Data Protection Strategy

2021-2023

Brunel University London

Document properties

Authority

Associate Director of Privacy

Sponsor

Chief Governance Officer

Responsible Officer

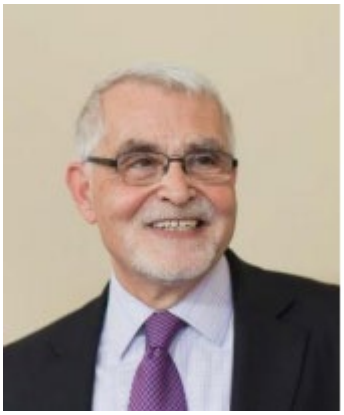
Data Protection Officer

Version history

Version	**Author**	**Comments**	**Date**
0.1	Associate Director of Privacy	Initial Draft for comment	20/07/2021
0.2	Associate Director of Privacy	Amendments following consultation	17/09/2021
0.3	Associate Director of Privacy	Proofing prior to approval	10/10/2021
1	-	Formal approval by the Information Assurance Board	12/10/2021

Contents

Foreword



As a leading HE institution both nationally and internationally, we are trusted with a vast amount of personal data about our staff students and the wider Brunel community. While data driven decision making and innovative technologies continue to drive developments in pedagogic design and play an increasingly important role in our strategic thinking, we must strive to ensure that people trust us with their data and have the assurance they need that any personal data that we collect, or use will be done fairly and in a way that complies with our legal and regulatory obligations.

The university has developed a Data Protection strategy and embarked upon a programme of work to ensure that we can demonstrate compliance, build trust, and ensure that people can exercise their legal rights in a way that is straight forward and transparent. While non-compliance with data protection legislation has a range of reputational, financial, and commercial consequences, the impact that poor practices have on those affected can be far more serious. By delivering this strategy we are committing to respecting peoples fundamental right to privacy and ensuring that we consider data protection in all business processes that involve personal data.

Professor Michael Spyer

Chair of Council

Introduction

The protection of personal data and how organisations ensure that an individual's right to privacy is respected has become a significant strategic objective of all businesses including those within the Higher Education sector in recent years.

The introduction of the General Data Protection Regulation (the GDPR) and the Data Protection Act 2018 have placed a significant legal obligation on Brunel University London to ensure that we:

- Are accountable, responsible, and transparent in our use of personal data.
- Have policies, processes and procedures in place that effectively allow data subjects to exercise their information rights and be able to exercise control of their data.
- Embed controls to ensure the security and confidentiality of personal data and to protect it from loss, unauthorised access, misuse, and corruption.
- Ensure that the collection, use, storage and sharing of personal data is necessary and proportionate for the purpose for which it was collected, and its use complies with the data protection principles.

Failure to comply with the obligations set out in the legislation present significant risks of non-compliance and could limit the ways in which we can lawfully operate. Non-compliance with our legal requirements may result in financial penalties and enforcement action from the UK regulator for data protection, the Information Commissioner's Office.

While regulatory enforcement action would be damaging for the University, we would also suffer negatively from the reputational damage caused by a loss of trust that follows a data breach and the risk of harm or distress to the people who trust us to protect their personal data.

In order to ensure that we can comply with the requirements of data protection legislation and appropriately protect the personal data we use across the university, the Governance, Information & Legal Office have developed a robust privacy program to ensure compliance with the law utilising a pragmatic, risk-based approach to how we manage personal data.

This strategy sets out the core elements of the framework that when fully embedded, will ensure that privacy and the protection of personal data is considered as part of our business-as-usual activity and has a place in all of our information processes.

Scope

This strategy, the privacy framework and associated policies, procedures and processes apply to Brunel University London as Data Controllers. In addition, this strategy and the contents of the framework also apply to:

- All individuals who have access to systems, software or information repositories that contain personal data.
- All personal data processed, in any format, by the University pursuant to its operational activities.
- Internal and external processes used to process personal data.
- Third parties that provide services to the University and process personal data on our behalf.

Roles & Responsibilities

Compliance with the GDPR and associated laws is the responsibility of any staff member or student that processes personal data in the scope of the legislation.

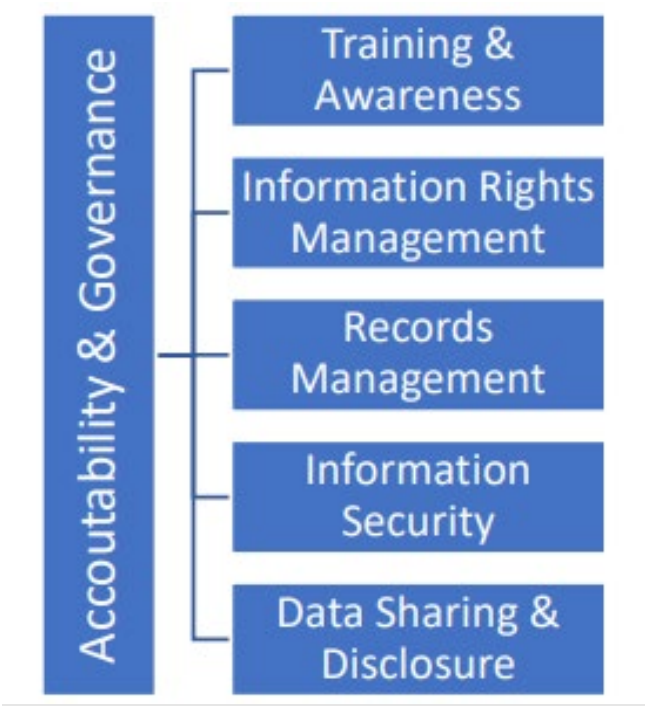
Management of the privacy program is the responsibility of the Data Protection team which will also monitor compliance and provide the appropriate support, advice, tools, and resources for staff to use. A detailed description of roles and responsibilities, as well as a framework of agreed service levels under which the data protection team will operate are set out in Annex B of this strategy.

Aim

The aim of this strategy is to support and enable planning and governance to effectively manage personal data provided to the university as an asset, ensuring that data is collected, created, stored, and processed in a compliant manner that is also in the best interests of the wider University.

Guiding Principles

This strategy is underpinned by guiding principles that are set across six strategic themes that the University has adopted in order to fully comply with the legislation. The strategic themes are set out below:



Accountability & Governance

The GDPR contains a legal requirement for Brunel to be accountable for the decisions we make about how we use personal data. The Accountability principle requires us to proactively demonstrate how we comply with the data protection principles. To meet this requirement, the University, with the support of the University Council will:

- Promote a culture of respect for privacy and the protection of the personal data of everyone associated with Brunel University London through the work of a dedicated Information Assurance Board which monitors our level of compliance with the legislation and has the authority of the University Executive to effectively manage data protection risks and ensure the level of risk is proportionate to the university risk profile

- Review the Accountability Framework published by the Information Commissioner's Office and work with Colleges, Research Centres, Academic Partnerships and Services to assess our current level of compliance using the published accountability tracker to review and embed the relevant controls that will enhance the overall level of assurance the university can offer when complying with the accountability principle of the UK GDPR.

- Implement university wide data protection polices, processes and procedures to ensure that working practices operate in line with the legislation.

- Ensure that appropriate information about our data protection practices and our controls is publicly available and transparent, giving data subjects clear information about how we protect their personal data and how they can exercise their rights.

- Make clear the responsibilities of all staff and students who use personal data as part of their role or activities by ensuring that our training and awareness activities focus on our core processing, all relevant data protection policies are communicated and enforced, and processes and procedures are documented and circulated.

- Identify and mitigate areas of concern or non-compliance within existing codes of practice published by the Information Commissioners Office (ICO) by ensuring that the Data Protection team produce briefing notes that communicate risks, and proposals for mitigation.

- Undertake regular Information and Data Protection Audits in collaboration with the Data Protection Champions across the University to identify and document high risk and non-compliant processing activities.

- Implement an internal governance structure that allows us to respond rapidly with data protection issues. Using a set of metrics designed to monitor our level of GDPR compliance, we will identify and respond to data protection issues promptly within a defined period of time.

- In collaboration with our Cyber Security and INFOSEC teams, build data protection and privacy controls into the design phase of all new projects and procurement activities and ensure privacy is considered as a priority for all existing systems.

- Collaborate with our existing data processors and suppliers to ensure that where they are acting on our behalf, they can meet their own legal obligations set out in the GDPR.

- Embed due diligence processes on all prospective data processors or joint data controllers to ensure that the University has the appropriate level of assurance when sharing personal data for use by third parties.

Training & Awareness

The ability to demonstrate that the institution provides clear and dedicated data protection training to its staff is a core requirement in demonstrating ongoing GDPR compliance. The training must ensure that all staff understand their responsibilities both generally around data protection but also on a more role specific basis based on particular risks associated with a business function.

As well as training for staff and students we are required to ensure that we create and maintain material that provides people with information relating to their rights in accordance with the GDPR including specific obligations around transparency. To meet our training and awareness obligations the Data Protection team will:

- Develop a comprehensive data protection training program for all staff and students that includes:
    - Content designed to act as an introduction to data protection and our obligations.
    - Training to cover specific risks and scenarios.
    - A dedicated intranet site with resources and tools to offer guidance and support.
    - Learning and development sessions focusing on data protection issues encountered by the Data Protection Champions.

- Deliver College, Service and Research specific briefing sessions to inform of specific privacy risks and provide best practice advice.

- Provide centralised access to current best practice guidance and resources via a dedicated intranet which will be regularly updated.

- Promote best practice in how to comply with the GDPR using existing communication channels for both staff and students as well as specific focus groups and the Data Protection Champions.

- Actively demonstrate our commitment to the importance of good data protection and adherence by communicating regular reminders and helpful information about topical issues.

- Ensure that all Data Protection Champions receive Continuous Professional Development opportunities to strengthen their understanding of Data Protection.

Records Management

Good records management practice is required across the University in order to comply with the need to only keep personal data for as long as necessary and to ensure that Brunel:

- Can locate the right personal data in response to Information Rights requests.
- Ensure that data quality and governance are fit for purpose in data driven projects and that the personal data being used is necessary and proportionate for the purpose.
- Protect its information from accidental loss, destruction, or modification.
- Ensure information is secured against unauthorised access and disclosure.
- Preserves its records for future use where there is a public interest.

The volume and format of information that we process is significant, complex and consists of archived, manual, and electronic records. Regardless of format, the University are required to have oversight of the location, type, category, and purpose of processing of the data for the duration of its lifecycle from inception to destruction. In order to attain a greater degree of compliance with our data protection obligations relating to records management Brunel must:

- Ensure that data protection requirements are embedded within our records management policies and procedures.

- Maintain retention schedules for our use of personal data that reflects the purpose for processing and the appropriate retention schedule based on the nature and scope of the personal data used for that purpose.

- Ensure that processes that are in place are effectively communicated and followed in order to manage personal data held in our electronic systems that has met the retention criteria set out in the specified retention schedule. Processes for the destruction/erasure of personal data, the amendment of the retention period and archiving of personal data in the public interest should be in place.

Information Security

Ensuring that we can protect personal data and ensure its security and confidentiality regardless of its context is essential for maintaining the trust and confidence of the people who trust us with their data. In order to comply with the security requirements of data protection law, Brunel must ensure that we implement appropriate technical and organisational measures into new and existing systems to ensure ongoing information security of both our electronic and manual processing activities. The security of information within our systems is managed by our Cyber and Information Security team while physical security is overseen by the Commercial Services Directorate. Archiving and Records manage the security controls in place to protect our archives.

Our Cyber & INFOSEC strategy make clear that the security of personal data is of core strategic importance to university operations. As part of this strategy, we maintain an Information Security Management System that is aligned to ISO27001 which acts as an internationally recognised standard in ensuring information security of information assets.

While the work of our cyber security team and data protection team over-lap in many areas, the data protection team are specifically responsible for ensuring that the organisational and technical controls in place to protect the security and confidentiality of personal data are sufficient to meet our legal obligations set out in the GDPR including the mandatory obligation to report on personal data breaches. To achieve these requirements, we will collaborate with our colleagues across departments in Information Services (IS) and beyond to:

- Review and advise on the technical and organisational controls in place to protect the security and confidentiality of personal data in Brunel's electronic systems that are already in place or considered for implementation as part of the procurement or project management processes. Such advice will consider the nature and scope of the processing involved, the type and sensitivity of the personal data within the system, the type of technology or processes available and the cost of implementation.

- Ensure that all university projects that intend to make use of personal data undergo data protection checks to embed privacy controls at the design stage (Privacy by Design and Default).

- Carry out Data Protection Impact Assessments on new processing activities to ensure that data protection risks are identified, documented, and mitigated to within established tolerance limits.

- Develop and disseminate a standardised Personal Data Breach notification and Personal Data Breach incident handling process that enables the University to meet its mandatory breach notification and documentation obligations.

- Review our list of suppliers and data processors to ensure that where Brunel is considered the Data Controller, we can offer assurance that they are meeting their own specific security obligations by carrying out an appropriate level of due diligence.

Information Rights

Within the GDPR, are a set of information rights that every data subject has when they give their personal data to Brunel. These rights are fundamental human rights which give everyone greater control over how the university manages their personal data and Brunel must have controls in place to ensure that we can allow people to exercise these rights effectively. The information rights are:

1) The right to be informed about how personal data will be used by the university using tailored Privacy Notices.
2) The right to access copies of the personal data Brunel holds about an individual.
3) The right to rectification of incorrect or inaccurate personal data.
4) The right to erasure of personal data in some circumstances.
5) The right to restrict processing of personal data in some circumstances.
6) The right to data portability of personal data from one organisation to another organisation in some circumstances.
7) The right to object to the processing of personal data in some circumstances.
8) Rights in relation to automated decision making and profiling.

It is a core responsibility of the University to ensure that data subjects have the ability to exercise these rights and that we can handle all such requests efficiently, in line with our legal obligations. As part of the privacy program, we are required to:

- Ensure that any data subjects that use our services are fully informed of their rights and freedoms.
- Audit and update existing Privacy Notices for all types of processing activity within Brunel whether the personal data belongs to staff, students, visitors, alumni, or academic partners.
- Review our information rights processes to ensure our ability to investigate and comply with requests.
- Review the purpose and legal basis for processing the personal data we hold to ensure that the rights that are available correspond to the lawful basis we use for processing personal data.

- Review our marketing practices to ensure that we can meet our obligations around consent, explicit consent (where required) and the removal of consent.
- Identify any areas of automated decision making or profiling and ensure that these activities are carried out in accordance with our obligations around transparency and the protection of rights and freedoms.

Data Sharing

As a collaborative institution with a global reputation, the sharing of personal data plays an essential role in our ability to provide our services, undertake world leading research, promote growth, and offer a world class education to our students both domestically and internationally. While the sharing of personal data between the university and other organisations is likely to be business critical in many scenarios, the sharing of personal data must be done in a way that respects the privacy of individuals and be carried out in line with specific provisions on data transfers and sharing. To ensure that the sharing of personal data is lawful, Brunel must:

- Incorporate Information Sharing Agreements into all new supplier contracts that require sharing of personal data.
- Ensure that a data protection due diligence process is created and embedded for all new suppliers, partnerships, collaborations, or third-party service providers that will process personal data supplied by Brunel as a Data Controller.
- Where data sharing is to be subject to transfer outside of the European Economic Area, or it is considered to involve significant risk, implement Standard Contractual Clauses into our contracts and Terms of Business.
- Where the data sharing taking place meets the criteria for the mandatory completion of a Data Privacy Impact Assessment, this will be identified as early as possible ideally at the design or specification gathering stage to give enough time for this to be completed.

Intended Outcomes

Implementing of this strategy and its inherent goals and objectives, will result in the following outcomes:

- The university will benefit from increased transparency and accountability in its data practices which will enhance the trust and confidence of our stakeholders.
- The university will be able to demonstrate significant assurance that its GDPR compliance program is fit for purpose and has the strategic approach necessary to achieve a high level of compliance with data protection legislation.
- The university will reduce the risk of personal data breaches and the resulting enforcement action from the Information Commissioners Office.

Delivering the strategy

Delivering the data protection strategy is the key to ensuring that Brunel can provide a robust data protection compliance program which will help us comply with the law while enabling the university to make better use of its data. By fulfilling the objectives of this strategy, we will reduce the risk of data breaches occurring and reducing the subsequent risk of enforcement action, financial penalty, loss of income or opportunity to work with collaborative partnerships, reputational damage and a loss of trust and confidence in Brunel to operate lawfully and with accountability.

The Information Assurance Board (IAB) are tasked with providing oversight with regards to how the key objectives within this strategy are met. Key metrics will be reported to the IAB on a quarterly basis to allow monitoring of the compliance program.

Responsibility for operational delivery of this strategy sits within the remit of the Data Protection team.

Ensuring that the university complies with the requirements of the legislation is the responsibility of every member of staff. Compliance with the legislation will be achieved by adhering to all policies, procedures and processes relating to data protection. Annex A sets out the roles and responsibilities of university staff in order to ensure effective compliance of the GDPR. Further details can be found in the Data Protection Policy.

Annex B sets out the specific roles and responsibilities of the data protection team and the agreed service levels we will follow.

Annex A: Roles & Responsibilities

Compliance with the GDPR and Data Protection Act 2018 is the responsibility of the university as a whole with every member of staff, and any student that processes personal data having an important role to play. This Annex sets out the roles and responsibilities for ensuring compliance with the legislation

Role	Responsibilities
Information Assurance Board	The Information Assurance Board has oversight of the GDPR compliance program as a whole and is responsible for providing the resources required to ensure that the program is fit for purpose. The focus of the IAB for the duration of this strategy is to ensure that Brunel has the accountability controls in place in order to provide assurance to the University Council that we comply with the legislation. The IAB reports progress of the strategy and significant data protection issues or events to the University Executive.
Associate Director of Privacy	The Associate Director of Privacy has responsibility for delivering a privacy program that achieves the objectives of this strategy and ensuring that the data protection team effectively monitors compliance with the legislation.
Data Protection Officer Data Protection Team	See Annex B
Data Protection Champions	The Data Protection Champions (DPC's) are the first points of contact for data protection queries that cannot be answered using the resources available on the intranet or internet. The DPC's work with the Data Protection team on a range of issues including: • Providing best practice advice relating to data protection queries relevant to their areas.

	• Acting as a contact point for reporting and investigating personal data breaches. • Completing Legitimate Interest Assessments and Data Protection Impact Assessments. • Advising on Privacy Notices. • Periodically reviewing the processing that takes place within the DPC's area and working with the Data Protection team to complete information mapping questionnaires where new processing is identified. • Highlighting training opportunities
Management Staff	Any member of staff with line management responsibilities is responsible for: • Ensuring that the personal data held by their department is kept securely and used properly, within the principles of the GDPR and Data Protection Act 2018. • Advising the Data Protection team or delegated representative of the types of personal data held in their College, Research area or Professional Service, and of any changes or new holdings. • Notifying the Data Protection Officer of any instances that could be considered a breach of the legislation. • Ensuring that any advice, guidance, or instruction issued by the Data Protection Officer, or delegated authority in terms of data protection compliance are given due consideration and where appropriate, passed down to team level for action.

	• Ensuring that all staff or where appropriate, students receive data protection training. • Ensure that where necessary, staff are provided with resources required to complete mandatory data protection activities including responding to information rights requests and Data Protection Impact Assessments
Brunel Staff	All staff that process personal data are responsible for: • Only processing personal data for the purposes explicitly required for their role. • Ensuring that data they are responsible for is kept securely and protected against unlawful processing, accidental loss, damage, or destruction. • Attending data protection training if any part of their role could involve processing personal data. • Reporting known or suspected breaches of data protection to their immediate line manager. • Ensuring that any processing of personal data takes place within the limits of Brunel's Privacy Notices and complies with our policies. • Notifying the Data Protection team if they wish to use an application, system or service that is not supported by Information Services that will involve the processing of personal data.

	• Using the templates and resources produced and available on the intranet and internet sites.
Brunel Students	• Students must ensure that all personal data provided to Brunel is accurate and up to date. They must also ensure they notify the University promptly about changes to any of their data (such as a change of address). • Students who use Brunel computing facilities may process personal data as part of their studies. If personal data is processed, students have a responsibility to ensure that all processing is in line with the data protection principles.
Staff responsible for scientific and historical research and archiving in the public interest. This includes full time records management staff, researchers, research fellows, PhD students and post- doctoral researchers	Where personal data is used for the purpose of scientific, or historical research, statistical purposes or for archiving purposes in the public interest, the researcher is responsible for: • Ensuring that where appropriate the appropriate ethical approval has been obtained. • We have the appropriate documented consent in place for research participants • The participants have been provided with the relevant privacy notice so that they understand how their data will be used and there right to withdraw consent at any time.

Annex B: Role of the Data Protection Team

The Data Protection team plays a key role in ensuring that the university complies with the requirements of the legislation. It does this by:

- Producing policies, processes and procedures that allow the university to operate within the boundaries of the law.
- Providing training and advice to all staff to ensure that they understand what their roles and responsibilities are when processing personal data.
- Working with the university when a data subject exercises their information rights to ensure that requests can be met within statutory limits.
- Investigating reports of data breaches and working with stakeholders to manage and reduce risks.
- Working with regulators and data subjects to respond to breaches and complaints.

While the Data Protection team are responsible for providing the tools and resources that help the university comply with the law, it is not directly responsible for ensuring overall compliance, which instead rests with the university as a whole.

In order to ensure that the Data Protection team can provide an efficient level of service to the rest of the institution and to data subjects, we have put the following service levels in place for our most common services and these will be assessed as performance metrics which will be reported to the Information Assurance Board on a quarterly basis. This list is not exhaustive.

Service Levels

Service	**Target Response Time *** * - statutory requirement	**Prerequisites**
Provision of general advice	Two working days for acknowledgement One week for the provision of detailed advice.	All emails will be acknowledged within two working days. Where detailed advice is required, meetings will be arranged to discuss and formal advice
Data Protection Training (General Overview)	1 week turnaround from initial request	1 hour session. Minimum of 5 people per session
Data Protection Training (Role Specific)	2-week turnaround from initial request	1–2-hour session. Minimum of 5 people per session
Contract review and feedback on Data Protection clauses	1 - 3 week turn around depending on the complexity and value of the contract	Contracts are legally binding on the institution. Sufficient time must be provided to

		ensure that any changes can be considered by all parties. Feedback provided merely as a “tick box” exercise - i.e., the contract has already been agreed without prior input from the Data Protection team will be recorded and the contract signatory accepts the risk of any compliance issues identified. The Data Protection team cannot sign contracts on behalf of the university.
Data Protection Impact Assessment Advice (DPIA’s)	Acknowledgement within 3 working days and sign posting to DPIA resources	DPIAs are live documents that evolve as a project progress. The Data Protection team will work with project stakeholders throughout the process but cannot sign off a project as compliant
Record of Processing Activity Logging	1 month	The university is required to keep a record of the processing it undertakes. The Data Protection team will regularly review the work it has received and update our records on a monthly basis.
Data Breach investigation	48 hours after initial report*	The Data Protection team will work with all parties to determine the scope, severity and the risk caused by any data breaches.
Information Rights process management	Acknowledgement 2 working days after initial submission of a request	* Information rights must be responded to within one calendar month of a valid request. Where the request

	Formal response within 1 month* of valid request being received.	is complex this can be extended by an additional two months.
Legitimate Interest Assessment Drafting/Review	2 weeks after initial request	The lawful basis for processing must be considered as Legitimate Interest and fall outside of the scope of existing Assessments
Privacy Notice Drafting/Review	2 weeks after the initial request	Bespoke privacy notices can be complex. All new privacy notices will be drafted using the standardised Brunel template.
Data Sharing Agreement Drafting/Review	2 weeks after the initial request	As with contracts, Data sharing agreements are legally binding and must be agreed before sharing of personal data can take place.