University of Bristol
Information Security Policy

Title:	**Investigation of Computer Use**
Reference:	**ISP-18**
Status:	**Draft**
Version:	**1.4**
Date:	**September 2013**
Reviewed:	**June 2021**
Classification:	**Public**

Contents

- Introduction
- Authority
- Scope
- The University's Powers to Access Communications
- The Powers of Law Enforcement Authorities to Access Communications
- Other Third Parties
- Covert Monitoring
- Procedure

Introduction

This Investigation of Computer Use Policy is a sub-policy of the Information Security Policy (ISP-01) and outlines the circumstances in which it is permissible for the University to monitor and access the IT accounts, communications and other data of its members.

The University respects the privacy and academic freedom of its staff and students and recognises that investigating the use of IT may be perceived as an invasion of privacy. However, the University may carry out lawful monitoring of its IT systems when there is sufficient justification to do so and when the monitoring has been authorised at an appropriately senior level.

Staff, students and other members should be aware that the University may access records of use of email, telephone and other electronic communications, whether stored or in transit. This is in order to comply with the law and applicable regulations, to ensure appropriate operation and use of the University's IT systems and to ensure compliance with other University policies. Routine monitoring to ensure the security and effective operation of University IT systems occurs at all times, though more targeted monitoring and access to records and logs may also occur. All access and monitoring will comply with UK legislation including the Regulation of Investigatory Powers Act 2000 (RIPA), the

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBP), the Human Rights Act 1998 (HRA) and the Data Protection Act 2018 (DPA).

Authority

Decisions to access the IT accounts, communications or other data of members will not be taken by IT Services nor any member of the faculty/division of the individual to be investigated in order to ensure that such requests are free of bias and are not malicious. Decisions to undertake such investigations will therefore be made by the Director of Legal Services and Deputy Secretary, or the Information Governance Manager, or an appropriate nominee of either position, who will also determine the scale of the work to be undertaken.

Scope

All members (staff, students and associates) of the University together with any others who may have been granted permission to use the University's information and communication technology facilities are subject to this policy.

Exceptions to this policy may include communications carried out on, or data housed in, areas of the University network that for contractual or legal compliance reasons are exempted, for example autonomous networks specifically obtained for these purposes and for which an agreement has been obtained with IT Services and the University Secretary's Office.

The University's Powers to Access Communications

Authorised University staff may access files and communications, including electronic mail files, stored on any IT facilities owned, managed or provided by the University and may examine the content of these files and any relevant traffic data.

The University may monitor use of IT facilities, access files and communications for the following reasons:

- to ensure the confidentiality, integrity and availability of its data (for example the University may take measures to protect systems from, and actively monitor for, viruses and other threats to information security)
- to establish the existence of facts relevant to the business of the institution (for example, where a case of suspected plagiarism is being investigated

and there is sufficient evidence, the contents of an individual's communications and/or files may be examined without their consent with the authority of an authorised person);

- to investigate or detect unauthorised use of its systems;
- to investigate or detect unacceptable use of its systems as defined by ISP:09 Acceptable Use policy
- to ascertain compliance with regulatory or self-regulatory practices or procedures relevant to the University's business;
- to monitor whether or not communications are relevant to the business of the University (for example, checking email accounts when staff are absent, on holiday or on sick leave);
- to comply with information requests made under the Data Protection Act or Freedom of Information Act (individuals would in normal circumstances be notified).

The Powers of Law Enforcement Authorities to Access Communications

A number of other non-University bodies and persons may be allowed access to user communications under certain circumstances. Where the University is compelled to provide access to communications by virtue of a Court Order or other competent authority, the University will disclose information to these noninstitutional bodies/persons when required and in response to legitimate requests as allowed under the Data Protection Act 2018

For example, under the Regulation of Investigatory Powers Act 2000 a warrant may be obtained by a number of law enforcement bodies regarding issues of national security, the prevention and detection of serious crime or the safeguarding of the economic well-being of the UK.

Other Third Parties

The University makes use of third parties in delivering some of its IT services. These third parties may intercept communications for the purpose of ensuring the security and effective operation of their service (for example, a third party which provides email services to the University may scan incoming and outgoing email for viruses and spam).

Information on our current email provide for staff, Microsoft, can be found at the below website:

https://www.microsoft.com/en-gb/trust-center/product-overview

The University may also make use of third party services to ensure the security of its information and IT assets. For example, this may include monitoring of University network traffic and device activity, vulnerability scanning or penetration testing being carried out by a third party on behalf of the University.

Covert Monitoring

Covert monitoring of computer use will only be authorised in exceptional circumstances where there is reason to suspect criminal activity or a serious breach of University regulations and notification of the monitoring would be likely to prejudice the prevention or detection of that activity. The period and scope of the monitoring will be as narrow as possible to be able to investigate the alleged offence and the monitoring will cease as soon as the investigation is complete. Only information gathered in relation to the alleged offence will be retained. This information will only be viewed by those for whom access is strictly necessary, for example in relation to potential disciplinary proceedings.

Procedure

Requests for investigation under this policy may be made by any member of staff or student, although typically the request will come from a head of department, school or division. Occasionally requests are made from outside of the University, for example by the police. The request should be made to the University Secretary's Office and should include the following information:

a. the name and department of the student or staff member whose computer or computing activity you wish to be investigated;
b. the reasons for the request;
c. where computer misuse is alleged, the evidence on which this is based;
d. the nature of the information sought;
e. how the requested information will be used
f. any other relevant information, for example, that the request relates to ongoing disciplinary or grievance procedure.

In order to monitor the number and type of requests made, the University Secretary's Office will keep a record of the requests that have been made and those which were acceded to.