

# Data Protection Policy

## 1 Introduction

The University needs to collect and use certain information about its employees, students and other people connected with the University in order to fulfil its contractual and legal obligations and to conduct the business of the University. Where this information comprises personal data, the University must comply with the principles set out in the Data Protection Act 1998. In summary, these state that personal data shall:

- Be processed fairly and lawfully and shall not be processed unless certain conditions are met;
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
- Be adequate, relevant, and not excessive for that purpose;
- Be accurate and kept up-to-date;
- Not be kept any longer than is necessary for that purpose;
- Be processed in accordance with the data subject's rights;
- Be kept safe from unauthorised access, accidental loss or destruction;
- Not be transferred to a country outside the European Economic Area, unless that country has an adequate level of protection for personal data.

This policy describes the standards and obligations to be met with respect to the processing of personal data by members of the University.

### 1.1 Status of this policy

It is a condition of employment that employees will abide by the rules and policies made by the University. Failure to follow this policy may therefore result in disciplinary proceedings.

## 1.2 Breaches of policy

Any student or member of staff who considers that this policy has not been followed should raise the matter with the relevant Department or School, and report the alleged breach to the Information Access Officer. If the matter is not resolved, it should be raised as a formal complaint.

## 2 The Data Controller

The University is the Data Controller under the Act. The overall designated controller is the Secretary to Council.

The Information Access Officer, in the Office of the Secretary to Council, is responsible for renewal and update of the University's Notification to the Information Commissioner, handles subject access requests, and provides advice on compliance with the Act. The Information Access Officer can be reached at [data-protection@brunel.ac.uk](mailto:data-protection@brunel.ac.uk).

## 3 Personal data

“Personal data” means any information held by the data controller, which relates to a living individual who may be identified from such data. This includes any expression of opinion about the individual, and any indication of the intentions of the data controller or any other person in respect of the individual.

Anyone who believes the University holds their personal data is entitled to know

- What information the University holds and processes about them and why
- How to gain access to the information
- How they can keep it up-to-date
- What the University is doing to comply with its obligations under the Data Protection Act.

The University provides standard data collection notices for this purpose. These are available on the Intranet. In addition, the student data collection notice is published in the Student Handbook each year.

### 3.1 Conditions for processing personal data

Personal data can only be processed in the following circumstances:

- performance of a contract, e.g., staff contract or enrolment contract;
- compliance with a legal obligation;

- the administration of justice, compliance with statutory requirements or the exercise of public functions carried out in the public interest;
- legitimate interests of the data controller, unless prejudicial to the interests of the individual;
- protection of the data subject's vital interests, i.e., cases of life or death; or
- with the **consent** of the individual.

More specific rules must also be applied to sensitive personal data. Sensitive personal data include health, ethnic origin, political opinions, religion, trade union membership, and criminal convictions. These data must be treated with a high level of security and can be processed only:

- for performance of a legal duty in relation to employment;
- for protection of a data subject's or third party's vital interests;
- where the information has been made public by the data subject;
- in connection with legal proceedings;
- for the administration of justice or compliance with statutory requirements;
- for medical purposes (including pre-employment screening and occupational health records);
- for ethnic or racial monitoring; or
- with the **express consent** of the individual (i.e., consent in writing).

Some jobs or courses may bring applicants into contact with children (people under the age of 18). The University has a duty under enactments to ensure that staff are suitable for the job, and students for the courses offered. The University also has a duty of care to all staff and students and must therefore make sure that employees and those who use the University facilities do not pose a threat or danger to other users.

It is sometimes necessary to process information about a person's health, criminal convictions, race and gender, and family details. This may be to ensure the University is a safe place for everyone, or to monitor University policies, such as the Equal Opportunities Policies.

## 4 Obligations and responsibilities of staff

All staff are obliged to

- Ensure that any information they provide to the University in connection with their employment is accurate and up-to-date, and must inform the Human Resources Department of any changes to information which they have provided, e.g., address, contact details for next of kin, etc.

- Provide information in response to Data Protection censuses and Data Protection audits.

Heads of Schools, Directors of Specialist Research Institutes, and Directors and Heads of corporate services must ensure that any collections of personal data held within their Schools, Institutes or departments are registered within the University with the Information Access Officer, who has the power to require modification or deletion of data to ensure compliance with the Act.

Heads of Schools, Directors of Specialist Research Institutes, and Directors and Heads of corporate services are responsible for ensuring that their staff are acquainted with the requirements of the Data Protection Act 1998. In cases of uncertainty about an issue of compliance, they should contact the Information Access Officer.

In the event of a subject access request, staff must provide all relevant information to the Information Access Officer.

If and when, as part of their responsibilities, staff collect information about other people, e.g., students' coursework, opinions about ability, references, or details of personal circumstances, they must comply with this Policy and any other pertinent policies and guidelines. These are available on both the University Internet and Intranet pages.

## 4.1 Security of personal data

All staff are responsible for ensuring that:

- Any personal data which they hold are kept securely;
- Personal data are not disclosed either orally or in writing, accidentally or otherwise to any third party, without authorisation.

Staff should note that unauthorised disclosures will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal data should

- be kept in a locked filing cabinet, drawer, cupboard or room;
- not be visible to anyone not authorised to see it, either on desks or on computer screens;
- if it is computerised, be password protected (including the use of password-protected screen savers);
- be sent in a sealed envelope, if transmitted through the post, whether internally or externally;
- not be sent via e-mail if it is sensitive personal data.

Personal data **should not** be put on laptops, CD-ROM devices, memory sticks, or other portable media. Staff wishing to use documents or files stored on network drives while off-campus should use VPN (Virtual Private Network) to access such documents or files.

More information on VPN can be obtained from the Computer Centre.

## **5 Obligations and responsibilities of students**

Students must ensure that all personal data provided to the University are accurate and up to date. They must ensure that changes to their personal data, for example, address, name, or contact details of next of kin, are notified to their School office, either on a Student Record Amendment form or through the appropriate Web forms.

### **5.1 Use of personal data by students**

Students who use personal data must comply with the Data Protection Act 1998. Such information should only be held with the express authority of a member of staff such as a lecturer/research supervisor who is responsible for the work being done.

The student should consult with the member of staff to ensure that they are aware of the Data Protection Act requirements, the application of the principles, including the criteria for legitimate processing, and security arrangements for the data. The lecturer/supervisor will provide the Information Access Officer with specifics of the personal data being collected, and their use.

## **6 Rights of access**

### **6.1 Subject access requests**

Everyone has the right of access to personal data that is being kept about them. Any person who wishes to exercise this right in connection to personal data held by the University should complete the Subject Access Request form and send it to the Information Access Officer. The form is available on the internet (<http://www.brunel.ac.uk/about/administration/infoaccess/dataprot/policies>). Details may be required to help identify an individual and the information requested. An administrative charge may be levied on each occasion that access is requested. (For more information regarding fees, refer to the Fees for Subject Access Requests policy (also on the internet).) The University will reply within 40 days of these being received by the Information Access Officer.

Students are entitled to information about their marks for both coursework and examinations; however, this may take longer to provide than other information. The University may withhold certifications, accreditation or references in the event that the full course fees have not been paid, or where all books and equipment have not been returned to the University.

### **6.2 Requests under the Freedom of Information Act**

Information that is already in the public domain is exempt from the Data Protection Act 1998. Additionally, personal data may be released under the Freedom of Information Act. In line with the University's commitment as stated in the Strategic Plan to improve methods of communication, information will be made as freely available within the institution as is possible without compromising the right of individuals to protect their own privacy.

## 7 Retention of data

The University keeps some forms of information longer than others. In line with the spirit of the Act, information will not be kept for longer than necessary. Both paper and electronic records should be kept in accordance with the University's Records Retention Schedule (<http://intranet.brunel.ac.uk/admin/OSR/recman/pdfs/Schedules.shtml>).

## 8 Conclusion

Compliance with the Data Protection Act 1998 is the responsibility of all members of the University. Any deliberate breach of this policy may lead to disciplinary action being taken, access to University facilities being withdrawn, or criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the relevant School or Department, the Information Access Officer, or the Secretary to Council.

## 9 References and further information

- University Internet: <http://www.brunel.ac.uk/about/administration/infoaccess/dataprot>
- Internal policies and registration form: <http://intranet.brunel.ac.uk/admin/OSR/foi/home.html>
- Data Protection Act 1998: <http://www.opsi.gov.uk/acts/acts1998/19980029.htm>