University of Bristol
Information Security Policy

Title:	**Human Resources**
Reference:	**ISP-05**
Status:Approved	
Version:	**1.2**
Date:	**July 2014**
Reviewed:	**August 2019**
Classification:	**Public**

Contents

Introduction

This Human Resources Policy is a sub-policy of the Information Security Policy (ISP-01) and sets out the Human Resources processes that must be implemented to ensure that employees are able, trained and required to protect the University's information assets.

Recruitment, references and screening

For roles involving handling of strictly confidential information or accessing sensitive information systems, Human Resources may use a pre-employment or change of role screening process to help ensure that employees selected are suited to the demands of the job.

Employment contract terms

Employees are to sign a contract binding them to comply with the Rules of Conduct for Members of Staff (Appendix 1 of Ordinance 28) and the Terms and Conditions of Employment.

An example of behaviour which may constitute misconduct as outlined in Appendix 1 of Ordinance 28, is :

> ‘unauthorised use, processing or disclosure of personal data contrary to the University’s policies and procedures in relation to data protection.’

It is a stipulation of the Terms and Conditions of Employment that:

> ‘During the course of employment, staff are expected to comply with all of the University's employee rules, regulations, statutes, ordinances, procedures, policies and codes of practice, including those relating to the use of computers and data protection.’

Information security education and training

The University is committed to providing staff with sufficient training to ensure that they are able to fulfil their specific information security responsibilities. The University’s information security training programme is mandatory for all staff, and can be accessed from the My Review system.

Information system users will be provided with instructions and training to ensure they do not compromise security through lack of awareness or skill.

Employee termination, suspension or change of appointment

Upon termination, suspension or change of appointment, Human Resources will revise the staff records system accordingly. This will trigger appropriate account management processes on centrally managed IT systems. Managers, however, should be aware that access to many sensitive systems is not yet automatically controlled and should make appropriate requests for access, change of permissions or denial of access to the relevant system managers.

Upon termination, all employees, contractors and third parties must return all information assets and equipment held which belong to the University.

It is stated in the general terms and conditions that:
‘10.1 Any property of the University shall remain the property of the University (except for intellectual property belonging to a member of staff under clause 11) and shall be handed over by staff to the University on demand and in any event on the termination of employment’.

IT usage monitoring and access

The Secretary’s Office may authorise for the legally compliant monitoring of its IT systems to be undertaken for legitimate University purposes. The policy relating to how the University may monitor usage of its IT systems is outlined in the Investigation of Computer Use Policy (ISP-18).

Conduct procedure

Employees who, after an investigation, have been found to have breached security or violated policy, may be subject to disciplinary action under the Conduct Procedure (Ordinance 28).

Unless the police are involved from the outset, when different procedures may apply, Human Resources and IT Services will coordinate the investigation of any suspected improper use of University IT facilities. Human Resources will coordinate any resultant disciplinary action.

Where there are reasonable grounds for suspecting misuse of a computer account, the Secretary's Office may authorise for that account to be suspended and/or investigated by IT Services.

Third party compliance

Precautions, in the form of a contract, should be taken to protect the information security interests of the University where external organisations or individuals are:

- Employed to work on University information systems.
- Provided with or given access to confidential information.

Further guidance is outlined in the Outsourcing and Third Party Compliance Policy (ISP-04).

If you are employing a University of Bristol undergraduate or postgraduate student as an intern, consideration must be given to the information they are able to access. Access levels must be appropriate based on the role they are performing. Access to the personal data of other University students and staff is unlikely to be appropriate.

Further guidance

Conduct Procedure for Members of Staff (Ordinance 28)
http://www.bristol.ac.uk/hr/policies/ord28index.html

General terms and conditions of employment for all staff
http://www.bristol.ac.uk/hr/terms/generalterms.html#a15

Mandatory information security training
http://www.bristol.ac.uk/infosec/training/

Information Security Staff Training Issues
http://www.bristol.ac.uk/infosec/uobdata/staff/

Investigation of Computer Use Policy (ISP-18)
http://www.bristol.ac.uk/infosec/policies/docs/isp-18.pdf

Outsourcing and Third Party Compliance Policy (ISP-04)
http://www.bristol.ac.uk/infosec/policies/docs/isp-04.pdf

University Data and You
http://www.bristol.ac.uk/infosec/uobdata/