UNIVERSITY OF WINCHESTER

Security Monitoring Policy
01.08.2025

Document Title:	Security Monitoring Policy
Responsible Role and Department:	Director of Knowledge & Digital Services
Approving Body:	University Leadership Team
Date of Approval:	19th September 2025
Date Effective From:	01 August 2025
Review Date:	31st July 2026
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 Knowledge & Digital Services will use monitoring and logging approaches to assure the data and network that the University creates, manages and maintains.

TABLE OF CONTENTS

1. Scope of the policy

1.1. The information the University manages is 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, students 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 behave accordingly.

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

- IT Acceptable Use Policy is the core and principal policy
- Home and Mobile Working Policy (IT Elements)
- Bring Your Own Device Policy (Student)
- Network Security Policy

2. Monitoring

2.1. Networks and computers are monitored and usage logged. Logs are kept secure and are only available to personnel authorised by the Director of Knowledge & Digital 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 authorised
- 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 other sites that have been flagged to the University by services provided by our Internet

Service Provider (Jisc, working with the National Cyber Security Centre), our Firewall provider and from threat intelligence sources where a risk to University IT systems is identified, or where there is evidence of other activities not lawful to the University business. At times the University may place a manual block on sites we are informed of as a risk to individuals' personal data as investigations by internal or external agencies, including law enforcement, has stated the users of our system are at risk of targeting for purposes including identity theft. Use of University provided technology, authorised or unauthorised, constitutes consent by the user to monitoring of these systems.

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.

2.7. Line managers / investigation officers may request a log of a staff member's use of IT, including websites visited, as part of any disciplinary process. In the same way a student's use of our network, including as used when in our accommodation, can be accessed as part of a disciplinary or criminal investigation.

3. Email scanning

3.1. Incoming e-mail is 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.

Equality Impact Assessment	
Summary of process undertaken to determine equality impacts:	An initial screening was carried out to identify potential impacts on protected groups. Relevant data and stakeholder feedback were reviewed to assess risks and opportunities. Where necessary, mitigation actions were proposed to ensure fairness and compliance with the Equality Act 2010. The assessment will be monitored and updated as needed.
University Committee (name/ date) where equality impacts discussed (may be Committee of approval, or another):	University Leadership Team
Identified equality impact(s) on colleagues and students (i.e. any specific impacts related to this policy that may cause disadvantage for people due to one or more particular protective characteristic)	
Protected Characteristic	Impact(s) identified and any action(s)/mitigation(s) to address these impact(s), as necessary.
Age	No impact identified
Disability	No impact identified
Gender Identity	No impact identified
Marriage/Civil Partnership	No impact identified
Pregnancy and Maternity	No impact identified
Race (incl. nationality)	No impact identified
Religion and Belief	No impact identified
Sex	No impact identified
Sexual Orientation	No impact identified