University of Bristol

Information Security Policy

Title	Human Resources
Reference	ISP-05
Status	Approved
Version	2.0
Date created	July 2013
Last reviewed	January 2023
Next review	January 2024
Classification	Public

Contents

1. Introduction 1

2. Scope 1

3. Policy 2

3.1 Recruitment, References and Screening 2

3.2 Employment Contract Terms 2

3.3 Information Security Education and Training 2

3.4 Employee Termination, Suspension or Change of Appointment 2

3.5 IT Usage Monitoring and Access 3

3.6 Suspected Misconduct 3

3.7 Interns and Student Hires 3

3.8 Honorary and Associate Staff 3

3.9 Third Party Compliance 3

4. Further Guidance 3

1. 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.

2. Scope

This policy applies to all members of the University who have been given Staff status (this includes any contractors, students, interns, honorary and associate or temporary members with a contractual agreement to work for the University).

3. Policy

3.1 Recruitment, References and Screening

For roles involving handling of data classified as Confidential or above, Human Resources may use a pre-employment or change of role screening process to help ensure that employees selected are suited to the requirements of the job.

Further guidance on pre-employment checks can be found at
http://www.bristol.ac.uk/hr/resourcing/practicalguidance/appointment/checks.html

3.2 Employment Contract Terms

Employees are to sign a contract binding them to comply with the Rules of Conduct for Members of Staff (Ordinance 10, Section 4, Appendix A: http://www.bristol.ac.uk/media-library/sites/university/documents/governance/constitution/ordinance-10-employment.pdf) and the Terms and Conditions of Employment.

An example of behaviour that 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 members of staff are expected to:

> *"Observe all University rules, regulations, codes of practice and policies including but not limited to the Data Protection Policy and the Equality and Diversity Policy".*

3.3 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 University's learning management system. This training must form part of staff induction and must be taken by all staff on an annual basis thereafter.

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

3.4 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 should be aware that access to many sensitive systems is not yet automatically controlled. Therefore managers should make appropriate requests for access, change of permissions or denial of access to the IT Service Desk who will assign the request to the relevant System Administrator to action.

Upon termination, all employees, contractors and third parties must return all University owned information assets and equipment.

It is stated in the general terms and conditions of employment 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".

The full list of terms and conditions can be read at: http://www.bristol.ac.uk/hr/terms/

3.5 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 use of its IT systems is outlined in the Investigation of Computer Use Policy (ISP-18).

3.6 Suspected Misconduct

Where there are reasonable grounds for suspected misuse, as identified in the Investigation of Computer Misuse Policy, the Secretary's Office may authorise that account to be suspended and/or investigated by IT Services.

Employees who, after an investigation, have been found to have breached University Policy or their contract of employment, may be subject to disciplinary action under the Conduct Procedure.

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.

3.7 Interns and Student Hires

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 not acceptable.

3.8 Honorary and Associate Staff

If you are sponsoring honorary or associate staff, consideration must be given to the data they are able to access. Access levels must be appropriate based on the capacity in which they are working with the University.

3.9 Third Party Compliance

Guidance on the engagement with third-parties is outlined in the Outsourcing and Third Party Compliance Policy (ISP-04).

4. Further Guidance

- Conduct procedure for members of staff:

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

- 'Develop' site for mandatory information security staff training: https://develop.bristol.ac.uk/

- 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 Security: http://www.bristol.ac.uk/infosec/data-security/