Information Governance &

Document properties

Authority

Associate Director of Privacy

Sponsor

Chief Governance Officer

Responsible Officer

Data Protection Officer

Version history

The current version (March 2022) is derived from, and supersedes, the version published in July 2018 and earlier versions.

Contents

At a Glance Summary

- This policy applies to any individual that processes personal data on behalf of Brunel University London. Personal data is any data that can identify a living individual.

- The Data Protection Policy is a key part of the Data Protection Strategy that sets out how Brunel's privacy program complies with data protection legislation. You can find our strategy on the Data Protection intranet pages.

- Some personal data is particularly sensitive and must be handled with extra care. This is known as Special Category Data. Data about someone's religion, health or ethnicity for example can only be used when certain conditions have been met. It is unlawful to use Special Category data without satisfying these conditions.

- Complying with data protection legislation is a legal obligation. Complying with this policy is therefore a condition of employment or study at Brunel. Failure to comply with the policy could result in disciplinary action in line with established HR disciplinary processes.

- The use of personal data must comply with the data protection principles. We must ensure that any use of data is **necessary** and **proportionate** and has a clear business purpose.

- All staff must ensure that they keep personal data secure and follow the obligations of this policy in order to:
    - Prevent the loss of personal data
    - Prevent unauthorised access to or disclosure of personal data
    - Prevent the loss of access to personal data

- If any of these three things happen it could be a **personal data breach** and must be reported to the Data Protection team as soon as reasonably possible, including where necessary out of hours. The Data Protection team will assess the risk associated with the personal data breach and determine what action to take.

- Everyone has rights about how their personal data is managed. Requests to exercise rights can be submitted in any way and staff should alert the Data Protection team as soon as practical if they receive a query.
- Data Protection can be a complex area of law and we don't expect anybody to be an expert. If you need any assistance with anything in this policy, or with any processing of personal data, you can contact the Data Protection team on data-protection@brunel.ac.uk.

- Provide advice on Data Protection Impact Assessments
- Act as a contact point with Supervisory Authorities

The Data Protection Officer is not responsible for carrying out tasks that are required to ensure the university compv9J0.001 Tc sory( )0.66(y)73Tw 30 y

ensure that changes to their personal data, for example, address, name, or contact details of next of kin, are notified to the relevant programmes' office, either on a Student Record Amendment form or through the student e-vision portal.

Use of Personal Data by Students

Students who use personal data are subject to the obligations of this policy. Any use of personal data by a student must have a clear and specific purpose and be limited to what is necessary. Where a student volunteers to work or is paid to work for Brunel and is required to access our systems as part of that role, the access must be strictly limited to only what is necessary for their role. Before access is provided, they must be provided a copy of this policy and understand that misuse of the personal data within Brunel systems, may constitute a criminal offence. If access to systems is required for greater then one month the student must attend a data protection workshop.

Security of Personal Data

All staff are responsible for ensuring that:

- Any personal data which they hold are kept securely in line with Information Services and INFOSEC polices.
- Personal data are not disclosed either verbally or in writing, accidentally orotherwise to any third party, without authorisation.
- When you are using personal data in a paper form, it must be kept in a locked filing cabinet, drawer, cupboard, or room.
- Personal data must not be visible to anyone not authorised to see it, either on desks or screens.
- Wherever possible, personal data must be password protected or in a restricted folder. The password should be known only to those that need to access the data, and should be changed, if the password becomes common knowledge.
- Where data is to be shared by post, the data should be sent in a sealed envelope. When sending post externally, if it contains personal data, it should be sent by recorded delivery.
- Any personal data shared electronically should be shared via approved and supported systems including Brunel Dropoff, Teams, OneDrive, or SharePoint in the first instance, as this method of sharing has been configured in a way that is compliant with legislation. OneDrive or SharePoint should be the default sharing method when sharing of data is to take place **internally.**
- If sharing via OneDrive or SharePoint is not possible, personal can be sent as an email as long

as the following safeguards are in place:

- If being sent to an **external** third party, any email that contains personal data should be encrypted

- Obtain access to documents, emails or other personal data that may be in scope of an information rights requests.
- Review data to establish if an exemption applies.
- Consider the applicability of any relevant exemption.
- Make disclosures required to fulfil our obligations relating to information rights.

Any individual that is impacted by a request, e.g., the data protection team need to request a search for the emails of a specific member of staff, will unless circumstances prevent it, be informed of the existence of a rights request, and asked to supply any relevant information or data as soon as is practical. If co-operation is not provided or the individual concerned is off sick or on leave, the Data Protection team, may seek to access the required information through a formal request to Information Services. Any request for access will be strictly limited to what is necessary to fulfil the rights request, and detailed records will be maintained.

Exercising Information Rights

If an individual wants to exercise an information rights request, they are entitled to do so verbally or in writing. It is important to note that rights requests can be submitted to

Retention of Personal Data

The University keeps some forms of personal data longer than others. In accordance with the storage limitation principle of the legislation, personal data can only be retained for as long as it is necessary in order to achieve the purpose for which it was collected. There are two drivers for retention of personal data

1) A legal requirement that sets out a statutory retention period or
2) A justified business need for the retention of personal data

The retention period assigned to a piece of personal data can vary on a variety of factors,

- Systematic monitoring
- Processing Special Category data
- Large scale data sets
- Matching datasets to identify trends
- Vulnerable participants (children, lack of capacity, victims of crime, power imbalance etc.)
- Innovative techniques (AI/ML some genomics)
- Processing that limits rights.

Complying with this Policy

This policy applies to all staff and students, and every effort should be made to ensure that it is read and understood. Compliance with the