Information Compliance

Handling Staff Personal Data

June 2019

© 2019 Brunel University London

Document properties

Authority

Chief Information Officer

Sponsor

Chief Information Officer

Responsible Officer

Data Protection Officer

Version history

The current version (June 2019) is derived from, and supersedes, the version published in June 2017 and earlier versions.

© 2019 Brunel University London

1 Introduction

The Data Protection Act 2018 (incorporating the General Data Protection Regulation (GDPR)) and the Freedom of Information Act 2000 are the two pieces of legislation that govern access to information about individuals held by the University.

The Data Protection Act is concerned with personal information about an individual, for example, name, address and date of birth, and lays down sensible rules for the handling of personal data. The Act also confers rights on any individual about whom personal information is processed or held. The Freedom of Information Act provides a general right of access, subject to certain prescribed exemptions, to all information such as policies and procedures, committee minutes and papers held by the University.

Each member of staff who handles personal information must not only comply with the requirements of the Data Protection Act 2018 and the Freedom of Information Act 2000 but will be expected to understand that the need for confidentiality extends far beyond the requirements of the Acts, particularly where special category personal information is concerned.

This policy has been developed to support the University's Data Protection Policy and the University's commitment to protecting the privacy and confidentiality of all staff data as far as is reasonably practicable.

2 Executive summary and key points

2.1 Collection and management of staff data

Personal information about staff is collected by the University for a number of purposes, both internal to the University and for external education-related agencies.

Staff handling personal data have a duty to ensure that the information collected

- suits the stated purpose;
- is factual;
- is kept securely; and
- is destroyed in accordance with University and statutory regulations.

2.2 Disclosure of staff personal data

Staff should contact the Data Protection Officer if they have any questions regarding disclosure of personal data.

Staff information should not be disclosed to anyone without proper authority. Examples of information which might be disclosed under the Freedom of Information Act are provided in section 4.3. All Freedom of Information requests should be forwarded to the Data Protection Officer for action.

 © 2019 Brunel University London

2.3 Subject Access requests under the Data Protection Act

Staff members have a right to know

- what information the University holds about them;
- for what purpose(s); and
- to whom such information might be disclosed.

However, the staff member does not have an automatic right to see all the information.

All Subject Access Requests should be forwarded to the Data Protection Officer for action.

2.4 Related policies and further guidance

A list of University policies and other documents affecting confidentiality of staff information is provided in section 6.

An appendix is attached which provides more detailed guidance regarding various types of personal data and their disclosure.

3 Collection and management of staff data

3.1 Collection of data

Information about staff is obtained from University job applications and other forms/documents connected to employment at the University. In addition, some personal data will be collected from referees.

3.2 Purposes for which data are held

The University needs to hold personal information about staff for various administrative purposes, including:

- administration of salary, pensions, sickness and other payments
- academic qualifications
- training and development
- disciplinary and grievance procedures
- academic and research administration
- health and safety
- access to facilities such as the library and computing

© 2019 Brunel University London

- monitoring quality and performance
- security and car parking
- compliance with other legal requirements, e.g., equal opportunities, Disability Discrimination Act, returns to external bodies such as HESA.

3.3 Special category personal data

Certain types of information are considered to be special category data, as the information is sensitive in nature. These include:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- membership of a trade union
- genetic data
- biometric data
- health
- sex life or sexual orientation
- commission or alleged commission of a criminal offence
- proceedings, disposal of proceedings, or results of proceedings against a person for a criminal offence.

Some of these data are collected for use in statistical analyses, particularly by the Higher Education Statistics Agency (HESA). However, for this purpose, the data are used anonymously – there is no connection with a particular person.

3.4 Responsibilities of data users

Each member of staff who has access to other staff members' personal data as part of their job should at all times ensure that:

- data are only used for the purpose(s) for which they were collected
- data confidentiality is maintained at all times
- data accuracy is maintained
- data are held securely – see 3.6 below — Security of data
- only data that are necessary for the conduct of normal University business are retained
- confidential data, whether held in paper format or electronically, are securely destroyed when no longer required.

 © 2019 Brunel University London

Please note that the Human Rights Act 1998, Article 8, states, "Everyone has the right to respect for private and family life, his home and his correspondence".

Any staff member who discloses another individual's personal data without proper authorisation may be subject to disciplinary proceedings.

3.5 Information to be recorded

The contents of all personnel files, whether paper or electronic files, should be limited to documents that reflect normal University business. The content of these documents should not come as a surprise to the staff member.

All information recorded should be **factual**. Judgements, comments or opinions should not be included unless information exists to support those judgements or opinions.

3.6 Security of data

Personal data should be stored securely whether you work in a private or open-plan office, in accordance with the University's Data Protection Policy.

All staff should ensure that personal data are:

- kept in a locked filing cabinet, drawer, cupboard or room, whether it is in paper or electronic format (e.g., CD, memory stick, etc.) when not being worked on or when the office is left unattended (even for a short time)
- not visible, either on desks or on computer screens, to anyone not authorised to see it; you should be aware of your surroundings. Ensure screen savers and computer screen locks are used
- sent in a sealed envelope, if transmitted through the mail, either internally or externally
- properly classified in accordance with the Information Classification Procedure, and sent with appropriate encryption via email, if it is special category information
- not disclosed orally or in writing without the permission of the staff member unless it is part of a legitimate University process
- not left on shared printers/photocopiers
- disposed of securely in line with the Retention and Disposal Policy (https://intra.brunel.ac.uk/s/GILO/records/Pages/Retention-Policy.aspx) whether in paper format or electronically.

3.7 Retention and disposal of information

All staff personal data should be retained in accordance with the University Retention and Disposal Schedules available on the web at: https://intra.brunel.ac.uk/s/GILO/records/Pages/Retention.aspx.

© 2019 Brunel University London

4 Disclosure of staff personal data

If you receive a request for staff information is received that is out of the ordinary, you should pass the request to the Data Protection Officer for action.

Special category personal data **must not be disclosed** without the express consent of the staff member or without proper authorisation.

4.1 Internal disclosure

Personal information should *only* be disclosed to other members of Brunel University London staff if the staff member concerned has given permission or if the disclosure is necessary for the legitimate interests of the University. Personal information must not be disclosed merely for social reasons.

If there is any doubt regarding the identity of the member of staff who is requesting the information, ask them to produce their ID card or check with the Human Resources Department (HR).

4.2 External disclosure

Generally, personal data should not be given out externally, except where there is a legal or contractual requirement to do so, without the permission of the staff member. It is permissible to provide personal data in **emergency** situations (i.e. where the individual's or someone else's life may be in danger).

Personal data should **not** be disclosed over the telephone unless you are certain of the identity of the caller, and that you are authorised to release the information.

Requests for information from the police or other investigatory bodies should be directed to the Data Protection Officer.

4.3 Disclosures under the Freedom of Information Act

Some information which a staff member might consider to be personal data may be disclosed in response to a request under the Freedom of Information (FOI) Act. A determination must be made as to whether the information requested relates to a staff member's **personal** life, or **professional** life. Information relating to a staff member's professional position, duties, expenses, and the like, will normally be disclosed.

Individual salaries will **not** usually be disclosed under FOI. The salary range would normally be provided. The Vice-Chancellor's salary is declared in the Financial Statements.

All requests for information under the Freedom of Information Act should be passed to the Data Protection Officer for action.

All requests for personal information received from the individual person concerned, even if requested under the Freedom of Information Act, will always be dealt with as a Subject Access Request under the Data Protection Act.

4.4 Financial information

Information about an individual staff member's salary and benefits is not normally disclosed to third parties (but see section 4.3 for exceptions to this). Any member of staff who wishes to have access

 © 2019 Brunel University London

to their records held in the Finance Department may do so without charge, by applying directly to that Department.

5 Subject Access requests under the Data Protection Act

Under the Data Protection Act 2018, every staff member has the right to be told whether the University holds personal information about them, to be given a description of those data, the purposes for which they are held and to whom they may be disclosed.

To obtain access to personal data the University may hold, staff members must submit a request specifying which data they would like to have access to, together with proof of identification to the Data Protection Officer (Information Services directorate).

It is the responsibility of the Data Protection Officer to contact relevant areas within the University and to ensure that the information requested is/can be released to the staff member. This must be completed within one month of receiving the request, proof of ID, and sufficient information to find the data requested.

If the request for access to personal data includes access to e-mail, the staff member requesting access must be able to supply the name(s) of the sender or recipient of the e-mail, and a reasonable time frame during which the e-mail was sent or received.

Information contained within the personal data which may identify a third party will usually be redacted prior to allowing inspection of a file or providing a copy of a document. In some cases, a summary of the personal data may be provided instead of a document copy.

6 Related policies and further guidance

Further information can also be found in the following University documents:

- Data Protection Policy
- Freedom of Information Policy and Procedures
- Records Management Policy
- University Retention and Disposal Policy and Schedules
- Electronic Mail Policy
- Network Account Policy
- Council Ordinances

© 2019 Brunel University London

For further guidance:

e-mail: data-protection@brunel.ac.uk

web page: http://www.brunel.ac.uk/about/administration/information-access/data-protection.

© 2019 Brunel University London

7 Appendix A – Types of data and disclosures

7.1 Personnel records

The official personnel record for a member of staff is the one held in the Human Resources Department. A facility is available which allows staff members to update their own personal data. The Department or College in which a staff member is employed may also hold a personnel record, but this should contain a subset of the data in the official record.

The University allows individual staff members to inspect their official personnel file. If the staff member requests copies of any documents within the file, those copies will be provided at that time.

The Equal Opportunities monitoring section of the job application form should be deleted or securely destroyed once the anonymised data have been supplied to HESA and other monitoring organisations.

7.1.1 Confirmation of employment

Banks, prospective landlords and others may require confirmation that an individual is a member of staff at the University. If the request is made by telephone, the caller is advised to put the request in writing to the Human Resources Department.

The Human Resources Department confirms dates of employment over the telephone only if the caller provides the dates.

7.1.2 Training records

Staff Development maintains a list of courses requested and attended by each member of staff. Each staff member can access their own training report for compliance training on the intranet (https://intra.brunel.ac.uk/s/StaffDev/default.aspx.

Staff can also see a list of workshops for which they have registered, or which they have attended, by selecting *Your Records* on the same web page.

7.2 Occupational health records

Disclosure of medical information given by a staff member to medical staff or occupational health advisors is restricted by the Data Protection Act and by the Access to Medical Reports Act 1988. Other than in exceptional circumstances, written consent to the disclosure of such information must be obtained.

These records normally consist of health questionnaires (including pre-employment medical questionnaires), results of any health-related screening or surveillance, GP or specialist reports, reports to management and documentation of any consultations with the Occupational Health Advisor or Physician.

Staff members may provide written consent for access to this information by third parties. However, the Occupational Health Advisor reserves the right to refuse such access if, in his/her opinion, the consent was given under duress.

Line managers do **not** have an automatic right to see this information.

Requests from staff members who wish to see their own occupational health records should be made directly to the Occupational Health provider.

© 2019 Brunel University London

7.3 Financial information

Information about an individual staff member's salary and benefits is not normally disclosed to third parties (but see section 4.3 for exceptions to this). Any member of staff who wishes to have access to their records held in the Finance Department may do so by applying directly to that Department.

7.4 Contact information

Staff members' names, e-mail addresses, and work telephone numbers are considered to be personal data; however, as this information relates to each individual's *professional* life rather than *personal* life, these may be disclosed under some circumstances.

Contact details for Dean, directors, and managers may be disclosed in response to Freedom of Information requests.

The staff telephone directory is **not** a public document. For individuals who are not managers, wherever possible, contact data which are disclosed to third parties should refer to a position rather than an individual's name, and the switchboard or other "group" telephone number should be used rather than an individual's direct-dial number.

Information Services is able to create position-related mail aliases, such as finance-director@brunel.ac.uk and it is preferable to use these in external Web pages and official documents.

Use of a staff member's name, e-mail address, work telephone number or photograph on an external Web page is permitted with the staff member's consent.

Please note that the Information Commissioner considers that there is no conflict with the Data Protection Act where staff members' names appear in the minutes of a meeting.

Individual staff members are, of course, free to disclose their own contact data to third parties as they see fit.

7.5 Personal data in the public domain

The fact that some of a staff member's personal data is in the public domain does not mean that such data can be freely provided to anyone requesting it. Consideration must be given to the manner in which the information was made public. If the information was made public by the staff member, or by the University as part of an official communication, then any subsequent release is unlikely to cause distress. If, however, the information was made public by a third party without authorisation, then further release of the information is considered unfair.

7.6 E-mail

Although a staff member's e-mail address is considered to be personal data (because it reveals the staff member's name and place of employment), the account belongs to the University. Likewise, all e-mail sent to or from a University-supplied account belongs to the University and is considered to be part of official University records. The University e-mail account should not be used for personal e-mail.

University e-mail is subject to disclosure under both the Data Protection Act and the Freedom of Information Act.

If a staff member is on long-term leave, or absence due to sickness, access to their account should be provided to another member of staff who can deal with any incoming messages. If a member of

 © 2019 Brunel University London

staff decides to leave the University's employment, they should delete any unnecessary e-mail from their account prior to their date of departure. E-mail which must to be retained should be forwarded to another member of staff, or saved to the appropriate folder(s) on the Department or College's network drive.

More information about e-mail accounts can be found on the Information Services intranet pages.

7.7 Network files

Like e-mail, files saved to a Department or College network drive or a home-directory network drive are considered to be University records. As such, they are subject to disclosure under the Data Protection Act and the Freedom of Information Act.

Members of staff who leave the University's employ should save any files on their home-directory network drive to the Department or College network drive before departing, or delete them.

7.8 Monitoring

Telephone calls to staff members working in customer service positions may be monitored for training and quality assurance purposes.

7.9 Disclosures to investigatory bodies

Personal data may be passed to the police and other law enforcement or investigatory bodies (such as Local Government Authorities and fraud investigators) where a particular Act places an obligation on the University to provide information (e.g., Taxes Management Act) or a court order has been served.

Schedule 2(2) of the Data Protection Act 2018 does allow the police and other law enforcement bodies to request disclosure in certain situations where it is believed that not releasing the information would be likely to prejudice:

- prevention and detection of crime, including fraud
- apprehension or prosecution of offenders
- assessment or collection of taxes.

Any request for a staff member's personal data from the police or other investigatory body should be referred to the Data Protection Officer, or in his/her absence, the Chief Information Officer, or the Chief Operating Officer.

© 2019 Brunel University London