Information Compliance

Data Protection Policy

July 2018

Document properties

Authority

Chief Information Officer

Sponsor

Chief Information Officer

Responsible Officer

Data Protection Officer

Version history

The current version (July 2018) is derived from, and supersedes, the version published in February 2017 and earlier versions.

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 General Data Protection Regulation (GDPR) and the provisions contained in the Data Protection Act 2018. In summary, these state that personal data shall:

- Be processed lawfully, fairly and in a transparent manner and shall not be processed unless certain conditions are met;
- Be collected for specified, explicit and legitimate lawful purposes and shall not be further processed in any manner incompatible with those purposes;
- Be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;
- Be accurate and, where necessary, kept up-to-date;
- Kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data are processed;
- Be processed in a manner than ensures appropriate security of the 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 College, and report the alleged breach to the Data Protection 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 GDPR and the Data Protection Act 2018.

2.1 The Data Protection Officer

The Data Protection Officer is Mary Liddell. She is responsible for

- Informing and advising the University and its staff regarding their obligations under the GDPR and the Act;
- Monitoring compliance with the GDPR, providing training to staff and conducting data protection audits;
- Providing advice regarding data protection impact assessments and monitoring the performance of such assessments;
- Co-operating with the Information Commissioner's Office;
- Acting as a point of contact for the ICO;
- Handling subject access requests.

The Data Protection Officer can be reached by email at data-protection@brunel.ac.uk or by post at

Data Protection Officer
Information Services
Brunel University London
UB8 3PH

3 Personal data

"Personal data" means any information relating to an identified or identifiable natural person, who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

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 GDPR and the Act.

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

Where a form is used to collect personal data, a link to a Privacy Notice is included on the form.

3.1 Special categories of personal data

Special categories of personal data include information which is considered to be, or may be, particularly sensitive. These include

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health
- Sex life
- Sexual orientation
- Commission or alleged commission of an offence
- Proceedings or sentence for an offence.

3.2 Processing

'Processing' means any operation which is performed on personal data, whether manually or by automated means, including

- Collection
- Recording
- Organising
- Structuring
- Storage
- Adaptation or alteration
- Retrieval
- Consultation
- Disclosure
- Alignment or combination
- Restriction
- Erasure or destruction.

3.3 Conditions for processing personal data

Personal data can only be processed in the following circumstances:

- with the **consent** of the individual;
- performance of a contract, e.g., staff contract or enrolment contract;
- compliance with a legal obligation;
- protection of the individual's or another person's vital interests, i.e., cases of life or death;

- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

- for the legitimate interests of the data controller or a third party, unless prejudicial to the interests of the individual.

More specific rules must also be applied to special categories of personal data. These data must be treated with a high level of security and can be processed only:

- with the **explicit consent** of the individual (i.e., consent in writing);

- for the performance of a legal duty in relation to employment, social security and social protection law;

- for protection of an individual's or third party's vital interests where the individual is unable to give consent;

- where the information has been made public by the data subject;

- in connection with legal proceedings;

- when necessary for reasons of substantial public interest;

- for medical purposes (including pre-employment screening and occupational health records);

- for reasons of public health; or

- for archiving purposes in the public interest, historical research, or statistical purposes.

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.

College Deans, Institute Directors, and Directors and Heads of corporate services are responsible for ensuring that their staff are acquainted with the requirements of the GDPR and the Act. In cases of uncertainty about an issue of compliance, they should contact the Data Protection Officer.

In the event of a subject access request, staff **must provide all relevant information** to the Data Protection 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 or in a restricted folder (including the use of password-protected screen savers);
- be sent in a sealed envelope, if transmitted through the post, whether internally or externally;
- be sent as a password protected attachment if it is sensitive personal data and is being sent externally by email.

Personal data **should not** be put on laptops, CD-ROM devices, flash drives, or other portable media if those media are not encrypted. 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 (https://intra.brunel.ac.uk/s/cc/kb/Pages/AnyConnect-VPN.aspx).

5 Staff training

All staff who have a Brunel University London network account, and access to a computer while at work, are required to complete the on-line data protection module *every year*.

Staff who are line managers, or who work with special categories of personal data, must periodically attend a data protection briefing.

6 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 College, either on a Student Record Amendment form or through the appropriate Web forms.

6.1 Use of personal data by students

Students who use personal data must comply with the GDPR and the Act. 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 requirements of the GDPR and the Act, the application of the principles, including the criteria for legitimate processing, and security arrangements for the data.

7 Rights of individuals

Individuals have certain rights with regard to the use of their personal data. These include

- Provision of a privacy notice when personal data are collected
- Right of access to their personal data
- Rectification of inaccurate personal data
- Right of erasure
- The right to restrict the use of their personal data
- Data portability
- The right to object to the use their personal data for some situations
- The right not to be subject to automated decision-making, including profiling.

7.1 Exercising a right

To exercise any of the rights listed above, individuals should contact the University's Data Protection Officer. Contact details can be found in section 2.1 of this document.

With the exception of the provision of a privacy notice, such communication to the Data Protection Officer should include details of the relevant personal information, and proof of identification. The University will reply within 30 days of these being received by the University.

It should be kept in mind that some of these rights are not absolute. Where that is the case, and the University declines to take the action requested, the reasons for the University's decision will be provided to the individual.

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.

8 Offences under the GDPR

There are specific offenses under the GDPR:

- Obtaining, disclosing, procuring the disclosure to another person, or retaining personal data without the consent of the data controller, or selling personal data so obtained;
- Re-identification of de-identified personal data without the consent of the controller;
- Processing re-identified personal data;
- Where a request has been made by an individual for access to his/her personal data, altering that data in any way with the intention of preventing disclosure to the individual.

'De-identified' personal data refers to personal data which has been pseudonymised or anonymised.

9 Requests under the Freedom of Information Act

Information that is already in the public domain is exempt from the GDPR. 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.

10 Retention of data

The University keeps some forms of information longer than others. In line with the spirit of the Regulation, 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 (https://intra.brunel.ac.uk/s/GILO/records/Pages/Retention.aspx).

11 Conclusion

Compliance with the GDPR and the Act is the responsibility of all staff at 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 College or Department, the Data Protection Officer, or the Chief Information Officer.

12 References and further information

- University Internet: http://www.brunel.ac.uk/about/administration/information-access/data-protection
- Data Protection Act 2018: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- General Data Protection Regulation: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
- Information Commissioner's Office: www.ico.org.uk
- Information and Cyber Security: https://intra.brunel.ac.uk/s/cc/security/Pages/default.aspx

