Information Compliance

Handling the Personal Data of Staff and Students

September 2024

(Draft)

Document properties

Authority

University Secretary and General Counsel

Sponsor

University Secretary and General Counsel

Responsible Officer

Data Protection Officer

Version history

The current version (September 2024) is derived from, and supersedes, the version published in June 2019 and earlier versions.

Table of Contents

1 Introduction

The Data Protection Act 2018 (incorporating the UK General Data Protection Regulation (UK 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.

Anyone 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 and Information Access 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 data

Personal information about staff, students and alumni 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

- meets 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 personal data

2.2.1 For staff

Staff should contact the Privacy Team at data-protection@brunel.ac.uk 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 Privacy Team at foirequests@brunel.ac.uk for action.

2.2.2 For students

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 Privacy Team at data-protection@brunel.ac.uk if they have any questions regarding disclosure of student information.

2.3 Subject Access requests under the Data Protection Act

Staff and 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, no individual has an automatic right to see all the information.

All Subject Access Requests should be forwarded to the Privacy Team at data-protection@brunel.ac.uk for action.

2.4 Related policies and further guidance

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

Sections which provide 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 can be found in the appendices:

Appendix A – Types of data and disclosures for staff

Appendix B – External disclosures for students

Appendix C – Services bound by a professional code of ethics

3 Collection and management data

3.1 Collection of data

3.1.1 For staff

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.

3.1.2 For students

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 employees for various administrative purposes and about students for various teaching, research and administrative purposes in order to administer their academic career, including:

- administration of salary, pensions, sickness and other payments
- academic qualifications
- training and development
- employment procedures such as disciplinary and grievance
- academic and research administration
- health and safety
- access to facilities such as the library and computing
- monitoring quality and performance
- security and car parking
- confirmation of awards
- compliance with other legal requirements, e.g., equal opportunities, Disability Discrimination Act, returns to external bodies such as HESA
- 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
- internal research, including monitoring quality and performance
- archiving in the public interest.

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.

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

3.4 Statutory disclosure

In addition, the University has a statutory obligation to disclose anonymised 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. We also use this data to comply with our statutory reporting obligations.

The University also has a statutory obligation to provide information where there is a Complaint Investigation by the independent regulator, the Office for the Independent Adjudicator (OIA). Students can refer an internal complaint outcome to the OIA for independent review.

3.5 Responsibilities of data users

Each member of staff who has access to staff 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.

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 member of staff.

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

3.6 Information to be recorded

The contents of all HR and student files, whether paper or electronic files, should be limited to documents that reflect normal University business and, where applicable, that have either been copied to the student or could be copied without causing any distress. The content of any HR documents should not come as a surprise to the member of staff.

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

3.7 Security of data

Personal staff and 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 individuals 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 any visitors or 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 unless it is part of a legitimate University process
- not left on shared printers/photocopiers
- disposed of securely in line with the Data Protection and Information Access Policy (see Section 4.9.1), whether in paper format or electronically.

3.8 Retention and disposal of information

3.8.1 For staff

All staff personal data should be retained in accordance with the University Retention and Disposal Schedule: Human Resources Retention Schedule.

3.8.2 For students

All student files should be retained in accordance with the University Retention and Disposal Schedule: Student Records Retention Schedule.

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 staff personal data

If you receive a request for staff information that is out of the ordinary, you should pass the request to the Privacy Team at data-protection@brunel.ac.uk for action.

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

4.1 Internal disclosure

Personal information should ***only*** be disclosed to other members of staff of Brunel University London if the member of staff 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 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

4.2.1 For staff

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 member of staff. 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 Privacy Team at data-protection@brunel.ac.uk.

4.2.2 For students

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.

4.3 Disclosures under the Freedom of Information Act

Some information which a member of staff 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 member of staff's **personal** life, or **professional** life. Information relating to a member of staff'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 Privacy Team at foirequests@brunel.ac.uk 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'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 payroll/salary records held in the Human Resources Department may do so without charge, by applying directly to that Department.

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 Privacy Team at foirequests@brunel.ac.uk for action.

6 Subject Access requests under the Data Protection Act

Under the Data Protection Act 2018, every individual, be they staff or 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, individuals must submit a request specifying which data they would like to have access to the Privacy Team at data-protection@brunel.ac.uk. (NB: Any individual external to the University who is neither current staff nor student, **must** submit their request together with relevant proof of identification.)

It is the responsibility of the Privacy Team to contact relevant areas within the University and to ensure that the information requested can be released to the requester. 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 email(s), the employee requesting access must be able to supply the name(s) of the sender or of the email(s), and a reasonable time frame during which the email(s) was/were sent or received.

Information contained within the personal data which may identify a third party will usually be redacted (removing or hiding 3rd party personal information) 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.

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) or parts of 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 and Information Access Policy
- Freedom of Information Policy and Procedures
- Records Management Policy
- University Retention and Disposal Policy and Schedules
- University Archive Policy
- Human Resources policies and procedures
- IT Acceptable Usage Policy
- Council Ordinances

For further guidance:

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

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

8 Appendix A – Types of data and disclosures for staff

8.1 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 to update their own personal data. The Department or College in which staff work may also hold a personnel record, but this should contain a subset of the data in the official record.

The University allows individual staff to inspect their official personnel file. If staff request 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.

8.1.1 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.

8.1.2 Training records

Organisational Development maintains a list of courses requested and attended by each member of staff.

Employees can also see a list of workshops for which they have registered, or which they have attended, by clicking on the *Subscription alerts* icon at the top of their Brightspace account page.

8.2 Occupational health records

Disclosure of medical information given by an employee to medical staff or occupational health advisors is restricted by the Data Protection Act 2018 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 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 who wish to see their own occupational health records should be made directly to the Occupational Health provider.

8.3 Financial information

Information about an individual staff 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 payroll/salary records held in the Human Resources Department may do so by applying to that Department.

8.4 Contact information

Staff 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 Deans, 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 member of staff's name, e-mail address, work telephone number or photograph on an external Web page is only permitted with their consent.

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

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

8.5 Personal data in the public domain

The fact that some of staff 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 member of staff, 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.

8.6 E-mail

Although an e-mail address is considered to be personal data (because it reveals the staff 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 (see the Acceptable Use Policy).

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

If a member of staff is on long-term leave, or absence due to sickness, delegated access to their account can be granted to another member of staff who can deal with any incoming messages for the time that the individual is absent. If this is not actioned before the individual is absent then any access to a personal email account should be cleared with the privacy team, and the manager should provide a business need statement along with a timeline for gaining access. If a member of 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-mails which must be retained should be forwarded to another employee, 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.

8.7 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.

Employees who leave the University's employ should save any files containing information which is related to University business, which are stored on their home-directory SharePoint drive, to the Department or College or project SharePoint drive before departing, or delete them.

Any records stored in One Drive will be deleted when the email account is deleted, except where records management requirements or legal obligations override normal practice.

8.8 Monitoring

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

8.9 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 an employee's personal data from the police or other investigatory body should be referred to the Privacy Team at data-protection@brunel.ac.uk, or in their absence, the University Secretary and Legal Counsel, or the Chief Operating Officer.

9 Appendix B – External disclosures for students

9.1 E-mail

Every Student who studies at Brunel University London will receive a brunel.ac.uk email account. Although an e-mail address is considered to be personal data (because it reveals the student name and place of study), 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 (see the IT Acceptable Usage Policy).

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

9.2 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.

9.3 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 the Privacy Team at data-protection@brunel.ac.uk.

9.4 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.

9.5 Potential employers

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

If a potential employer, or an agency conducting personnel checks for a potential employer, requests verification of a degree award, this information can verify the authenticity of a past student's 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.

If they are unable to access VerifyAward then the request must be in writing (email 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 and the request includes a release form from the student. 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 via another route such as text, , ask the person making the request to submit it by email or letter and they should include a release form from the student.

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.

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

9.6 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 Privacy Team at data-protection@brunel.ac.uk.

9.7 Statutory bodies

The University also has a statutory obligation to provide information where there is a Compliant Investigation by the independent regulator, the Office for the Independent Adjudicator (OIA). Students can refer an internal complaint outcome to the OIA. When students refer to the OIA following their internal complaint outcome, they consent to sharing of relevant and applicable data, which may include special category data. Students are usually copied in to any requests for information from the OIA, and it is their responsibility to withdraw consent should they choose to do so.

9.8 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 Privacy Team at data-protection@brunel.ac.uk. The team 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 University Secretary and Legal Counsel or his/her designated agents (Data Protection Officer or the Head of Records, Archives and Special Collections) 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.

9.9 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 Privacy Team at data-protection@brunel.ac.uk or the Head of Security and Emergency Planning. A photocopy of the court order and bailiff's identification, are kept.

9.10 Solicitors and legal representatives

If a solicitor or other legal representative requests access to a student's file, the request should be forwarded to the Privacy Team at data-protection@brunel.ac.uk.

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

9.11 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 Privacy Team at data-protection@brunel.ac.uk.

9.12 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 Privacy Team or the University Secretary and Legal Counsel.

9.13 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).

10 Appendix C – Services bound by a professional code of ethics

10.1 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.

10.2 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.

10.3 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.

10.4 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.