**IT MONITORING NOTICE**

The University is required by law to bring to the attention of all users the following notices.

**(1) Regulation of Investigatory Powers Act 2000**

As required by UK legislation, Cardiff University draws to the attention of all users of the University's Data and Telecommunication Networks the fact that their communications may be intercepted as permitted by legislation.

The legislation (including the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000) provides that interceptions are authorised for:

* monitoring or recording communications:
  + to establish the existence of facts, to ascertain compliance with regulatory or self-regulatory practices or procedures or to ascertain or demonstrate standards which are or ought to be achieved (quality control and training);
  + in the interests of national security (in which case only certain specified public officials may make the interception);
  + to prevent or detect crime;
  + to investigate or detect unauthorised use of telecommunication systems or;
  + to secure, or as an inherent part of, effective system operation;
* monitoring received communications to determine whether they are business or personal communications;
* monitoring communications made to anonymous telephone helplines.

The University does not need to gain consent before intercepting for these purposes although we need to inform staff and students that interceptions may take place.

**(2) Data Protection Act 2018 - Monitoring**

IT Services hold user registration data and various information on the use of the university's computer systems and network; this includes log-in and log-out times and locations, printing logs, World Wide Web cache logs and network traffic logging.

While normally only used for resolving operational problems, these logs will be analysed (under paragraphs 7 and 8of the university's IT Regulations) down to the individual user where a breach of the Regulations or other university rules is suspected or to audit system access in the case of an information security incident.

The information will also be used to communicate with individuals to alert them to malfunctions within the Cardiff University IT facilities or to request action to correct the malfunctions which may be putting the normal operation of the IT facilities in jeopardy.

The university may also deploy the use of manual or automatic searches in order to ascertain compliance with software licensing as well as terms and conditions relating to software usage. This may entail a search of all software programs installed on university IT equipment in both the physical and virtual environment. This data may be used for investigation of breaches of the university IT Regulations in addition to management of the university’s IT facilities.

In addition, statistical analysis may take place to provide management information on teaching space, footfall, laboratory, software, printing, cache, network and general computer usage for the purposes of management of the university’s facilities.

Where there is a potential for information held on the university’s systems to be required for legal proceedings, the university may place a legal hold on this data to prevent its loss. The university does not need to gain consent to do so.

**(3) Web Content Filtering**

In accordance with the Website Filtering Policy Cardiff University filters web content into the university as it passes through the university firewalls for the purpose of protecting the reputation of the university and ensuring that the acceptable use policy of our network provider (JANET) is safeguarded.

**Logging and Access**

Access to log data will be restricted. In accordance with (2) above these logs will be analysed (under paragraphs 7 and 8of the university's IT Regulations) down to the individual user where a breach of the IT Regulations is suspected. All allegations relating to use of the university’s IT facilities in connection with the possession of indecent images of children, or other illegal material in connection with children, shall be reported to the Designated Officer under the [Safeguarding Children and Vulnerable Adults Policy](https://www.cardiff.ac.uk/public-information/policies-and-procedures/safeguarding). Web content filtering data may also be provided to law enforcement bodies where it is necessary for the prevention or detection of crime, prosecution or apprehension of offenders or national security.

High level data provided by the logs for the provisioning of metrics for management information purposes will be anonymised.

**(4) Third Party Access to ‘Personal’ file stores and university email accounts**

For recovery of university systems, Head of Schools and Departments have the ability to request access to users' filestore within their remit.

On occasion it may also be necessary for business purposes to enable/edit out of office messages in email accounts or to access information held on university IT Facilities without the account owner’s consent. All such interventions must be authorised by the Head of School/ Professional Services Department and any searches will take place in the presence of another. In order to limit access to business data only in these circumstances, all users are encouraged to store any personal records held on university IT facilities in a folder clearly marked ‘Personal’.

|  |  |
| --- | --- |
| **Version Control Table** | |
| **Document Name:** | **IT Monitoring Notice** |
| **UEB Policy Sponsor:** | Senior Information Risk Owner – University Secretary and General Counsel |
| **Policy Owner:** | Senior Compliance Advisor and Data Protection Officer University Secretary’s Office |
| **Policy Author:** | Senior Compliance Advisor and Data Protection Officer, University Secretary’s Office |
| Version Number: | Version 4.2 |
| Approval Date: | 27 March 2023 |
| Approved By: | Information Security Operations Group |
| Date of implementation: | April 2023 |
| Date of Last Review: | May 2018 |
| Date of Next Review: | April 2024 |
| For Office use – keywords for search function |  |