Monitoring Policy

Originator name:	Donald Macinnes
Section / Dept:	Information Compliance Unit
Implementation date:	TBA
Date of next review:	TBA
Related policies:	Data protection policy IT Acceptable Use Policy Information Security Policy Security Sensitive Research Policy
Policy history:	N/A

Version History

Version	Author	Revisions Made	Date
1	Donald Macinnes	First Draft	5 October 2018
2	Donald Macinnes	Revisions from Lorne Bozinoff included	7 September 2020

1	**Introduction**
	Forum Research Inc. respects the privacy of its staff and clients and acknowledges that the private lives of individuals overlaps with their working lives. For example, the personal use of corporate email accounts and the internet at work is permitted provided it does not interfere with the proper performance of a staff member's duties. Any automatic monitoring of employees and the computer equipment issued to them by the company risks privacy intrusion and will only be undertaken with a high level of justification and in appropriately controlled conditions. Any monitoring of specific individuals (targeted monitoring) will only be undertaken in exceptional circumstances, in appropriately controlled conditions and with adequate justification and oversight. Forum also acknowledges that the filtering of access to certain websites might compromise the ability of staff to undertake research freely. It must balance its support for research freedom within the law against its obligation to protect the company and its staff/clients from the risk of harm or legal action that might arise from accessing certain sites. Filtering, under appropriately controlled conditions, will therefore be allowed.
1.1	**Purpose**
1.1.1	This policy sets out the controls and rules to be followed for those undertaking any monitoring to ensure that the privacy of all colleagues is appropriately protected and to protect the interests of staff engaged in monitoring who may discover activities amounting to misconduct so seriousthat they cannot reasonably be expected to ignore it. The policy aims to set expectations for staff on the degree of privacy they can expect when using corporate issued IT systems and equipment. The policy does not include rules or guidance on the use of corporate issued IT equipment or required standards of staff conduct. For guidance on the use of corporate issued IT equipment staff and students should review the IT Acceptable Use Policy. The policy also 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. The filtering that is implemented will prevent access only to those sites likely to contain harmful and/or illegal material or giving rise to a risk that vulnerable people might be drawn into illegal activity including terrorism.
1.2	**Scope**
1.2.1	This policy applies to all forms of monitoring including, but not limited to, the use of scanning software to monitor system events and user behaviour. This may mean that staff in IT Services, who manage the software which undertakes the monitoring, gain access to information about individual user behaviour. No monitoring of staff activity on staff owned devices is permitted as these are considered entirely private. However, staff owned devices using University networks may be monitored. Forum will normally co-operate with a lawful request to help law enforcement agencies investigate crime. Automated monitoring will apply to all those who use corporate systems so will include staff, students and others who may be given access to systems and networks.

	Targeted monitoring will apply only to Forum staff. Filtering will apply only to those sites identified as potentially harmful but will affect all users.
1.3	**Equality Analysis**
1.3.1	TBA
1.4	**Definitions**
1.4.1	**Automated monitoring** – monitoring undertaken at the network level to identify system events or anomalies that might help identify, prevent or mitigate cyber attacks and other threats to the Company's networks, systems and data. **Targeted monitoring** – monitoring aimed at a specific individual(s) to investigate conduct that may breach corporate policies or the law. **Filtering** – the selective disabling of access to external websites.
2	**Policy**
2.1	**Principles**
2.1.1	All members of staff should be aware that their use of corporate computing equipment may be monitored. This monitoring may be automated or targeted. Although the technical solutions to enable monitoring may be available to staff, no monitoring will ever be permitted because it is technically possible. All monitoring will be justified on the following grounds only: **Automated monitoring** Forum may undertake automated monitoring for the either of the following purposes: • The effective and efficient planning and operation of IT facilities • The detection, mitigation and prevention of cyber threats Where automated monitoring reveals activity which the company cannot reasonably be expected to ignore, the matter will be referred to Head of Security.

	Targeted monitoring Non automated (targeted) monitoring may be undertaken if criminal activity, which the company cannot reasonably be expected to ignore, is detected as a consequence of automated monitoring. Non automated (targeted) monitoring of IT facilities and systems issued to, and used by, staff members will only be undertaken to the extent permitted by or as required by law and as necessary or justifiable for the following purposes: • Detection and prevention of infringement of these and other policies and regulations • Investigation of alleged misconduct • Handling email and other electronic communications during an employee's extended absence • To find lost messages or to retrieve messages lost due to computer failure • To comply with any legal obligation
2.2	**Procedures**
2.2.1	Automated monitoring will be subject to the oversight of the Information Security and Governance Steering Group (ISAGG). 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 company's networks, systems or data. Requests to undertake automated monitoring will be made by the Chief Information Officer (or nominee) to the Information Security and Governance Group (ISAGG) who will consider the purposes of the monitoring and any privacy implications before granting approval. A privacy impact assessment (PIA) may be undertaken. When it is not possible or practicable to secure prior consent from ISAGG for automated monitoring, for example, when facing an immediate and serious cyber-attack, then the CIO may authorise automated monitoring without prior approval but should report fully to ISAGG at the next available opportunity. Targeted monitoring must never be undertaken without explicit prior approval. Authorisation to conduct targeted monitoring will be granted by the VP HR or member of Executive Board. Any targeted monitoring will be proportionate and reasonable steps will be taken to protect staff members' private lives. The Senior Information Risk Officer and Data Protection Officer should be consulted before approval is granted. The company will comply with lawful requests for

	information from law enforcement and government agencies for the purposes of detecting, investigating or preventing crime and ensuring national security. **Filtering** The selective disabling of access to external websites will be implemented only by IT Services under the direction of the Chief Information Officer. The list of disabled websites will be reported to ISAGG but may be updated as required by the CIO.
3	**Governance Requirements**
3.1	**Responsibility**
3.1.1	The Chief Information Officer is responsible for ensuring that any automated monitoring using technical measures is undertaken in compliance with this policy. Corporate Legal Counsel and Senior Information Risk Officer is responsible for assessing the privacy implications of any automated or targeted monitoring and will take advice from the Data Protection Officer. The VP HR or other member of Executive Board are responsible for authorising any targeted monitoring within the scope of this policy. The CIO is responsible for authorising the list of websites to be disabled as part of the company's filtering arrangements. The CIO is responsible for reporting to ISAGG on all automated monitoring and filtering implemented by IT Services. ISAGG is responsible for approving the list of filtered websites under the filtering provisions of this policy and for approving any automated monitoring.
3.2	**Implementation / Communication Plan**
3.2.1	The key elements of this policy which require communication to all staff are included in the IT Acceptable Use policy. No site wide communication of this policy is therefore required. The policy will be published on the company policies website.
3.3	**Exceptions to this Policy**
3.3.1	As this policy outlines the procedures to follow to undertake any form of monitoring which means that, provided the appropriate conditions are in place, monitoring is possible. No exceptions to the policy are envisaged.
3.4	**Supporting documentation**
3.4.1	N/A