Information Governance & Compliance

Data Protection and Information Access Policy

Document properties

Authority

Data Protection Officer

Sponsor

University Secretary and Legal Counsel

Responsible Officer

Data Protection Officer

Version History

The current version (April 2024) is derived from, and supersedes, all earlier versions of any Brunel Data Protection and Freedom of Information policy.

Version 1.0

Document Control

Version	Author	Date	Comments
0.1	Head of Privacy	14/03/2024	First draft circulated
0.2	Head of Privacy	18/03/2024	Amendments on the permanent archiving of records
0.3	Head of Privacy	20/03/2024	Amendments to statements around retention of data for archive purposes.
0.4	Head of Privacy	04/04/2024	Amendments to statement of responsibility to reflect University language and structure.
1.0	Head of Privacy	08/04/24	Approved - IAC

Contents

1 Introductory Purpose and Background

Brunel University London ('BUL') is committed to protecting the rights, privacy and security of Personal Data relating to employees, students and other third parties in accordance with Data Protection Legislation.

BUL is Controller in respect of Personal Data and will determine how Personal Data is Processed.

This Policy promotes transparency, accountability and the safeguarding of an individual's privacy rights and sets out the minimum standards which must be complied with by BUL and its employees when Processing Personal Data. It outlines BUL's responsibilities under Data Protection Legislation and applies to all Personal Data Processed by BUL irrespective of the format or media on which that Personal Data is stored or who it relates to.

2 Scope

This policy applies to any individual or organisation that processes Personal Data for, or on behalf of BUL or another business affiliated with our activities, including employees, students, and third parties working for or on behalf of BUL (such as honorary/associates, hourly paid lecturers). It is important that all employees and students ('you' / 'your') understand the scope of Data Protection Legislation. It is your responsibility to familiarise yourself with this Policy which explains how you should carry out your role or research to ensure compliance with Data Protection Legislation.

BUL, as a public body, has the responsibility to provide other forms of information upon request. BUL is subject to the requirements of the Freedom of Information Act 2000 and the Environmental Information Regulations. This requires us to disclose the information requested unless it is covered by one or more exemptions, which are applied on a case-by-case basis. Data Protection Legislation works alongside the FOI/EIRs principles, protecting personal data. The principle of fairness and transparency, as well as accountability underpin BULs approach to responding to information requests.

Compliance with this Policy is mandatory and failure to comply with this Policy or its associated Policies and Procedures may result in disciplinary action. Non-compliance with this Policy and related Policies / Procedures may also result in damage to the BUL's reputation, financial loss, and legal and regulatory non-compliance.

3 Definitions

Anonymised	The process of permanently removing or altering certain identifying information from data in such a way that it can no longer be attributed to an individual directly or indirectly and ensures that the individual cannot be re-identified.
Consent	Agreement which must be freely given, specific and informed in terms of an indication of the Data Subject's wishes to Process Personal Data relating to them.

Controller	The organisation who determines when, why and how to Process Personal Data.
Data Protection Legislation	The UK GDPR and DPA 2018 as updated and re-enacted from time to time and applies to the processing of Personal Data.
Data Subject	A living individual about whom we hold Personal Data.
DPA 2018	The UK Data Protection Act 2018 which supplements the UK GDPR.
DPIA	Data Protection Impact Assessment, which is an assessment used to identify and reduce risks of Processing and is carried out as part of Privacy by Design.
DPO	The Data Protection Officer appointed by BUL and who is BUL's main representative on data protection matters.
EIR	Environmental Information Regulations 2004
FOI	Freedom of information Act 2000
ICO	Information Commissioner's Office – the UK Supervisory Authority and regulator for data protection and information access legislation.
Lawful Basis	One of the lawful bases set out in UK GDPR Articles 6, 8 and 10, as relevant. This could be contract, legal obligation, protecting vital interests, task carried out in the public interest, a legitimate interest or the data subject has given their Consent. Processing of Personal Data will only be legal if it is necessary and there is a lawful basis for processing.
PECR	Privacy of Electronic Communications Regulations 2003 (PECR) which applies to marketing carried out through email, text or other electronic methods.
Personal Data	Information relating to a Data Subject, who can be identified directly or indirectly from that information. Personal Data can be factual (such as name, email address) or an opinion about that person's actions or behaviour. It does not include anonymised data.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

Privacy by Design	Implementation of appropriate technical and organisational measures in an effective manner to comply with the UK GDPR and safeguard individual rights.
Privacy Notices	Notices setting out information provided to Data Subjects when Personal Data is collected. These generally take the form of a notice to specific groups (such as employees, students, etc.).
Processing or Process	An activity that involves the use of Personal Data including the obtaining, recording or holding of that data or carrying out any operation or set of operations on that data which can include organising, amending, retrieving, using, disclosing, erasing or destroying it.
Pseudonymisation / Pseudonymised	Replacing information which directly or indirectly identifies an individual with one or more artificial identifiers so that person cannot be identified without additional information which is kept separately and secure.
Special Category Data	Personal Data where additional safeguards apply, these include information revealing, racial or ethnic origin, religious or similar beliefs, physical/mental health conditions, sexual life/sexual orientation, biometric/genetic data, political opinions, trade union membership, and data relating to criminal offences/convictions
UK GDPR	Data Protection Act 2018 and Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 No. 419, as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020, which incorporate into UK law an amended version of the EU GDPR ("UK GDPR"), (as supplemented by section 205(4)) of the DPA 2018.
We	Brunel University London (BUL

4 Policy

4.1 Key Principles

If you are Processing Personal Data on behalf of BUL you must observe and comply with the six principles of the Data Protection Act 2018 and Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 No. 419, as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020, which incorporate into UK law an amended version of the EU GDPR ("UK GDPR"), other information rights legislation and the common law on confidentiality, which are:

a. Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency)

b. Collected only for specified, explicit and legitimate purposes (Purpose Limitation)
c. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed (Data Minimisation)
d. Accurate and where necessary kept up-to-date (Accuracy)
e. Not kept in a form which permits identification of data subjects for long than is necessary for the purpose for which the data is processed (Data Limitation)
f. Processed in a manner that ensures its security using appropriate technical and organizational measures to protect against unauthorised or lawful processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality)

There is an additional principle that makes sure BUL can demonstrate compliance with Data Protection Legislation by ensuring that we have documented processes, procedures and policies in place.

BUL must also have a lawful basis as a condition for processing personal data and information. No lawful basis is better than another, but their use depends on various factors. There are six lawful bases in total:

a. Public task
b. Vital interests
c. Legal obligation
d. Contract
e. Consent
f. Legitimate interests

Public task, consent and legitimate interests will be the most commonly used lawful bases in BUL, but all can be applied to our data. See Annex I for full description of lawful bases for processing.

BUL must also ensure that Personal Data is not transferred outside the UK (and EEA) to another country without appropriate safeguards being put in place. (see paragraph 4.5.2).

4.2 Key roles and responsibilities

All Employees, Students, Contractors and visitors to BUL have a responsibility to keep Personal Data and other information confidential, safe and well-managed.

BUL's Executive Board (EB) has overall responsibility to ensure BUL meets its legal and regulatory responsibilities under Data Protection Legislation and to ensure compliance with this Policy. The Information Assurance Committee (IAC) is responsible for overseeing the maintenance, implementation and performance of this Policy.

Faculty Pro-Vice Chancellors, Directors of Professional Service Departments and Line Managers are responsible for ensuring employees within their respective areas, including all new employees, are aware of this Policy and for ensuring that their employees undertake data protection training. Each Director of Service is responsible for promoting and modelling best practice regarding data protection within their teams and keeping the DPO informed of changes in the collection, use, and security measures used for the processing of Personal Data within a college, service or unit. To support this requirement, the Privacy Team will engage and support BUL staff to act as Data Protection Champions responsible for promoting best practice and reporting issues within their own departments.
All employees and research students who process Personal Data are responsible for

complying with Data Protection Legislation and attending data protection training as required.

BUL has appointed a Data Protection Officer (DPO), to assist BUL in the monitoring and compliance of its obligations under Data Protection Legislation. BUL's DPO is the Head of Privacy, and you can contact them at data-protection@brunel.ac.uk.

The DPO is the first point of contact for Supervisory Authorities and for individuals whose data is processed.

BUL is registered with the Information Commissioner's Office as a Controller. Our registration number is: Z6640381.

4.3 Accountability

The Controller (BUL) must demonstrate compliance with the data protection principles which means having adequate resources and controls in place including:

a. Appointing a suitably qualified and experienced DPO, providing them with adequate support and resource
b. Integrating data protection into internal documentation such as Policies, Procedures and other best practice guidance.
c. Providing regular training on data protection and retaining a record of those employees who undertake that training
d. Ensuring, where Processing is identified with sufficient risk to the rights and freedoms of Data Subjects, BUL carries out an assessment of those risks by undertaking a Data Protection Impact Assessment (DPIA) – see paragraph 4.7.3
e. Regularly testing measures implemented and conducting periodic reviews to assess compliance across BUL.

4.4 Key considerations of this policy

4.4.1. What Personal Data do we process?

BUL processes Personal Data, from which an individual can be identified either directly or indirectly, to meet its educational purposes. This includes the collection, organising, recording, using and reusing, sharing, storing, archiving and destroying in line with agreed records retention schedules any data that identifies an individual.

4.4.2. Information Rights

Under Data Protection Legislation everyone has the following rights:

a. The right of **access** to their own data – the right to ask BUL for copies of their Personal Data
b. The right of **rectification** – the right to ask BUL to rectify personal information that is inaccurate or incomplete.
c. The right to **erasure** – the right to ask BUL to erase their own personal information in certain circumstances and where we do not have a legal requirement to hold information
d. The right to **restrict processing** – the right to ask BUL to restrict the processing of their own personal information in certain circumstances

e. The right to **object to processing** – the right to object to the processing of personal information in certain circumstances
f. The right to data **portability** – the right to ask that BUL transfer their personal information to another organisation, or to them, in certain circumstances
g. The right in relation to preventing **automated decision making and profiling**, in certain circumstances

For more information on data protection rights, who to contact if you want to make a request or have a complaint or concern about the accuracy, retention or processing of personal information, please contact data-protection@brunel.ac.uk.

If an individual is unhappy with how BUL has processed their data and dealt with any complaints they are able to complain to the ICO. They can do this by visiting https://ico.org.uk/for-the-public/how-to-make-a-data-protection-complaint/.

The right to **restrict processing** and the right to **erasure** are not absolute rights and BUL will consider all requests against business or legal requirements. This includes considering which information will be held for archiving purposes or in the public interest.

A request for a copy of Persona Data (Data Subject Access Request), can be made verbally or in writing, including via social media. A valid request is from an individual asking for their own Personal Data and can be made to any part of BUL or any employee of BUL, they do not need to use a specific form of words, refer to legislation or direct the request to a specific contact. **Any requests for personal data access must be forwarded immediately to the Privacy Team (data-protection@brunel.ac.uk), as we have a limited amount of time to respond.**

A request for information under FOI/EIR legislation must be made in writing, but can be made to any part of BUL or any employee, they do not need to use a specific form of words, refer to legislation or direct the request to a specific contact.

Any request for information must be forwarded immediately to the Privacy Team (data-protection@brunel.ac.uk), as we have a limited amount of time to respond.

4.4.3. Fair processing notices

Where BUL acts as a Data Controller, we will provide information about how we process the Personal Data of subjects and our purposes for processing that data. We will also identify circumstances under which transfers take place and provide information about routine disclosures to other parties and recipients.

BUL's General Privacy Notice and Copyright Statement is available on our website.

4.5. Sharing and transferring Personal Data

4.5.1. Data sharing

BUL may share Personal Data either within the University or with an external third party provided it has identified one or more valid lawful bases for processing.

BUL will only share Personal Data we hold with third parties, such as our service providers,

where:

a. There is a need to know for the purposes of providing contracted services and a written contract is in place.
b. Where the third party complies with required data security standards, policies and procedures and puts adequate security measures in place
c. Where the transfer complies with applicable data protection legislation

Sharing of Personal Data must be set out in relevant privacy notices provided to the Data Subject.

Where you are looking to share Personal Data with a third party, please discuss with the Privacy Team by contacting data-protection@brunel.ac.uk.

4.5.2. International data transfers (transferring data outside of the UK)

The UK GDPR restricts data transfers to countries outside the United Kingdom to ensure the level of protection afforded to individuals' Personal Data is not undermined. Where data is transferred outside the United Kingdom this is referred to as a 'restricted transfer' and Personal Data may only be transferred where:

a. There are UK adequacy regulations that cover the country or territory where the data receiver is located
b. Appropriate safeguards are in place such as standard contractual clauses issued by the ICO or a certification mechanism applies

BUL must ensure that Data Subjects will continue to have a level of protection that is in essence equivalent to that under Data Protection Legislation. This is achieved by BUL undertaking a risk assessment (Transfer Risk Assessment) which considers the protections, safeguards and legal framework of the destination country.

Where a restricted transfer is not covered by UK adequacy regulations or an appropriate safeguard, it can only take place where it is covered by one of the limited exceptions set out in Article 49 of the UK GDPR:

The Data Subject has provided consent to the transfer, after they have been informed of potential risks.

The transfer is necessary for one of the reasons set out in the UK GDPR such as performance of a contract (occasional and not regular transfers), public interest, to establish, defend or exercise legal claims or to protect the vital interests of the Data Subject (where they are incapable of giving consent), and in some cases, our legitimate interests.

If you are looking to transfer Personal Data outside the UK you **MUST** speak to the Privacy Team and / or the DPO at data-protection@brunel.ac.uk.

4.5.3. Direct Marketing

BUL is subject to specific rules and privacy laws when it comes to marketing its students, alumni and other data subjects. Electronic marketing is subject to the additional rules imposed

by the Privacy of Electronic Communications Regulations 2003 (PECR). Consent is required for electronic marketing (for example, email, text, etc). If you are collecting data for one purpose and intend to also use it for marketing activities, you must provide the option to 'opt-out' at that point and in each subsequent message the right to object to marketing (i.e. change their marketing preferences) must be specifically stated. A record of when consent was obtained, for what purposes, and if consent is withdrawn or unsubscribed from marketing communications, is maintained centrally by Marketing, Communications and Recruitment, and this should be updated promptly.

There is an exception to the explicit consent requirement, and that is for individual students who are currently undertaking a course at BUL and we are marketing services/activities/similar courses or services to them. They must be given the opportunity to 'op-out' of marketing, regardless, and have the right to object to marketing processing. This does not prevent them from being communicated with administrative support during their time with BUL.

BUL should not undertake direct marketing to any individual who is not an existing student or has an existing relationship (commercial/contractual) without the individual's consent.

4.5.4. Marketing and automatic profiling

Automated decision-making, including profiling, is a key part of organisational operations. Profiling is an important tool which can help to tailor content for individuals and make decisions about them.

BUL's approach to profiling is that an individual's personal information must only be used in a compliant, transparent, fair and responsible manner. We do not use profiling to make decisions about students and their access to services.

Creating and applying profiles to individuals to market to them is the most common reason for using profiling. Profiling can also be used for recruitment, research, and statistical analysis. There are statutory requirements under Article 22 of UK GDPR that govern how an organisation may carry out profiling which BUL complies with to process data and information in this way.

4.5.5. Research exemption

Some data protection rules do not apply where Personal Data is being used for research purposes. This applies where the following conditions are met:

a. Appropriate technical and organisation safeguards exist to protect the data, such as data minimisation, pseudonymisation, or access controls
b. There is no likelihood of substantial damage/distress to the Data Subject as a result of the processing
c. The research will not lead to measures or decision taking would prevent or seriously impair the research purpose.

Where the above conditions apply, the following applies:

a. Personal Data originally collected for another purpose can be used for research and retained indefinitely

b. The right of individuals to access their Personal Data does not apply if the research results ae made public in a form which does not allow them to be identified (anonymised)
c. The right of rectification, erasure, restriction and objection do not apply.

4.5.6. Publication of Brunel University London Information

As a public authority subject to the Freedom of Information Act 200, it is the policy of BUL to make public as much information about the University as possible. In particular, the following personal data will be available for public inspection via our website, annual accounts or by submission of a Freedom of Information Request:

a. Names of members of BUL Boards and Committees (including Council and Senate).
b. Names and job titles of staff members. This may include academic and/or professional qualifications.
c. Organisation diagrams
d. Awards and Honours (includes Honorary Graduates and prize winners).
e. Graduation programmes and video or other media versions of graduation ceremonies.
f. Information within prospectuses (including photographs), annual reports, staff newsletters and campus news etc.
g. Staff / Student information on the BUL intranet (including photographs).
h. Staff names and role information on the BUL website.

4.5.7. Records and Archiving

As a public authority we hold archive records that contain may personal data because they're judged to be a vital addition to Brunel's corporate memory, or because they relate to our Collecting Policy in some other way. The collection contains a wide range of material that has been selected for permanent preservation because of its enduring evidential and historical value to Brunel as an institution. The Brunel Archives also hold, for public interest, student information to support and evidence any award verification requests made to BUL's Awarding Team.

The Brunel University London Archives contain an historic record from 1798 to date. They have been maintained and accumulated from wide range material, including internal transfer, an acquisition or a deposit / donation from an external done, such as the British and Foreign Schools Society collection. (see our Archives and Special Collections Policy for more information)

4.5.8. Law enforcement requests and disclosures

In certain circumstances, personal data will be shared without the knowledge or consent of a Data Subject. This is the case where the disclosure of personal data is necessary for any of the following purposes.

a. The prevention or detection of crime
b. The apprehension or prosecution of offenders
c. The assessment or collection of a tax or duty
d. By the order of a court or by any rule of law

If BUL or a known third-party processes personal data for one of these purposes, then it may

apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice a potential investigation.

If any BUL employee receives a request from a court or any regulatory or law enforcement authority for information relating to personal data held by Brunel, the request must be directed to the Head of Security and Campus Safety and/or Data Protection Officer.

4.5.9. CCTV

BUL is committed to maintaining a safe and secure environment across all its campuses through the implementation of Closed-Circuit Television (CCTV) installations. Our comprehensive surveillance system encompasses static cameras, body-worn cameras, and cameras equipped with advanced number plate recognition technology in key areas such as carparks.

BUL CCTV installations are multifaceted, aligning with BUL's commitment to safety and security. These include:

g. Safeguarding the well-being of our staff, students, visitors, and the valuable assets of the BUL community is our top priority.
h.
i. Deterring criminal activities, as well as investigating and detecting disciplinary offenses in strict accordance with University disciplinary procedures.
j.
k. Supports the apprehension and prosecution of offenders in both criminal and civil proceedings.
l.
m. Continuous monitoring of our premises enhances overall security, allowing for timely responses to potential threats or incidents.

CCTV footage is held in line with BUL's Campus Support Retention Schedule.

4.6. The Consequences of non-compliance

Breaching Data Protection Legislation can lead to fines and or claims for compensation in addition to the reputational risk of negative publicity for BUL and risks to our colleagues and students.

A failure to comply with the principles set out in this policy may amount to a disciplinary offence and may be addressed through the relevant procedures which includes, but is not limited to, the Disciplinary Policy and Procedures and University Regulations.

4.7. How compliance with this Policy will be measured

4.7.1. Reporting personal data breaches

Personal Data Breaches or suspected Personal Data Breaches must be reported to the Privacy Team without delay as soon as they are identified. BUL is required to notify the ICO within 72 hours of a breach incident being identified where it poses a high risk to the rights and

freedom of individuals. The decision to report to the ICO will be taken by the Data Protection Officer.

If you are aware of or suspect a Personal Data Breach, do not attempt to investigate the matter, immediately report to the DPO/Privacy Team though the data breach form or contact data-protection@brunel.ac.uk. You should preserve all evidence relating to the incident, ensuring it is secure and that any immediate steps to stop the data breach are implemented and recorded.

Failure to report a Personal Data breach could lead to disciplinary action against you. Compliance with this Policy is vital to ensure any Personal Data Breach is dealt with promptly to protect an individual's Personal Data.

Some common examples of events leading to personal data breaches include (but are not limited to):

a. Misdirected emails or documents
b. Inadequate disposal of information
c. Physical information lost or left unprotected (such as bank cards, passports, confidential correspondence)
d. Leaving IT equipment unattended when logged-in to a user account without locking the screen to prevent others accessing information
e. Loss or theft of laptop, mobile device or USB
f. Physical security e.g. forcing of doors or windows into a secure area or restricted information left unsecured in an accessible area
g. Unauthorised use of a BUL systems and information i.e. hacking
h. Virus or other malicious (suspected or actual) security attach on IT equipment systems or networks
i. Disruption to, failure of loss of access to information or services due to fire, flood, power outage, cyber-attack, theft or any other disruptive action that prevents access to Personal Data.

BUL has in place appropriate procedures to deal with a Personal Data Breach and it will notify the ICO and/or Data Subjects as required. You **must** observe and comply with BUL's Data Breach Procedure.

4.7.2. Privacy by Design

Privacy by design should be a key consideration in the early stages of any project and/or process change and should continue throughout its lifecycle. It allows us to identify and minimise data privacy risks, as well as building trust with employees, students, alumni's and anyone else who works with us. By designing projects, processes, products and systems that incorporate privacy principles, BUL ensures that:

a. Potential privacy problems are identified early
b. Privacy and data protection practice is embedded, and good practice remains at the forefront of everyday activities
c. Projects, processes, products and systems are more likely to meet the legal obligations and less likely to breach privacy legislation
d. Actions are less likely to be privacy intrusive and have a negative impact on individuals

To help ensure privacy by design, a risk assessment must be carried out at an early stage for any proposed new system or an existing system or process that is being significantly changed where personal information is being collected or shared.

4.7.3. Data Protection Impact Assessments (DPIA)

A Data Protection Impact Assessment (DPIA) identifies any risks to personal information or data because of the new or changed system or process and identify any mitigations to those risks. Cost is not a factor - the relevant consideration is whether a proposal involves the processing of personal data. If personal data is to be used to any extent, the proper use and safeguarding of that data needs to be considered. A DPIA will assess:

a. The nature, scope, context and purpose of the processing
b. Necessity, proportionality and compliance measures
c. The risks posed in terms of likelihood and severity of risk to individuals, identifying additional measures to mitigate risks

A DPIA should always be conducted when implementing new systems and technology or business processes change programmes, including:

a. Use of new technologies (systems or processes) or changing technologies
b. Large scale processing of special category and protected characteristics data
c. Large scale and systematic monitoring of publicly accessible areas.

Where you are responsible for implementing or managing a project that may require a DPIA, you should speak to the Privacy Team (data-protection@brunel.ac.uk). Where one is required, a DPIA must be completed before the commencement of a project or implementation (go live) of a new system.

4.7.4. Interest Tests

A risk assessment will also be applied where there is the intention to reuse collected personal information for additional purposes, for which consent has not been sought. In this instance a Legitimate Interest Assessment (LIA) would be carried out to ensure that the rights and freedoms of the individual have not been impacted.

In the case of a Freedom of Information or Environmental Information Request a Public Interest Test (PIT) would be required when considering whether or not information should be withheld under an FOI qualified exemption or any exceptions of the EIRs. (see the Freedom of Information/EIRs Operational Process for more details).

4.7.5. Fees

Where BUL has the right to apply fees to the processing of a request, as determined by Data Protection and/or Information Access Legislation, then the rates and definitions of use are set out in The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004.

4.8. Annual Training

All staff at BUL are expected to undertake statutory annual training on Data Protection, Security and Information Compliance in order to keep the knowledge and skills up to date.

A good level of understanding of privacy responsibilities is a requirement of the DPA 2018 and the UK GDPR. This enables to understand more directly how awareness of privacy responsibilities, or lack of it, can impact BUL's ability to function legally, effectively and ethically and how it impacts on individuals.

Improved awareness should result in better protection of confidential and personal information from unauthorised access by staff and contracted third parties, or inadvertent disclosure and theft, etc. Information is less likely to fall into the wrong hands and is less likely to be compromised or misused.

4.9. Provisions for monitoring and reporting relating to the Policy

BUL will conduct regular periodic audits/spot checks to assess compliance with this Policy and related Procedures.

4.9.1. Retention

BUL will keep some forms of information for longer than others, in accordance with legal, financial, archival, or other business requirement. In accordance with the storage limitation principle, BUL will dispose of or delete any personal data no longer required for a specified purpose or legal requirement, in accordance with our agreed Record Retention Schedules. These records are held by the Records Centre, which is the centralised repository for University Records. The Records Centre retain a permanent register of how the data has been processed while in the custody of the Centre, including its confidential destruction at the end of its lifecycle. This applies to paper records and equally, the growing collection of digital records.

4.9.2. Records of Processing Activities (ROPA)

BUL keeps full and accurate records of its processing activities in accordance with Data Protection Legislation. This should include a description of the types of Personal Data and Data Subjects, processing activities and purposes, third party recipients, storage locations and retention periods. BUL also keeps a record of any Personal Data Breaches, requests for information and data subject access requests, which are held in accordance with our Records Retention Schedules.

Systems and processes must ensure they comply with this Policy and check that adequate governance controls are in place to ensure proper use and protection of Personal Data.

4.9.3. Information Assurance Committee (IAC)

Regular updates relating to monitoring statistics relating to this Policy are reported to the IAC. This includes but not limited to:

a. Data breach statistics
b. Subject Access Request

c. Freedom of Information/Environmental Regulation requests
d. Information Risk Log

5 Review

This Policy will be reviewed biennially by the DPO, IAC and the University Executive Board. It may also be revised as needed to ensure compliance with applicable laws, promote operational efficiencies, advance BUL strategy, and reduce institutional risks.

6 Related policies, procedures, standards and guidance

Data Breach Procedures

Data Sharing Procedures and Guidance

Data Protection Impact Assessment Guidance

Legitimate Interest Guidance

FOI Publication Scheme

CCTV Policy

Records Management Policy and Records Retention Schedules

Records Retention and Disposal Policy

Freedom of Information Policy

FOI/EIRs - operational process

SAR and Information Rights – operational process

Archives and Special Collections Policy

Appendix I

Lawful basis for processing personal data

The University must have a valid lawful basis in order to process personal data and, in most cases, will also need to be satisfied that it is 'necessary' to process personal data to achieve the relevant purpose.

There are only six potential lawful bases for processing personal data:

a. Public task – this applies when the processing is necessary for the University to perform a task in the public interest or as part of its official functions.
b. Legitimate interests - this applies when the processing is necessary for the legitimate interests of the University or a third party, (unless there is a good reason to protect the individual's personal data which overrides those legitimate interests).
c. Contract – this applies when the processing is necessary for a contract the University has with the individual, (any processing of personal data under this category must be targeted and proportionate).
d. Legal obligation – this applies when the processing is necessary for the University to comply with the law. This can relate to legal, regulatory and other compliance obligations, as well as matters such as the prevention or detection of crime.
e. Vital interests – the processing is necessary to protect the vital interest of someone, normally this means to protect their life.
f. Consent – the individual has freely given clear, informed consent for the University to process their personal data (this will always be for a specific purpose).

Appendix II

UK GDPR Data Protection Principles explained.

1.1. Lawfulness, Fairness and Transparency

BUL must have a lawful basis for collecting and processing Personal Data and must do it for a specified purpose. Without a lawful basis the processing will be unlawful and unfair. You will need to consider one of these grounds when processing Personal Data:

a. The Data Subject has given their consent.
b. The Processing is necessary for the performance of a contract with the Data Subject.
c. To comply with BUL's legal obligations.
d. To protect the vital interests of the Data Subject or another person.
e. To perform a task carried out in the public interests (this would be teaching and research in BUL's case); or
f. To pursue BUL's legitimate interests where those interests are not outweighed by the rights and interests of the Data Subject.

BUL must identify at least one of the above grounds and document why it is relying upon it when Processing Personal Data.

1.2. Consent as a lawful basis

Consent is one of the legal bases which can be relied upon when Processing Personal Data but in order for consent to be valid you must consider the follow:

a. Consent must be 'freely given', specific and informed. Which means there must be a clear indication of agreement (consent). Therefore, pre-ticked boxes or inactivity cannot be taken as consent.
b. Data Subjects must be able to freely withdraw their consent at any time and a wish to withdraw consent must be acted upon promptly.
c. Consent should be refreshed regularly especially if you intend to Process Personal Data for a different or an incompatible purpose for which it was initially disclosed.
d. Consent must be evidenced and documented – this forms part of the accountability principle.

1.3. Transparency

Transparency requires BUL to ensure that any information provided to Data Subjects about how their data will be processed is clear, concise, easily accessible and written in plain language. Such information is provided through Privacy Notices. A Privacy Notice will contain information about the Controller (the University) and the DPO and will set out how BUL will use, Process, protect, disclose and retain Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting/receiving the Personal Data. We must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis

which considers our proposed Processing of that Personal Data, i.e., that the individual knew that their Personal Data was going to be passed to us and for what purpose.

1.4. Purpose Limitation

BUL must only collect and Process Personal Data for a specified, explicit and legitimate purpose and where Data Subjects have been communicated with (Privacy Notice). Personal Data must not be further Processed in a manner which is incompatible for the purpose in which it was first collected. If BUL intends to use it for a different purpose the Data Subjects must be informed of the new purposes and the lawful basis relied upon.

1.5. Data Minimisation

Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purpose for which it is Processed. Therefore, you can only collect Personal Data which is required for that specified purpose and should not seek more Personal Data than is necessary.

As an employee, you must only process Personal Data for the performance of your duties and tasks and not for any other purpose.

When Personal Data is no longer required for that specified purpose it must be deleted or anonymised in accordance with BUL's data retention guidelines. BUL's Data Retention Schedule provides information about the length of time BUL retains records. Personal Data records must be destroyed safely and securely.

1.6. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. Personal Data must be corrected or deleted without delay where BUL is made aware of its inaccuracy. You must ensure that you update all relevant records if you become aware that any Personal Data are inaccurate. Where appropriate, any out- of-date or inaccurate records should be deleted/destroyed.

Employees and students must ensure that they keep BUL updated regarding any change of circumstances.

1.7. Storage Limitation

Personal Data collected and Processed by BUL must not be retained in a form where the Data Subject could be identified for longer than is needed for the specified purpose(s) for which it was originally collected (other than where it is retained in order to comply with any legal, accounting or reporting requirements).

Where Personal Data is retained/stored for longer than necessary this may increase the severity of a data breach.

BUL's Data Retention Schedule sets out retention periods for records including Personal Data and records should be deleted, destroyed, or anonymised after a reasonable period of time following expiry of the purpose(s) for which they were collected. Employees must comply with BUL's Data Retention Schedule and should regularly review any Personal Data Processed in the performance of their duties and tasks to assess whether the purpose(s) for which the data

are collected have expired.

All Privacy Notices must inform Data Subjects of the period for which their Personal Data will be stored/retained.

1.8. Security, Integrity and Confidentiality

Personal Data must be secured by appropriate technical and organisational measures to protect it against accidental loss, destruction or damage and against unauthorised or unlawful processing.

BUL will develop, implement, and maintain safeguards appropriate to the scope and size of our business, available resources, the amount of Personal Data that we control/maintain and identified risks (this will include the use of encryption and pseudonymisation where applicable).

BUL will regularly test and evaluate the effectiveness of such measures to ensure they are adequate and effective.

You are responsible for ensuring the security of Personal Data processed by you in the performance of your duties and tasks and must follow all relevant procedures BUL has in place to maintain the security of Personal Data; and you must observe and comply with our Information Security Policy. You must exercise particular care in protecting Special Category Data from loss and unauthorised access, use or disclosure.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

a. Confidentiality means that only people who have a need to know and are authorised to use Personal Data can access it. This means if you have access to Personal Data but it is not required for you to perform your duties and tasks, you should not access this data.
b. Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
c. Availability means that authorised users can access Personal Data when they need it for authorised purposes. This means that you should not access or use any Personal Data if you are not permitted to.

You must not attempt to circumvent any administrative, physical or technical safeguards that have been implemented by BUL as doing so may result in disciplinary action.

Appendix III

Policy on Processing Special Categories of Personal Data and Criminal Offence Data

As part of its statutory functions and obligations as both a higher education provider and employer BUL processes Special Category Data and Criminal Offence Data in accordance with Articles 9 and 10 of the UK GDPR and Schedule 1 of the DPA 2018. This includes (but is not limited to) Personal Data relating to health, wellbeing, race, ethnicity and trade union membership. Further information can be found in the BUL privacy notices.

Schedule 1 of the DPA 2018 requires BUL to put in place an appropriate policy document in relation to the Processing of Special Category Data in accordance with Article 5 of the UK GDPR. This Appendix explains our processing and thus satisfied the requirements of Schedule 1 of the DPA 2018 and supplements BUL's staff and student privacy notices. It satisfies the substantial public interest condition and the condition for processing employment, social security and social protection data.

Article 9 of the UK GDPR defines Special Category Data as racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, genetic data, biometric data, physical and mental health data; or data concerning sex life or sexual orientation.

Article 10 and of the UK GDPR and Section 11(2) of the DPA 2018 covers processing in relation Criminal Offence Data. This includes the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing.

BUL processes Special Categories of Personal Data under the following UK GDPR Articles (these are not in order of requirement):

Article 9(2)(a) – Explicit Consent.

Article 9(2)(b) – where processing is necessary for the purposes of carrying out the obligations and exercising BUL's rights as a Controller or in connection with employment, social security or social protection – for example staff sickness absence.

Article 9(2)(c) – where processing is necessary to protect the vital interests of a Data Subject or another natural person. For example, processing health information in the event of a medical or other emergency.

Article 9(2)(f) – where it is necessary for the establishment, exercise or defence of legal claims. For example, employment tribunal or other litigation.

Article 9(2)(g) – where processing is necessary for reasons of substantial public interest and is necessary for BUL to carry out its role. For example, equality of opportunity.

Criminal Offence Data is processed under Article 10 of the UK GDPR – for pre- employment or pre-admission checks and declarations (for employees and students) in accordance with contractual obligations.

BUL processes Special Categories of Personal Data under Part 1 of Schedule 1 of the DPA 2018:

Paragraph 1(1) – for employment, social security and social protection purposes.

BUL processes Special Categories of Personal Data under Part 2 of Schedule 1 of the DPA 2018:

Paragraph 6(1) and 2(a) – for statutory purposes.

Paragraph 8(1) – to review absence of equality of opportunity or treatment between specific groups.

Paragraph 9(1) – where processing is carried out as part of a process of identifying suitable individuals to hold senior positions.

Paragraph 10(1) – preventing and detecting unlawful acts.

Paragraph 11(1) and 11(2) – where protecting the public against dishonesty.

Paragraph 12(1) and 12(2) – regulatory requirements relating to unlawful acts and dishonesty.

Paragraph 24(1) and 24(2) – disclosure of elected representatives.

BUL processes Criminal Offence Data for the following purposes under Part 1 and Part 2 of Schedule 1 of the DPA 2018:

Paragraph 1 – for employment, social security and social protection purposes.

Paragraph 6(2)(a) – statutory purposes.

April 2024