasional/covert	Observations by security staff in the University	Prevention of crime (especially theft)	Security	Observations are general, but may include staff, students, visitors, contractors, members of the public.	Head of Security
Occasional/covert	Monitoring of compliance with financial regulations and procedures	Anti-fraud	Finance	Any member of staff, team of staff, student or group of students suspected of possible fraud	Director of Finance
Occasional	Telephones	Staff training purposes	Telecoms	Any member of staff. Used for training purposes.	Director of Estates and Facilities
Occasional	Telephones	Prevention of crime and telephone misuse	Telecoms	Any member of staff. There is also the facility to record abusive or threatening phone calls that come through the switchboard.	Director of Estates and Facilities
Occasional	Telephones including	Budgetary purposes and prevention of	Telecoms	Any member of staff with a telephone extension or using a	Director of Estates and

	mobiles	misuse		University mobile phone.	Facilities
Occasional	IT use	Prevention of crime and IT misuse	CIS	Monitoring of staff or students may be carried out if misuse of IT or criminal activity is suspected. Internet sites may be blocked by JANET.	Chief Information Officer

Issuing Authority: University Secretariat Version 1 - December 2004

Reviewed and re-issued 1/10/2015