Information Governance & Compliance

Data Protection Policy

March 2022

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.

Introduction

The University needs to collect and use a wide range of information about its employees, students and other people connected with the University in order to fulfil its contractual and legal obligations and to conduct the general business of the University. Where this information comprises personal data, the University must comply with the principles set out in the UK General Data Protection Regulation (UK-GDPR) and the provisions contained in the Data Protection Act 2018.

This policy sets out how Brunel University London meets its data protection obligations. All staff and students are expected to comply with the obligations within this policy in order to ensure that the university meets its legal obligations.

Scope

This policy applies to any individual or organisation that processes personal data for, or on behalf of Brunel, or another business affiliated with our activities.

Processing of personal data occurs when an action is carried out on the personal data to complete a function. The terminology used in this policy and some key definitions are provided in Annex A of this document.

Data Protection Principles

The Data Protection Principles set out what we must do to comply with the law. These principles must be followed whenever we process personal data. Further advice and guidance about how to apply these principles can be found on the Data Protection intranet and internet pages or by attending data protection workshops which cover a variety of important data protection topics and how to apply this policy in practice. The principles apply to Brunel **and** any organisations or people to whom we send personal data.

Lawfulness, Fairness and Transparency: We must have a lawful reason to collect and use data about people. That reason must be fair and not cause harm or distress and we must have mechanisms in place to tell people what we do with their data.

Purpose Limitation: We must only collect and use personal data for clear and specific purposes. We cannot use data for alternative purposes that are not compatible without informing people.

Data Minimisation: We must only collect the personal data necessary to achieve the purpose. We should not collect more data then needed where it's not required for that purpose or "just in case" it becomes necessary.

Accuracy: We must have controls in place to be able to update data and ensure it is accurate where necessary.

Storage Limitation: We must retain personal data only for as long as it is necessary for us to achieve our purposes. Where it is no longer needed because we have fulfilled our purposes, we should take steps to either

delete the personal data, anonymise the personal data or archive the data if it is in the public interest for us to do so. (Please see the section on records retention for further information).

Integrity & Confidentiality: We must ensure that we have controls in place to keep personal data secure, including preventing unauthorised or unlawful access or use of the data and against accidental loss, destruction, or damage to that data.

Accountability - We must be able to demonstrate how we comply with the above principles by ensuring that we have documented processes, procedures, and policies in place for staff to follow.

Roles & Responsibilities

All staff have a role to play in ensuring that we can comply with the legislation. The following sections set out how the responsibilities are assigned

Overall Responsibility

The Council have overall responsibility for compliance with data protection law. They have delegated responsibility for oversight and monitoring of the effectiveness of the university privacy program of the Information Assurance Board.

The Role of the Information Assurance Board

The Information Assurance Board (the IAB) has responsibility for monitoring the strategic effectiveness of the privacy program. This is achieved by:

- Identifying high risk activities and ensuring controls are embedded that mitigate those risks
- Assessing our level of compliance against privacy Key Performance Indicators
- Monitoring our level of training and awareness compliance
- Promoting the data protection strategy at Senior Leadership level.

The Role of the Data Protection Officer

The university has a legal obligation to appoint a Data Protection Officer to monitor how the Brunel complies with the legislation. With the support of a Data Protection team, the Data Protection Officer role involves the following tasks:

- Provide advice and support on all data protection matters to support the university in complying with the legislation
- Monitor compliance with the legislation

- 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 complies with the legislation, their role is to ensure that the university has the necessary tools and oversight required to demonstrate compliance.

The Role of the Data Protection Champions

The university utilises Data Protection Champions to act as voluntary contact points for the Data Protection team. The Data Protection Champions have undertaken in depth training on key data protection concepts and can offer general advice and support to staff within their areas. The Data Protection Champions can also escalate issues or questions to the Data Protection team. Details of the Data Protection Champions for specific areas are available on the intranet. The Data Protection Champions will have regular opportunities to meet with the Data Protection team to discuss issues but can choose to opt out of the initiative at any time.

Obligations & Responsibilities of Staff

All staff have an obligation to ensure that their use of personal data complies with the law. Using personal data in a way that is not compliant with the legislation could constitute a personal data breach or in some circumstances be considered a criminal offence.

- Only use personal data to the extent that is necessary for you to fulfil your role.

- Do not store or use personal data that you access as part of your role for your own personal or commercial purposes.

- Do not access or use personal data that you are not permitted to use outside of the scope of your role without permission from the university.

- Ensure that the use of personal data is fair. Consider whether the use of that data is reasonably expected by the person about whom we are collecting the data.

- When obtaining personal data, we have a legal obligation to be transparent about how we collected it, where we got it from and how it will be used. The university meets this transparency obligation by using privacy notices. The processing you undertake must be covered by a privacy notice that is easily accessible and provided to the person about whom you want to collect data **before** it is collected.

Obligations & Responsibilities of Students

Students must ensure that all personal data provided to the University are accurate and up to date. They must

ensure that changes to their personal data, for example, address, name, or contact details of next of kin, are notified to 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 by clicking on the “encrypt” button when creating a new message and following the on-screen instructions.
- If an email contains an attachment and the attachment contains personal data, the attachment must be password protected.

The acceptable use of email is covered in more detail in our Email policy.

Personal data should not be held on any laptops, CD-ROM devices, flash drives, or other portable media or personal device if the device or portable media are not encrypted. Staff wishing to use documents or filesstored on network drives while off-campus should use VPN (Virtual Private Network) to access such documents or files.

More information on VPN can be obtained from the Computer Centre (https://intra.brunel.ac.uk/s/cc/kb/Pages/AnyConnect-VPN.aspx).

Data Protection Training

Anyone who uses or accesses personal data as part of their role must undertake data protection training annually. Data Protection training is delivered by the Data Protection team using a variety of formats including:
- General sessions
- Role specific workshops
- Intranet content
- Seminars
- Detailed technical sessions
- Bespoke training

The type of training required depends on the role you have within the university and the type of data involved. If you are carrying out processing that could be considered a high risk, for example you process lots of special category data or data that is highly confidential, bespoke training is mandatory as the general training sessions will not cover in specific detail, issues associated with higher risk activities. General sessions will be held at least once a month and can be attended by booking on to the relevant course that is listed on the Organisational Development pages of the Intranet.

Sharing of Personal Data

The sharing of personal data both internally and externally will occur for a variety of purposes. All sharing of personal data must be limited to what is necessary and proportionate to achieve a specific business purpose. Any sharing with external organisations on a routine basis must:

- Be subject to a written contractual agreement
- Have relevant data protection clauses within the contract

The Data Protection team are available to review data protection clauses within contracts and can be sent these by email to data-protection@brunel.ac.uk.

Sharing in Emergency Situations

Data Protection legislation contains specific provisions for sharing personal data in emergency situations including:

- Protecting life or preventing loss of life
- Providing emergency medical support (including disclosing allergies)
- Referring people to emergency support services

In such cases all staff are permitted to share the personal data necessary with any external organisation including the emergency services. It is important that you let the data protection team know as soon as practical that the data sharing has taken place and we will record it.

Information Rights

Everyone has rights with regards to how Brunel uses personal data about them. The rights are:

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

The rights are not absolute, and each right is subject to certain exemptions. Each rights request will be assessed on an individual basis and be processed by the Data Protection team. In order to ensure that the university can fulfil its statutory obligations in relation to information rights requests, The Data Protection team have been given the authority to:

- Obtain cooperation and assistance for dealing with rights requests.

- 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 **any department or communications channel of the university** including shared mailboxes, any front facing teams, line managers or via social media. Any staff that receive any query relating to data protection should contact data-protection@brunel.ac.uk as soon as practical.

Data Protection Offences

Data Protection legislation contains a number of scenarios that would constitute a criminal offence. Any individual found to have committed one of these offences is liable to be prosecuted by the Information Commissioners Office and subject to an internal investigation could be subject to disciplinary action including dismissal. Any investigation will assess the scope and the risk of the alleged offence and will be conducted in conjunction with the HR disciplinary process. The offences under the legislation are:

- Accessing, obtaining, disclosing, or using personal data for your own purposes, or for the purposes of another individual outside of the scope of your role without permission.

- Deliberately attempting to re-identify personal data that has been de-identified outside the scope of your role without permission.

- Using re-identified personal data for any purpose outside the scope of your role without permission.

- Acting to deliberately alter data, or prevent its legitimate disclosure by deleting, moving, removing, or otherwise suppressing disclosure once a request has been made by an individual for access to his/her personal data.

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, but you should consider the above drivers as a starting point. The retention periods for the university are set by our Records Team who are responsible for maintaining university records, archives, and special collections. You can find out more information on the retention periods for university data by visiting our records management pages on the intranet.

Data Protection and Research

Delivering world leading research is one of the core strategic aims of the university. Data Protection legislation supports the use of personal data for scientific and historical research providing a number of exemptions that don't apply to other processing activities. The exemptions provided are only available under certain circumstances and significant work is required to implement the appropriate safeguards required to ensure that the exemptions apply. Not applying the safeguards would be considered a breach of the legislation, the Data Protection policy and could give rise to a research misconduct claim.

Obligations of Research Staff, Students and Research Supervisors

Any staff member involved in carrying out or supervising staff or students responsible for carrying out research that includes the use of personal data must:

- Ensure that ethical approval has been obtained
- Ensure that the research does not cause harm or distress
- Only uses the minimum amount of personal data necessary for the purpose of the research
- Ensure that any consent for processing of personal data is collected and meets the GDPR standard.
- Apply minimisation techniques including pseudonymisation and anonymisation as soon as is practical
- Carry out a Data Protection Impact Assessment if the research is considered high risk and focuses on any **two** of the following parameters:
    - Evaluation or scoring of responses or characteristics
    - Tracking location
    - Risk of harm in the event of a breach
    - Automated decision making

- 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 obligations within this policy is fundamental to the success of our privacy program and the protection of personal data. If you are unsure about how this policy impacts you, or how to comply, you can contact the Data Protection team on data-protection@brunel.ac.uk