Security monitoring policy

February 2020

UNIVERSITY OF WINCHESTER

Document Title:	Security monitoring policy
Document Author:	Fiona Greig
Responsible Person and Department:	Fiona Greig Library & IT Services
Approving Body:	SMT
Date of Approval:	Enter date here
Date Effective From:	*17th Feb 2020*
Review Date:	***31st July 2021***
Indicate whether the document is for public access or internal access only Indicate whether the document applies to collaborative provision? *(Strikethrough text, as appropriate)*	**Public Access** ~~**Internal Access Only**~~ ~~**Applies to Collaborative Provision**~~
Summary: This policy outlines how Librayr & IT Services will use monitoring and logging approaches to ensure the data andnetwork that the University creates, manages and maintains.	

TABLE OF CONTENTS *(right-click table below and select 'Update Field' and, if given option, 'Update entire table').*

1. Scope

1.1. The information the University manages shall be protected against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information to authorised users. For information security to be effective it requires the participation and support of all University staff, student and other persons who have access to its information technology.

1.2. Information security at the University is governed by a number of interlinked policies which consists of a Network Security Policy and a number of subsidiary policies. This subsidiary policy covers the monitoring and logging of all uses of information technology. It is the responsibility of every user to know these policies, and to conduct their activities accordingly.

1.3. Additional policies cover specific issues, technologies and types of usage are listed below:

- Acceptable use policy
- Home and mobile working policy

2. Monitoring

2.1. Networks and computers may be monitored and usage logged. Logs are kept secure and are only available to personnel authorised by the Director of Library & IT Services and will only be kept as long as necessary in line with data protection guidelines and published retention plans.

2.2. Logs, and indeed any data on the network, may be shared as part of the University's requirements under the Freedom of Information Act.

2.3. The University's networks and computer may be monitored and logged for all lawful purposes including:

- Ensuring use is authorized
- Management of systems
- Protecting against unauthorised access
- Verifying security procedures
- System and operational security
- Compliance with University policies and regulations
- Detection and prevention of crime

2.4. Monitoring includes active attacks by authorised University users to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorised purposes. All information, including personal information, placed on or sent over this system may be monitored.

2.5. Monitoring is automated in the detection and removal of viruses, malware, spam, pornographic and inappropriate URL's and other activities not lawful to University business. Use of university provided technology, authorised or unauthorised, constitutes consent by the user to monitoring of these system.

2.6. Unauthorised use (as outlined in the associated policies listed above). Evidence of unauthorised use collected during monitoring may be used subsequently in a disciplinary, criminal or another form of proceedings. Use of the University IT systems constitutes consent to monitoring for these purposes.

3. Email scanning

3.1. Incoming e-mail may be scanned by the University including using virus-checking software. The software may block unsolicited marketing e-mail (spam), e-mail which has potentially inappropriate attachments, bad language or any other inappropriate material.

3.2. The University uses a system that will not deliver the email but inform users of captured suspicious material. From the sender and the subject each user is able to determine if the email should be released and delivered. Users must take decisions based on a risk profile.