# Information Compliance

# Handling Student Personal Data

June 2019

# 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 August 2017 and earlier versions.

 

# 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, in this case specifically student 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 student data as far as is reasonably practicable.

# 2 Executive summary and key points

## 2.1 Collection and management of student data

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

Staff have a duty to ensure that the information collected

- suits the stated purpose;
- is factual;
- is kept securely; and
- is destroyed in accordance with agreed University policies and procedures in line with legal record-keeping requirements..

## 2.2 Disclosure of student information under the Data Protection Act

Student information should not be disclosed to anyone without proper authority. Where disclosure is requested by someone external to the University, staff should neither confirm nor deny that the person being asked about is a student here.

 

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

## 2.3 Requests for student information under the Freedom of Information Act

Examples of information which might be disclosed under the Freedom of Information Act are provided in section 5. However, all Freedom of Information requests should be forwarded to the Data Protection Officer for action.

## 2.4 Subject Access Requests under the Data Protection Act

Students 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 student 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.

## 2.5 Related policies and further guidance

A list of University policies and other documents affecting confidentiality of student information is provided in section 7.

Appendices are attached which provide more detailed guidance regarding disclosure to particular people or groups, and disclosure by those services within the University that are bound by a professional code of ethics.

# 3 Collection and management of student data

## 3.1 Collection of data

Information about our students is obtained from UCAS and other Admissions Clearing Houses, from the University application and enrolment forms, and from individual students themselves. The information we collect enables the University to manage an individual student's academic career from admission to graduation, through to alumni and confirming qualifications into the future.

## 3.2 Purposes for which data are held

The University needs to hold personal information about students for various teaching, research and administrative purposes in order to administer their academic career, including:

 

- maintenance of the student record (including personal and academic details) and management of academic processes (for example, academic audits, examination boards and awarding of degrees)
- management of accommodation
- alumni operations, including fund-raising
- provision of advice and support to students via, amongst others, Student Services, personal tutors, Student Wellbeing and Professional Development Centre
- health and safety
- access to facilities such as the library and computing
- internal research, including monitoring quality and performance
- security and car parking
- confirmation of awards
- archiving in the public interest.

Student information is held in a number of different formats (e.g., on the SITS student database, College/departmental files) and various locations.

In addition, the University has a statutory obligation to disclose personal information about students to the Office for Students (OfS) and the Higher Education Statistics Agency (HESA), which is then passed to relevant government agencies that require the information to carry out their statutory functions in relation to the funding of education.

## 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 in 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 Duties of staff

Each member of staff who has access to student 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.

In addition, all staff should be aware of a student's right to privacy in matters relating to his/her health and welfare, and when advising students, staff should make it clear at the outset of a discussion whether the content is to remain confidential and the extent of the confidentiality to be afforded to any disclosures.

In particular, staff should inform the student of the:

- concern on the part of the University to respect privacy, wherever possible;
- circumstances, if any, under which information might be shared with a third party, taking account of the duty of care which may be owed to the individual and/or others; and
- individuals or University departments or other agencies who might be informed in such circumstances.

All staff should also inform a student, at the outset, of any limits to their impartiality imposed by their responsibility as a University employee.

*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 student personal data without proper authorisation may be subject to disciplinary proceedings.

## 3.5 Information to be recorded

The contents of all student files, whether paper or electronic files, should be limited to documents that reflect normal University business and that have either been copied to the student or could be copied without causing any distress.

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 student 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, flash drive, 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 any visitors; 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 internal mail
- 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 student 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 student files 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.

The majority of student data will be destroyed or deleted seven years after graduation. However, some student personal information will be retained indefinitely as part of the University's history so that at a later date, the University is able to provide proof of a student's achievement. Such information, however, should only be disclosed with the student's consent. If, however, it is known that a person is deceased, we would make some personal data, for example, study dates and/or confirmation of awards, available.

# 4 Disclosure of student information under the Data Protection Act

If you receive any request for student information that is out of the ordinary, you should pass the request on to the Data Protection Officer for action.

**You must not disclose** special category personal data without the express consent of the student or without proper authorisation.

## 4.1 Internal disclosure

Personal information should ***only*** be disclosed to other members of Brunel University London staff if you have the student's 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 you do not know 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

Information ***must not*** be given out externally, except where there is a legal or contractual requirement to do so, without the permission of the student. This includes supplying information to parents, legal guardians and next of kin.

If you receive a request via the telephone, you should neither confirm nor deny that the person being asked about is a student at the University. Ask the caller to put the request in writing, or provide their contact details and pass them to the student. Detailed guidance on how to deal with external disclosures can be found in Appendix A.

If confidential information is to be released *without* the student's permission, the permission of the College Dean or Head of Department responsible for the security of that information must be obtained and the student must be informed, except in cases where it is deemed legally inadvisable to do so.

If you are asked to disclose special category personal information regarding, for instance, a student's health or criminal convictions, and you do **not** have the student's permission, you should confine your statement to something like, "I'm sorry, but I am not in a position to comment." In certain cases, it may be necessary for approval to be granted from the Chief Information Officer and/or the Chief Operating Officer or their designated agents before information is released.

# 5 Requests for student information under the Freedom of Information Act

All requests for personal information received from the individual person concerned will always be dealt with as a Subject Access Request under the Data Protection Act.

Any request for **personal** information received from a third party (i.e., someone other than the student) about a student will not be released under a Freedom of Information request.

Student information released under a Freedom of Information request might include, for example, statistical data such as number of full-time/part-time students, age profiles, ethnicity, disabled student retention, student awards, etc., and information that is already within the public domain such as a press release.

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

 

# 6 Subject Access Requests under the Data Protection Act

Under the Data Protection Act 2018, every student 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, students must submit a subject access request, specifying which data they would like to have access to, 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 student. This must be completed within one month of receiving the request and sufficient information to find the data requested.

If the request for access to personal data includes access to e-mail, the student 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.

The only types of documents that a student making a subject access request does not have an automatic right to see, which may be kept on a student's file, are:

- references which are supplied in confidence, which will only be released if the referee has given consent
- examination scripts – any information recorded by a student on an examination script is exempt from a subject access request; however, any comments made by a marker whether or not they are on the script must be disclosed if a subject access request is made. Therefore, it is recommended that any comments and/or opinions are constructive and can be backed up if a subject access request is made. *Please note*: students are entitled to have their marks if they submit a subject access request even if they are in debt, although they will not be provided with their official certificates/transcripts and will not be allowed to attend their graduation ceremony
- document(s) which identify another individual(s).

# 7 Related policies and further guidance

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

- Data Protection Policy
- Records Management Policy
- University Retention and Disposal Policy and Schedules
- University Archive Policy
- ISMS policies and procedures

 

- Senate Regulations

For further guidance:

email: data-protection@brunel.ac.uk

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

 

# 8 Appendix A – External disclosures

## 8.1 Parents/spouses/other relatives

Students' relatives ***do not*** have a general right to information about their child/partner/relative, something which they often assume.

Information can only be provided if the student has given their permission.

If someone claiming to be a parent/spouse/partner or relative contacts the University wanting information, take their details and contact the student and ask them to contact the individual directly.

Do not confirm or deny that the person the caller is asking about is a student.

## 8.2 Sponsors

Sponsors and similar bodies (e.g., LEAs, Embassies, High Commissions, private companies, charities, etc.) ***do not*** have a general right to information about 'their students' personal data, although the University may provide academic information.

If you receive a request from a sponsor, ask them to submit their request in writing. If, on receipt of the request, you are unsure whether to release the information, contact your Head of Department or Data Protection Officer (Information Services).

## 8.3 Schools/colleges

Students' former schools/colleges **do not** have a right to information about their former pupils.

Information can only be provided if the student has given their permission.

If you receive a telephone request from a school, ask them to submit their request in writing and offer to forward their request to the student(s) concerned.

## 8.4 Potential employers

Potential employers of students **do not** have an automatic right to information about our students.

However, if a potential employer, or an agency conducting personnel checks for a potential employer, requests verification of a degree award, this information will be provided, if a release form from the student is included.

The request must be in writing (fax or letter) on headed paper, and must include the student's name and information to be verified, such as the type and subject of the award.

To ensure the information being verified is for the right person, it may be necessary to request the date of birth and/or year of the reward.

If you receive a request by telephone or e-mail, ask the person making the request to submit it by fax or letter.

If there is any question as to the genuineness of the request, you should contact the student and obtain their permission to verify the award.

 

Information other than verification of a degree award will not be provided without the consent of the student.

Potential employers are encouraged to verify the authenticity of a past students award by using the University's online verification system, VerifyAward . The system allows past students/alumni to link and share documents with third parties in a secure and efficient way. Date ranges for available data are as advertised.

Requests for verification of an award will normally be handled by the Awarding Team (awarding@brunel.ac.uk).

## 8.5 Council tax offices

Confirmation of a person's status as a student will normally be made to Council tax offices by the Student Centre.

However, if the person requesting the information is a fraud investigator, or works in a fraud investigation office, then the request should be forwarded to the Data Protection Officer.

## 8.6 Police and other law enforcement bodies

The Police and other law enforcement bodies ***do not*** have a right of access to information except 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.

However, 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
- apprehension or prosecution of offenders
- assessment or collection of taxes.

If the police request information about a student, refer them to the Data Protection Officer. The Data Protection Officer will ask them to submit a data protection form. The form should state:

- the identification of the student about whom they are requesting information
- the information they require
- the reasons why the information is required (one of the purposes outlined in Schedule 2(2) (see bullet points above))
- how the investigation would be prejudiced if the information is not supplied
- what the investigation is about (e.g., a named criminal investigation), and
- the signature of the investigating officer.

Authorisation to release student information must be given by the Chief Information Officer or his/her designated agents (Data Protection Officer or Records Manager) or the Chief Operating Officer or his/her designated agent(s) unless in exceptional circumstances (e.g. someone has committed a serious crime or it is believed a serious crime is about to be committed; or that the

 

person may be a danger to him/herself or others), in which case information may be released directly.

## 8.7 Bailiffs

Bailiffs **do not** have an automatic right to information about our students. Information must only be given if a court order is produced.

If the bailiff produces a court order then information can be provided. However, the bailiff should be directed to the Data Protection Officer or the Head of Security and Emergency Planning. The member of staff who deals with the request will ensure that copies of the information released, together with a photocopy of the court order and bailiff's identification, are kept.

## 8.8 Solicitors and other legal representatives

If a solicitor or other legal representative requests access to a student's file, the request should be forwarded to the Data Protection Officer.

Such requests are normally accompanied by a signed release by the student, and are handled as Subject Access requests.

## 8.9 UK Visas and Immigration

While UK Visas and Immigration (UKVI) (part of the Home Office) **may have** a right to information about our students, it is not an automatic right.

They may request information to determine:

- if a person is enrolled as a student at the University
- if a student is actually attending classes
- if a student has violated his/her visa conditions.

In addition, they may ask for information to determine if a student is involved in terrorism by, for example, belonging to a prohibited organisation.

If UKVI requests information by telephone, you should neither confirm nor deny if the person about whom they are asking is a student. You should ask the caller to make the request in writing, to the Data Protection Officer (Information Services directorate).

## 8.10 Media

Enquiries from the media must be treated with care. Simply confirming that an individual is or has been a student at Brunel University London can be an offence under the Data Protection Act 2018.

All media enquiries should be referred to the University's Press Office who will only release information regarding current and past students if the:

- individual student has agreed that the information can be released
- information is already in the public domain

 

- information is required to be released under the Freedom of Information Act 2000. In this case, information should only be released after consultation and agreement with the Data Protection Officer or Chief Information Officer.

## 8.11 Emergency disclosures

The Data Protection Act 2018 allows for emergency release of information to protect the individual's "vital interests", e.g.:

- disclosure of a known medical condition if a student were unconscious
- serious concerns that a student may harm themselves or others (i.e., where there is serious risk that the University will fail in its duty of care towards the student or other students)
- the student has been in contact with someone who has meningitis or other notifiable disease.

The decision to release information should be taken by the Head of Department/College Dean, the Secretary to Council or the Chief Operating Officer (or their designated agents).

 

# 9 Appendix B – Services bound by a professional code of ethics

## 9.1 Mental health advisors and medical services

Mental health advisors and Medical Services staff will not pass on personal information about a student (including a student's attendance at counselling, disability or surgery appointments) to anyone outside the Service subject to the following exemptions:

- where Student Wellbeing and Medical Services staff have the express consent of the student to disclose the information
- where Student Wellbeing and Medical Services staff would be liable to civil or criminal court procedure if the information was not disclosed
- where Student Wellbeing and Medical Services staff believe the student, or other students or staff within the University, may be in serious danger.

## 9.2 Disability and Dyslexia Service

Disability and Dyslexia Service staff will not pass on personal information about a student's disability/special need to anyone outside the Service (including academic staff) without the express permission of the student.

If the student does not give their consent, this decision will be respected, although the implications in terms of the level of support that can be put in place will be made clear.

## 9.3 Professional Development Centre

The Professional Development Centre staff operate according to the AGCAS Code of Practice on Guidance, and will not pass on personal information about a student without the permission of the student.

## 9.4 International students

All staff who provide guidance to international students will discharge their responsibilities in line with the Council for International Education/AISA code of ethics.