Document properties

Authority

Associate Director of Privacy

Sponsor

Chief Governance Officer

Responsible Officer

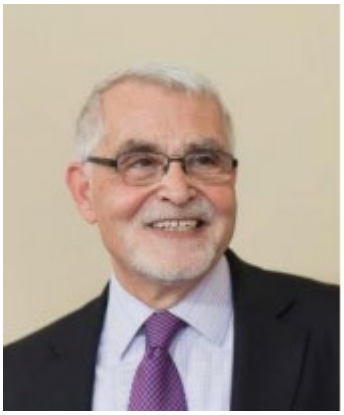
Data Protection Officer

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

- 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

Accountability & Governance

- 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.

x

- 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.

## Annex A: Roles & Responsibilities

Compliance wam he esGesRom romoa anen es e 2018 es he esromeesensan 7.5 (t)317 (y)6.6 esof he esvromes a Tc 0 TwTd (

| | |
|---|---|
| | x Acting as a contact point for reporting and investigating personal data breaches.<br>x Completing Legitimate Interest Assessments and Data Protection Impact Assessments.<br>x Advising on Privacy Notices.<br>x 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.<br>x Highlighting training opportunities |
| Management Staff | Any member of staff with line management responsibilities is responsible for:<br>x 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.<br>x 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.<br>x Notifying the Data Protection Officer of any instances that could be considered a breach of the legislation. |

| | |
|---|---|
| | x Ensuring that all staff or where appropriate, students receive data protection training.<br><br>x 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 |

| | |
|---|---|
| | x Using the templates and resources produced and available on the intranet and internet sites. |
| Brunel Students | x Students must ensure that all personal |

## 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 * <br> * - statutory requirement | Prerequisites |
|---|---|---|

ensure that any changes can be considered by all parties. Feedback provided