UNIVERSITY OF SURREY

Monitoring Procedure	
Enabling Policy Statement; Executive Owner; Approval Route:	Our Data - Chief Operating Officer - Compliance Committee
Is the Procedure for internal use only (Non-disclosable)?	Disclosable
Associated Policy Statements:	Our Colleagues - Chief People Officer Our Students - Chief Student Officer
Authorised Owner:	University Secretary and General Counsel
Authorised Co-ordinator:	Data Protection Officer
Effective date:	01/08/2023
Due date for full review:	3 years
Sub documentation:	N/A

Approval History

Version	Reason for review	Approval Route	Date
1.0	Migration under POPP	Compliance (data) Committee	01/08/2023

1. Purpose

1.1. This Procedure is in place to help protect the University's data assets against internal, external, deliberate or accidental threats and vulnerabilities. This Procedure will assist in achieving the following objectives of the Our Data Policy Statement:

- Reduce the risk of data leakage by negligence or human error;
- Ensure confidentiality, integrity and availability of our data;
- Reduce the risk of security incidents including those involving third parties; and
- Reduce the likelihood of a personal data breach that will affect our stakeholders.

1.2. The University respects the privacy of its staff and students and acknowledges that the private lives of individuals overlap with their working lives. For example, the personal use of University email accounts and the Internet at work is permitted provided it does not interfere with the proper performance of a staff member's duties.

1.3. The University also acknowledges that the filtering of access to certain websites is necessary to protect the University and its staff and students from the risk of harm or legal action that might arise from accessing certain sites. This Procedure sets out the governance of filtering arrangements to ensure that those with a legitimate need to research external websites that would normally be blocked, have a mechanism to do so.

1.4. All forms of monitoring will be justified and undertaken in a controlled and proportionate manner. This Procedure sets out the controls and rules to be followed for those undertaking any monitoring to ensure that the privacy of all users is appropriately protected and to protect the interests of staff engaged in monitoring who may discover activities amounting to misconduct so serious that they cannot reasonably be expected to ignore it.

1.5. This Procedure aims to set expectations for users on the degree of privacy they can expect when using University issued IT systems and equipment. This Procedure does not include rules or guidance on the use of University issued IT equipment or required standards of staff conduct. For guidance on the use of University issued IT equipment staff and students should review the IT Acceptable Use Procedure. For guidance on the required standards of staff conduct, staff should refer to the Employee Handbook.

1.6. This Procedure supports the Our Colleagues and Our Students Policy Statements by ensuring robust systems and controls are in place to ensure staff and student data is kept confidential and secure.

2. Scope and Exceptions to the Procedure

2.1. This Procedure applies to all users of University IT facilities, equipment, networks and systems (together referred to as "IT Systems"). This includes staff, students and others who are given access to University IT Systems.

2.2. This Procedure applies to the use of University IT Systems irrespective of whether the access is via a University owned and provided device or via any other device.

2.3. This Procedure applies to:

- Automated Monitoring (of all activity)
- Targeted Monitoring (of specific users)
- Filtering (of specific sites and categories of site identified as potentially harmful, for all users)

2.4. This Procedure permits the use of scanning software to monitor system events and user behaviour for the purpose of investigating information security incidents. As a consequence, staff in IT Services who manage monitoring and logging platforms will necessarily require access to information about individual user behaviour.

2.5. The University will normally co-operate with a lawful request to help law enforcement agencies investigate crime.

2.6. No exceptions to this Procedure are envisaged.

3. Definitions and Terminology

3.1. **Automated Monitoring** – monitoring undertaken to identify system events or anomalies that might help identify, prevent or mitigate cyber-attacks and other threats to the University's IT Systems and data.

3.2. **CIDO –** the University's Chief Information and Digital Officer or equivalent role.

3.3. **DPO** – the University's Data Protection Officer or equivalent role.

3.4. **Filtering** – the selective disabling of access to external websites.

3.5. **IT Systems** – all University IT facilities, equipment, networks and systems.

3.6. **Profiling** – any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviours, location or movements.

3.7. **SIRO** – the University's Senior Information Risk Owner or equivalent role.

3.8. **Targeted Monitoring** – monitoring aimed at a specific user(s) to investigate conduct that may breach University policies or the law or for other legitimate reasons.

3.9. **Users** – staff, students and others who are given access to University IT Systems.

4. Procedural Principles

4.1. The CIDO is responsible for ensuring that any Automated Monitoring using technical measures is undertaken in compliance with this Procedure.

4.2. The DPO (or Deputy DPO in their absence) and a member of Executive Board, or their nominees, are responsible for authorising any Targeted Monitoring within the scope of this Procedure.

4.3. The CIDO is responsible for authorising the categories of websites to be blocked as part of the University's filtering arrangements.

4.4. The CIDO is responsible for reporting annually to Compliance (Data) Committee on all Automated Monitoring and filtering categories implemented by IT Services.

4.5. Compliance (Data) Committee is responsible for approving the categories of filtered websites under the filtering provisions of this Procedure and for approving any type of Automated Monitoring.

4.6. All users should be aware that their use of University IT Systems is monitored. This monitoring may be automated or targeted.

Automated Monitoring

4.7. The University may undertake Automated Monitoring for either of the following purposes:

- The effective and efficient planning and operation of IT facilities and capacity planning.
- The detection, mitigation and prevention of threats to information security.

4.8. Automated Monitoring is carried out in relation to IT Systems activity and behaviour. It is not carried out on individuals themselves.

4.9. Where Automated Monitoring reveals activity which the University cannot reasonably be expected to ignore, the matter will be referred to the Head of Information Security and SIRO (who may consult with the DPO) who will decide whether the matter should be shared with law enforcement agencies or whether authorisation for Targeted Monitoring should be obtained.

4.10. Where additional Automated Monitoring is required in order to adhere to evolving formal compliance frameworks (e.g. PCI DSS Payment Card Industry Security Standard) or other contractual terms of service, these will be reviewed and approved by the Compliance (Data) Committee to ensure consistency with these procedural principles.

Targeted Monitoring

4.11. Targeted Monitoring may be undertaken if unusual and/or criminal activity, which the University cannot reasonably be expected to ignore, is detected as a consequence of Automated Monitoring. If a user is alleged to have engaged in any criminal activity, the University may report them to the police who will determine the nature and scope of any subsequent investigation.

4.12. Targeted Monitoring of IT Systems issued to, and used by, users will only be undertaken to the extent permitted by or as required by law and as necessary or justifiable for legitimate business reasons. Any Targeted Monitoring will be proportionate and reasonable steps will be taken to protect users' private lives.

4.13. The following are non-exhaustive examples of legitimate business reasons:

- Detection and prevention of infringement of this Procedure and other policies and regulations.
- Investigation of alleged misconduct.
- Handling email and other electronic communications during an employee's extended absence or following an employee's departure from the University where there is a business need.
- To find lost messages or to retrieve messages lost due to computer failure.

Profiling

4.14. Automated Monitoring may involve profiling. For example, if unusual login activity is identified via Automated Monitoring, this may trigger an automated action such as a multifactor authentication request being sent to the relevant user.

4.15. The University will not carry out any profiling which leads to a decision based solely on automated processing which produces legal effects concerning a user or similarly significantly affects a user in contravention of Article 22(1) UK GDPR.

4.16. If any Automated Monitoring, including profiling, reveals certain behaviours then Targeted Monitoring may be undertaken. Any decision to undertake Targeted Monitoring will be made by the DPO or Deputy DPO and a member of the Executive Board, or their nominees.

Filtering

4.17. The selective disabling of access to external websites will be implemented only by IT Services under the direction of the CIDO. The list of disabled websites will be reported to The Compliance (Data) Committee but may be updated as required by the CIDO.

4.18. Users wishing to view material on external websites whose access has been disabled by targeted filtering should refer to the Security Sensitive Research Procedure which outlines how access can be granted and any material acquired as a result should be stored. No attempt should be made to circumvent the filters without following the procedures in the Security Sensitive Research Procedure.

Procedures

4.19. Automated Monitoring may be carried out in relation to daily information security considerations in accordance with good industry practice. The Head of Information Security shall be responsible for determining the use of such Automated Monitoring.

4.20. Any other proposed Automated Monitoring will be subject to the oversight of Compliance (Data) Committee, including but not limited to the implementation of new systems. However, there may be circumstances when Automated Monitoring is justified and must be implemented urgently, for example in response to an ongoing cyber-attack or other threat to the security of the University's networks, systems or data.

4.21. Requests to undertake Automated Monitoring will be made by the CIDO (or nominee) to Compliance (Data) Committee who will consider the purposes of the monitoring and any privacy implications before granting approval. A privacy impact assessment (PIA) may be undertaken.

4.22. When it is not possible or practicable to secure prior consent from Compliance (Data) Committee for Automated Monitoring, for example, when facing an immediate and serious cyber-attack, then the CIDO may authorise Automated Monitoring without prior approval but should report fully to Compliance (Data) Committee at the next available opportunity.

5. Governance Requirements

5.1. Implementation: Communication Plan

- The key elements of this Procedure which require communication to all users are included in the Acceptable Use Procedure. No campus wide communication of this Procedure is therefore required. This Procedure will be published on the University policies webpage. Further information will be included in the IT Privacy Notice.

5.2. Implementation: Training Plan

- Not applicable

5.3. Review

- This Procedure will be reviewed every three years.

5.4. Legislative Context and Higher Education Sector Guidance or Requirements

- UK General Data Protection Regulation
- Data Protection Act 2018
- Regulation of Investigatory Powers Act 2000
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- Counter-Terrorism and Security Act 2015

5.5. **Sustainability**

- The sustainability impact of Automated Monitoring and filtering is considered within the core IT service offerings as part of a security-by-design approach.

6. Stakeholder Engagement and Equality Impact Assessment

6.1. An Equality Impact Assessment was completed on **31 July 2023** and is held by the Authorised Co-ordinator.

6.2. Stakeholder Consultation was completed, as follows:

Stakeholder	**Nature of Engagement**	**Request EB Approval (Y/N)**	**Date**	**Name of Contact**
Governance	Consultation	N	31 Jul 2023	Andrea Langley