IT Monitoring Policy

Version: **2020.11 Final**

Date: **November 2020**

Reviewed: **Annually**

Information Security Classification: **Public (when Final)**

Policy Statement on the Use, and Monitoring of the Use, of the University's IT and Communications System by Staff, Students and other Users

1. **Introduction**

1.1 The University encourages, and in some cases requires, the use of the Communications System by Users, as appropriate use helps communication and improves efficiency. Its inappropriate use, however, may cause problems ranging from minor distractions to legal claims against the University.

1.2 In the business environment, organisations need to monitor and inspect communications and data entering, leaving, or within, their communications systems. Such activity is regulated by various pieces of legislation. For example, the Data Protection Act 1998 ("DPA"), the Regulation of Investigatory Powers Act 2000 ("RIPA") and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ("TelReg"). From time to time, it is necessary for the University to Monitor certain Communications and Data, to ensure that its Communications System is not misused, and to ensure compliance with the requirements of the DPA, RIPA and TelReg, and any associated legislation and secondary legislation in force from time to time.

1.3 By using the Communications System, the User thereby consents to the Monitoring activities set out in this Policy and agrees at all times to use the Communications System for the purposes for which it is intended.

1.4 This Policy sets out:

1.4.1 the Monitoring measures that the University has decided are acceptable;

1.4.2 the type of circumstances in which Monitoring may be instituted;

1.4.3 the procedures that ensure Monitoring is carried out in appropriate circumstances, and that prevent abuse of the Monitoring process.

1.5 This Policy should be read in conjunction with the University's Regulations. All use by Users of the Communications System shall, at all times, be subject to this Policy and the University's Regulations.

2. **Statement of Policy**

2.1 The University reserves the right to Monitor any and all Communications and Data entering, leaving or within its Communications System in accordance with this Policy, the rights set out in the DPA, RIPA, TelReg, and other applicable legislation or secondary legislation that may be in force from time to time.

2.2 Users are hereby notified that:

2.2.1 Any personal Communications and Data, as well as Communications and Data relating to the functioning of the University, entering, leaving or within the Communications System may be Monitored by Relevant Staff in accordance with:

2.2.1.1 Applicable legislation; and/or

2.2.1.2 this Policy; and/or

2.2.1.3 the University's Regulations; and/or

2.2.1.4 valid rights and obligations contained in contractual agreements with third parties; and/or

2.2.1.5 valid requests under English law, by the police and by other recognised law enforcement agencies

2.2.2 The University is under a legal obligation, by virtue of the agreement that it has entered into with UKERNA, to ensure, as far as possible, that all Users do not use the JANET System to transmit or transfer certain types of electronic data and/or communications. Monitoring of Communications and Data entering, leaving or within the Communications System will be carried out by Relevant Staff to ensure the University's compliance with this legal obligation.

2.2.3 The University is under a legal obligation to report to the UK police, or any other recognised law enforcement agency via a relevant authority in the UK, the discovery of certain types of Communications and Data, if those Communications and Data enter, leave or are within the Communications System. The University may need to Monitor Communications and Data to ensure the University's compliance with this legal obligation.

2.2.4 The University agrees and acknowledges that Relevant Staff are not permitted to routinely access Communications and Data entering, leaving or held within the Communications System. All Monitoring will be carried out by Relevant Staff:

2.2.4.1 to ensure compliance by Users with this Policy and/or the University's Regulations; or

2.2.4.2 for the circumstances set out at Paragraph 2.2.1.

2.2.5 Attempts by any Relevant Staff or User to implement any system of Monitoring in breach of this Policy may be subject to disciplinary proceedings.

2.2.6 Many types of routine Communications System tasks will involve Relevant Staff having access to various levels of Communication and Data used, created, received or held by Users, for example when:

2.2.6.1 receiving mail failure notifications - these may contain the text of the failed message, which will be automatically sent by the e-mail server that rejected or redirected it;

2.2.6.2 making archive copies from fileservers - as part of the archiving process names of files held in Users' accounts can be read;

2.2.6.3 sorting output from printers prior to its dissemination to Users – as part of the dissemination process the content of the output may be visible;

2.2.6.4 using remote desktop management, or similar, software in circumstances such as installing new versions of software or dealing with problems being experienced by Users – such tasks must only be carried out with the knowledge of, and at times agreed by, individual Users;

2.2.6.5 using remote or local network management tools, or similar tools to locate, analyse, and resolve perceived, or actual, network problems, or similar;

2.2.6.6 using the Student Information System or any similar system.

Such access will not constitute a breach of this Policy, even when such access leads to the implementation of authorised Monitoring and/or disciplinary procedures against a User.

2.2.7 The University recognises that, due to the nature of the Communications System, Communications and Data passing across networks, or printed out on the University's equipment, may at times be visible in readable form either accidentally or incidentally. In such circumstances,

Communications and Data may be viewed by Relevant Staff or other Users. Such accidental or incidental viewing will not constitute a breach of this Policy, even when such viewing leads to the implementation of authorised Monitoring and/or disciplinary procedures against a User.

2.2.8 In addition to the circumstances where the University may Monitor Communications and Data, the University expressly reserves the right to Monitor Communications and Data entering, leaving or within the Communications System in the following circumstances:

2.2.8.1 where by virtue of carrying out routine Communications System tasks, Relevant Staff discover Communications and Data that are in breach of:

2.2.8.1.1 Applicable legislation; and/or

2.2.8.1.2 this Policy; and/or

2.2.8.1.3 the University's Regulations; and/or

2.2.8.1.4 valid rights and obligations contained in contractual agreements with third parties

2.2.8.2 where complaints are received by relevant authorities in the UK (such as law enforcement agencies) suggesting that the University's Communications System is being used to store, transmit or transfer Communications and Data that are in breach of:

2.2.8.2.1 applicable legislation; and/or

2.2.8.2.2 this Policy; and/or

2.2.8.2.3 the University's Regulations; and/or

2.2.8.2.4 valid rights and obligations contained in contractual agreements with third parties

2.2.8.3 where the University has been requested, or required, to monitor Communications and Data by the UK police, or by any other recognised law enforcement agency via a relevant authority in the UK, as part of an investigation;

2.2.8.4 where there is other reasonable suspicion that Users are storing, transmitting or transferring Communications and Data that are in breach of:

2.2.8.4.1 applicable legislation; and/or

2.2.8.4.2 this Policy; and/or

2.2.8.4.3 the University's Regulations; and/or

2.2.8.4.4 valid rights and obligations contained in contractual agreements with third parties

2.2.9 The University reserves the right to Monitor the nature and extent of Communications and Data uploaded and downloaded from the Internet or any other information resource. This may be carried out by various means, including random filename searches of fileservers, cache and cookie searches, file size checks, and so on.

2.2.10 Without prejudice to the provisions of Paragraphs 2.2.1 to 2.2.9, there may be circumstances where Monitoring of Communications and Data entering, leaving or within the Communications System, or a User's use of the Communications System, may from time to time be Monitored by computer software used by the University, such as, but not limited to, the use of anti-virus software, or software to filter out unsolicited email messages (so-called "junk mail"). Such Monitoring will not

constitute a breach of this Policy, even when such Monitoring exposes reasonable suspicion that Users are storing, transmitting or transferring Communications and Data, using the Communications System, which is in breach of:

2.2.10.1 applicable legislation; and/or

2.2.10.2 this Policy; and/or

2.2.10.3 the University's Regulations; and/or

2.2.10.4 valid rights and obligations contained in contractual agreements with third parties

2.2.11 There may be circumstances where Communications and Data entering, leaving or within the Communications System may be subject to Monitoring for the purposes of establishing whether such Communications and Data need to be actioned or forwarded. In these circumstances, Relevant Staff will not be required to obtain written consent for Monitoring as specified under section 3.1. For example, Relevant Staff may require any relevant User password to be disclosed or changed, solely for the purpose of obtaining access to the User's Communications and Data during absences from the office, due to holidays, sickness, time off in lieu, flexi leave, maternity leave or other similar reasons, when the User is no longer employed, registered, enrolled or actively involved with the University, or when the User is unable to access his/her Communications and Data. However, in these circumstances, Relevant Staff may only deal with those Communications and Data that are related to the University's business; they are not permitted to examine the contents of a User's Communications and Data that are clearly Personal Communications, unless these appear (from the data available to the Relevant Person, without opening the User's Communications and Data) to be in breach of:

2.2.11.1 applicable legislation; and/or

2.2.11.2 this Policy; and/or

2.2.11.3 the University's Regulations; and/or

2.2.11.4 valid rights and obligations contained in contractual agreements with third parties

2.2.12 Where Users use their own equipment, and/or systems, in connection with Communications and Data entering, leaving, or within, the Communications System, such use shall at all times be subject to the provisions outlined in this Policy.

3. **Other Monitoring Factors**

3.1 Monitoring of Communications and Data, and specific access to Communications and Data, by Relevant Staff, shall only be carried out under this Policy with the knowledge and written consent of at least one of the following:

3.1.1 the University Secretary-Registrar

3.1.2 the Director of Information Systems Aston

3.2 Monitoring of Communications and Data shall only take place for such time as is reasonably necessary to ascertain whether the User or Users concerned are using the Communications System to store, transmit, or transfer Communications and Data in breach of:

3.2.1 applicable legislation; and/or

3.2.2 this Policy; and/or

3.2.3 the University's Regulations; and/or

3.2.4 valid rights and obligations contained in contractual agreements with third parties.

3.3 Any long-term Monitoring shall only be permitted when this is specifically requested by the UK police, or by any law enforcement agency via a relevant authority in the UK, as part of a criminal investigation.

3.5 All Monitoring of Communications and Data shall be reported, along with the reasons for that action being taken, and the result, if any, of the Monitoring to the Chair of the Information Security Policy Implementation Group, as soon as such Monitoring is completed.

3.6 Communications and Data collected as a result of any Monitoring will, if not falling under the non-disclosure provisions set out in the DPA (for example where such disclosure would cause damage or distress), be disclosable as part of a subject access request under the DPA.

4. **Responsibility for this Policy and Amendments**

4.1 The Chair of the Information Security Policy Implementation Group shall be responsible for reviewing, amending, updating and submitting revised versions of this Policy to the University's Senate and Council for approval.

4.2 The Chair of the Information Security Policy Group reserves the right to update and/or amend this Policy at any time, following consultation with appropriate groups within the University. Any amendments or updates shall be effective immediately when the same have been approved by the University's Senate and Council.

5. **Appendix**

5.1 Definitions

In this Policy the following terms have the following meanings:

"Communications and Data" the creation, storage and processing of any and all communications and/or data by Users including without limitation emails, files (electronic or otherwise), faxes and post.

"Communications System" the University's systems, including without limitation computer terminals, mainframe computers, process automation computers, email system, fax system and related communications and information resources such as networks (private and public), telephony systems, the telecommunications systems, as well as all post.

"Monitor/Monitoring" the automatic or manual monitoring, or the automatic or manual interception, of the use of the Communications System by Users in accordance with this Policy and applicable legislation.

"Personal Communications" a User's Communications and Data that are marked "personal" or "private" or "confidential", or a User's Communications and Data that are obviously (without opening them) not directly or indirectly concerned with the business of the University.

"Policy" this statement on the Use, and Monitoring of the Use, of the University's Communications Systems by Staff, Students and other Users, as amended from time to time.

"Relevant Staff" the University's staff, as required for implementing this Policy and as shall be identified from time to time on the University website on a webpage linked to this policy.

"Staff" any and all staff, whether academic, administrative, technical or other, employed by the University.

"Students" any individual enrolled or registered with the University or undertaking study of any kind provided by, at, or under the auspices of the University.

"Student Information System" collectively, the communications systems used by the University to store, manage and retrieve information about, and pertaining to, its Students, including, without limitation, the SITS Aston Vision system and the DS Galaxy 2000 Library Management System.

"JANET System" the private, government funded network for education and research, managed by UKERNA. (All further and higher education organisations are connected to JANET, as are all the Research Councils). For more information on the JANET System visit: www.ja.net/about_JANET.html

"UKERNA" the company that manages the operation and development of the JANET System under a service level agreement from the Joint Information Systems Committee (JISC) of the UK Higher and Further Education Funding Councils. For more information on UKERNA visit:

www.ukerna.ac.uk/aboutukerna.html

"University" collectively Aston University, the address of which is Aston Triangle, Birmingham, B4 7ET, UK, and all other parts of Aston University, including without limitation Conference Aston, Aston Media and the Business Partnership Unit.

"University Regulations" collectively, the Regulations for the Use of University ICT Facilities and any associated regulations and guidelines for the use of the University's information, computing and communications facilities and services, in force from time to time and as amended from time to time.

"University Secretary-Registrar" the Secretary-Registrar of the University.

"Users" all users authorised by the University to use the Communications System, including without limitation Staff, Students, consultants, visitors and Alumni.

5.2 Learn More:

Users can find out more about what the various pieces of legislation aim to protect by reading below.

(Please note that where links are provided to websites any information contained on such websites is for general information only. They are not intended to be a clear statement of the law.)

Data Protection Act 1998 – Information Commissioner's Website

Regulation of Investigatory Powers Act 2000 – Regulation of Investigatory Powers (RIP) Act

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ("TelReg")

The TelReg permits employers, from 24 October 2000, to monitor and/or record many communications in order to:

- establish facts relevant to the University;
- ascertain Users compliance with the law and/or self-regulatory policies and procedures;
- prevent or detect crime;
- investigate or detect unauthorised use of the University's telecommunications system;
- ensure the effective operation of the University's telecommunications system.