Data Protection Policy	
Summary	This policy explains how Bridge School of Business (BSB) complies with the UK GDPR, the Data Protection Act 2018 and related data protection obligations when collecting, using, storing, sharing, retaining and deleting personal data. It sets out the standards expected of all staff and others who handle personal data for or on behalf of BSB
Policy owner	Senior Information Risk Owner (SIRO) and Data Protection Officer (DPO) – Academic Registrar
Approval authority	Board of Directors (via Finance and Audit Committee)
Applies to	Staff, contractors, agency staff, consultants, volunteers, directors, governors, shareholders, external or independent committee members, independent examiners, invigilators, job applicants, students, applicants, alumni, suppliers, and anyone who accesses BSB systems or whose personal data BSB processes
Version	1.0
Date of approval	11 May 2026
Date of next review	May 2027

Purpose

1. Bridge School of Business (BSB) collects, uses and shares personal data in order to carry out its academic, professional, governance, regulatory, employment, contractual, safeguarding, security and operational functions.

2. This policy sets out how BSB will protect personal data and meet its obligations under the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations where applicable, and associated ICO guidance.

3. This policy supports BSB's accountability obligations by requiring appropriate governance, records, training, controls, risk assessment, security, breach management, privacy notices, data sharing arrangements, retention controls and review mechanisms. ICO guidance identifies accountability as requiring organisations to take responsibility for compliance and keep evidence of the steps they take, including policies, data protection by design and default, contracts, documentation, security, breach recording/reporting and DPIAs.

4. This policy should be read alongside BSB's Privacy Notice, which explains to individuals how BSB collects, uses and shares their personal data and describes their rights. It should also be read alongside the Data Governance and Integrity Policy, which sets out BSB's approach to data quality, accuracy, integrity, ethical use, institutional oversight and external reporting.

Scope

5. This policy applies to all personal data processed by BSB, whether held electronically, on paper, in audio or visual form, in emails, in systems, in learning platforms, in HR systems, in student records, in finance systems, in CCTV or body-worn camera systems, or in any other format.

6. It applies to personal data relating to students, applicants, alumni, staff, workers, job applicants, contractors, consultants, suppliers, directors, governors, shareholders, volunteers, committee members, visitors and any other individual whose personal data BSB processes.

7. Where BSB processes personal data relating to individuals under the age of 18, including applicants or students, additional safeguards will be applied in line with ICO guidance on children's data, safeguarding obligations, and fairness and transparency requirements.

8. It applies to all BSB staff and associates who create, access, receive, use, disclose, store, amend, transfer, delete or otherwise process personal data. This includes permanent and temporary staff, contractors, consultants, agency staff, volunteers, governors, directors, external examiners, invigilators, suppliers, service providers and anyone else acting for or on behalf of BSB.

9. It applies to all personal data processing carried out for academic, student support, admissions, enrolment, assessment, progression, graduation, alumni, employment, payroll, finance, governance, safeguarding, immigration compliance, statutory reporting, security, estates, IT, marketing, research, complaints, disciplinary, audit and regulatory purposes.

10. Where another BSB policy provides more detailed requirements for a particular activity, this policy remains the overarching data protection standard and must be applied consistently with that more detailed policy.

Status of BSB as data controller

11. BSB is the data controller for the personal data covered by this policy where it determines the purposes and means of processing.

12. BSB may also act as a joint controller, processor or recipient in specific arrangements. Before entering into new processing or sharing arrangements involving personal data, the responsible staff member must assess whether BSB is acting as controller, joint controller or processor and ensure that appropriate contractual or data sharing documentation is in place.

13. BSB is registered as a data controller with the Information Commissioner's Office (ICO). BSB's ICO registration number and registered details are published in the BSB Privacy Notice.

14. ICO guidance states that understanding whether an organisation is a controller, joint controller or processor is crucial because obligations vary depending on that role, and that organisations should assess and document their status for processing activities.

15. BSB applies a documented assessment to determine controller, joint-controller or processor status for all new arrangements, with outcomes recorded and appropriate agreements put in place.

Key definitions

16. For the purposes of this policy:

16.1. **Personal data** means information relating to an identified or identifiable living individual. This may include names, identification numbers, location data, online identifiers, contact details, images, student numbers, staff numbers, IP addresses and other information that can identify an individual directly or indirectly.

16.2. **Special category data** means personal data that requires additional protection under data protection law. This includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, health data, sex life data and sexual orientation data.

16.3. **Criminal offence data** means personal data relating to criminal convictions, offences, allegations, proceedings, related security measures or relevant safeguarding information.

16.4. **Processing** means any operation performed on personal data, including collecting, recording, organising, structuring, storing, adapting, retrieving, consulting, using, disclosing, transmitting, sharing, restricting, erasing or destroying it.

16.5. **Data subject** means the individual to whom personal data relates.

16.6. **Controller** means an organisation that determines the purposes and means of processing personal data.

16.7. **Processor** means an organisation that processes personal data on behalf of a controller.

16.8. **Data Protection Officer ("DPO")** means the person designated to advise on data protection compliance, monitor compliance, provide independent oversight, advise on DPIAs and act as a contact point for the ICO and individuals.

16.9. **DPIA** means Data Protection Impact Assessment. It is a structured assessment used to identify and reduce privacy risks, particularly where processing is likely to result in a high risk to individuals

16.10. **ROPA** means Record of Processing Activities. It is BSB's documented record of the personal data processing activities it undertakes.

Data protection principles

17. BSB will process personal data in accordance with the UK GDPR principles. ICO guidance

identifies the seven key principles as lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.

18. BSB applies data protection principles consistently with its obligations under equality and anti-discrimination law. Personal data will not be used in ways that unlawfully disadvantage individuals or groups, and data protection controls support fairness, equality of opportunity and ethical decision-making.

19. BSB will therefore ensure that personal data is:

    19.1. Processed lawfully, fairly and transparently;

    19.2. Collected for specified, explicit and legitimate purposes;

    19.3. Adequate, relevant and limited to what is necessary;

    19.4. Accurate and, where necessary, kept up to date;

    19.5. Kept in identifiable form for no longer than necessary;

    19.6. Processed securely using appropriate technical and organisational measures; and

    19.7. Managed in a way that enables BSB to demonstrate compliance.

20. These principles apply to all stages of the personal data lifecycle, including design, collection, use, sharing, storage, retention, archiving and deletion.

21. The Data Governance and Integrity Policy supports these principles by establishing additional standards for data quality, accuracy, integrity, ethical use, transparency, fairness, accountability, risk management and continuous improvement.

Lawfulness, fairness and transparency

22. BSB will process personal data only where there is a valid lawful basis under UK GDPR.

23. BSB will identify and document the lawful basis for each personal data processing activity before the processing begins, normally through the Record of Processing Activities, privacy notices, DPIAs, data sharing documentation or other approved compliance records.

24. BSB will ensure that personal data is processed fairly. This means that BSB will use personal data in ways individuals would reasonably expect, will not use data in unjustified or misleading ways, and will take particular care where processing could affect individuals' rights, opportunities, welfare or access to services.

25. BSB will provide clear privacy information to individuals through the BSB Privacy Notice and, where required, through additional targeted privacy notices at the point of collection or before new forms of processing begin.

26. The BSB Privacy Notice explains that BSB processes personal data to keep proper records,

provide advice, manage and fulfil contracts, comply with legal obligations, pursue legitimate interests as a higher education provider, make and receive payments, and support students, staff, visitors and guests where health or disability information is relevant.

Lawful bases for processing

27. Depending on the activity, BSB may rely on one or more of the following lawful bases:

    27.1. The individual has given consent;

    27.2. Processing is necessary for a contract with the individual or to take steps before entering into a contract;

    27.3. Processing is necessary to comply with a legal obligation;

    27.4. Processing is necessary to protect vital interests;

    27.5. Processing is necessary to perform a task carried out in the public interest or in the exercise of official authority, where applicable; or

    27.6. Processing is necessary for legitimate interests pursued by BSB or a third party, except where overridden by the interests, rights and freedoms of the individual.

28. BSB will not rely on consent where another lawful basis is more appropriate. Where BSB relies on consent, it must be freely given, specific, informed and unambiguous, and the individual must be able to withdraw consent as easily as it was given.

29. Where BSB relies on legitimate interests, a Legitimate Interests Assessment (LIA) is completed and recorded prior to processing, and referenced in the Record of Processing Activities.

30. The BSB Privacy Notice identifies typical lawful bases across BSB activities, including contract, legal obligation, legitimate interests, public task where applicable, vital interests, medical purposes, substantial public interest, employment law obligations and consent where specifically required.

31. Staff must seek advice from the DPO where there is uncertainty about the correct lawful basis, where consent is proposed for a core institutional function, or where processing may be intrusive, novel, high-risk or unexpected.

Special category data and criminal offence data

32. BSB will process special category data only where it has both:

    32.1. a lawful basis under Article 6 UK GDPR; and

    32.2. a separate special category condition under Article 9 UK GDPR.

33. BSB identifies and documents the specific Article 9 UK GDPR condition relied upon for each

category of special category processing. A schedule mapping typical BSB processing activities to their applicable Article 9 conditions is maintained and reviewed by the DPO.

34. ICO guidance states that special category data needs more protection, and that organisations must identify both an Article 6 lawful basis and a separate Article 9 condition before processing it; in many cases, an appropriate policy document is also needed under the Data Protection Act 2018.

35. Where BSB relies on Schedule 1 conditions under the Data Protection Act 2018, processing will not commence unless it is covered by an approved Appropriate Policy Document (APD), which sets out applicable conditions, safeguards, and retention arrangements. The APD is reviewed at least annually.

36. BSB may process special category data for purposes including student support, safeguarding, welfare, disability support, reasonable adjustments, occupational health, employment law obligations, equality monitoring, health and safety, statutory reporting and protection of vital interests, where lawful and necessary.

37. BSB will process criminal offence data only where permitted by law and where the processing is necessary and proportionate. This may include safeguarding, DBS-related checks where relevant, security incidents, disciplinary matters, legal claims, regulatory compliance, right-to-work or immigration compliance, and other lawful purposes.

38. Staff must apply enhanced confidentiality and access controls to special category data and criminal offence data. Access must be limited to those who need the information for a legitimate operational, legal, safeguarding, welfare, employment or regulatory purpose.

Purpose limitation

39. BSB will collect personal data for specified, explicit and legitimate purposes.

40. Staff must not use personal data for a new or incompatible purpose unless:

    40.1. The new purpose is compatible with the original purpose;

    40.2. BSB has identified a new lawful basis;

    40.3. Individuals have been provided with any required privacy information; and

    40.4. Any required DPIA, data sharing assessment or DPO advice has been completed.

41. Where staff are considering a new use of personal data, particularly involving analytics, profiling, AI-enabled tools, data matching, new external disclosures or high-volume processing, they must consult the DPO at an early stage.

Data minimisation

42. BSB will collect and use only the personal data that is adequate, relevant and necessary for the purpose.

43. Staff must not collect personal data on a “just in case” basis. Forms, systems, spreadsheets, surveys and data collection processes must be designed to collect only the information required.

44. Where anonymised or aggregated data would meet the purpose, BSB will use anonymised or aggregated data rather than identifiable personal data wherever reasonably practicable.

45. Where pseudonymisation (replacing direct identifiers with artificial identifiers) can reduce risk while still enabling the purpose to be achieved, staff should use pseudonymisation where appropriate.

Accuracy and data quality

46. BSB will take reasonable steps to ensure that personal data is accurate and, where necessary, kept up to date.

47. Staff are responsible for entering, checking, correcting and maintaining accurate personal data in the systems and records they use.

48. Individuals should be encouraged to inform BSB promptly about changes to the information BSB holds about them, particularly contact details, immigration status where relevant, sponsorship arrangements, emergency contact details, bank details, health or disability information where relevant, and other information necessary for BSB’s functions.

49. The Data Governance and Integrity Policy requires BSB to maintain high-quality data that is accurate, complete, timely and fit for purpose, and to support effective decision-making, student success and regulatory compliance.
50. Where inaccurate personal data is identified, staff must take prompt steps to correct, complete, erase or restrict it as appropriate.

Storage limitation and retention

51. BSB will keep personal data in identifiable form for no longer than necessary for the purposes for which it is processed.

52. Retention periods are set out in BSB’s Records Retention Schedule. The Privacy Notice summarises these arrangements for transparency to individuals.

53. Staff must not retain personal data indefinitely unless there is a documented lawful, regulatory, archival, evidential or operational reason to do so.

54. Personal data must be securely deleted, destroyed, archived or anonymised at the end of the applicable retention period.

55. Where records are subject to a legal hold, complaint, appeal, investigation, audit, safeguarding concern, regulatory enquiry or litigation, deletion must be suspended until the matter is resolved and the retention position has been reviewed.

Integrity, confidentiality and security

56. BSB will protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

57. Staff must apply appropriate technical and organisational security measures, including:

    57.1. Using approved BSB systems for storing and processing personal data;

    57.2. Keeping paper records secure and out of public view;

    57.3. Locking cabinets, drawers and offices where confidential records are held;

    57.4. Using secure passwords and multi-factor authentication where provided;

    57.5. Not sharing passwords or access credentials;

    57.6. Locking screens when devices are unattended;

    57.7. Using encryption where required;

    57.8. Avoiding unnecessary use of removable media;

    57.9. Reporting lost devices, misdirected emails, unauthorised access or suspected compromise promptly;

    57.10. Checking recipients carefully before sending personal data;

    57.11. Using secure transfer methods for sensitive or high-volume personal data; and

    57.12. Following BSB's information security requirements.

58. Personal data must not be stored on personal devices, personal email accounts, unapproved cloud services or removable media unless expressly authorised and appropriately secured.

59. Special category data, criminal offence data, safeguarding data, immigration data, financial data, assessment data, disciplinary records and other sensitive records must be handled with particular care.

60. Failure to comply with data protection and information security requirements may lead to disciplinary action, contractual action, withdrawal of access, reporting to professional or regulatory bodies, or other appropriate measures.

Accountability and records of processing

61. BSB will maintain appropriate records to demonstrate compliance with data protection law.

62. BSB will maintain a Record of Processing Activities that documents, where applicable:

62.1. The purposes of processing;

62.2. Categories of individuals;

62.3. Categories of personal data;

62.4. Lawful bases;

62.5. Special category or criminal offence conditions where applicable;

62.6. Recipients or categories of recipients;

62.7. International transfers;

62.8. Retention periods;

62.9. Technical and organisational security measures; and

62.10. Responsible data owners or service areas.

63. ICO guidance states that the UK GDPR contains explicit provisions about documenting processing activities, including purposes, data sharing and retention, and that records must be kept up to date and reflect current processing activities.

64. All processing activities must be recorded in BSB's Record of Processing Activities prior to commencement, with assigned ownership and periodic review.

65. Staff introducing, changing or retiring systems, processes, data flows, sharing arrangements or personal data uses must ensure that the relevant processing records are reviewed and updated.

66. BSB will keep evidence of key compliance steps, including DPIAs, legitimate interests assessments, data sharing assessments, processor due diligence, privacy notices, breach records, training records, audit reports and policy reviews.

Data protection by design and default

67. BSB will embed data protection into the design and operation of systems, services, projects, processes, contracts, forms, reports, analytics, learning technologies and governance arrangements.

68. Staff responsible for new or changed processing must consider privacy and data protection at the earliest possible stage.

69. By default, BSB will ensure that:

69.1. Only necessary personal data is collected;

69.2. Access is limited to those who need it;

69.3. Personal data is not made public unless lawful and necessary;

69.4. Retention is defined;

69.5. Security is appropriate to the risk;

69.6. Individuals receive appropriate privacy information;

69.7. Data sharing is assessed and documented; and

69.8. Risks to individuals are identified and mitigated.

70. ICO guidance identifies data protection by design and default as one of the measures that supports accountability.

Data Protection Impact Assessments

71. BSB will carry out a DPIA where processing is likely to result in a high risk to individuals' rights and freedoms. A DPIA must normally be considered for:

71.1. New systems or technologies involving personal data;

71.2. Large-scale processing;

71.3. Special category or criminal offence data;

71.4. Systematic monitoring;

71.5. CCTV or body-worn camera changes;

71.6. AI-enabled tools;

71.7. Automated decision-making or profiling;

71.8. Learning analytics or risk scoring;

71.9. Data matching or data linkage;

71.10. New data sharing arrangements;

71.11. New uses of children's or vulnerable individuals' data;

71.12. Processing that may affect access to education, support, employment or services; and

71.13. Any other processing that is novel, intrusive or high-risk.

72. The Data Governance and Integrity Policy requires a DPIA for new high-risk data projects and states that this process should incorporate ethical considerations, including necessity, proportionality, bias, transparency, consent, impact and mitigation measures.

73. The DPO must be consulted on DPIAs and may make recommendations on risk reduction, safeguards, transparency, governance, retention, security, monitoring and whether ICO consultation is required.

74. Processing will not proceed where high risks remain unresolved and unless an appropriate senior decision-maker has considered the DPO's advice, the risks have been formally documented, and any required ICO consultation has taken place.

Individual rights

75. BSB will respect the rights of individuals under data protection law. Depending on the circumstances, individuals may have the following rights:

    75.1. The right to be informed;

    75.2. The right of access;

    75.3. The right to rectification;

    75.4. The right to erasure;

    75.5. The right to restriction of processing;

    75.6. The right to data portability;

    75.7. The right to object;

    75.8. Rights relating to automated decision-making and profiling; and

    75.9. The right to withdraw consent where processing is based on consent.

76. The BSB Privacy Notice states that these rights apply to all individuals whose personal data BSB processes, including students, applicants, alumni, staff, workers, officeholders, contractors and other contacts, and that the rights are subject to conditions and exemptions under data protection law.

77. Staff must forward any request that may involve individual rights to the DPO without delay. Requests do not need to mention data protection law or use formal legal terminology to be valid.

78. Unless a lawful extension applies, BSB will respond to all individual rights requests within one month of receipt. Where an extension, refusal or exemption is applied, BSB will explain this to the individual where required.

79. Staff must not delete, amend or conceal records because a request has been made. Once a request is received, relevant records must be preserved until the request has been handled.

Subject Access Requests

80. Individuals have the right to request access to personal data that BSB holds about them.

81. BSB will respond to Subject Access Requests without undue delay and normally within one month of receipt, unless an extension is permitted under data protection law.

82. No fee will normally be charged. A reasonable fee may be charged, or a request may be refused, where permitted by law, for example where the request is manifestly unfounded or excessive.

83. Staff must immediately forward any Subject Access Request to the DPO and must assist with searches, review, redaction and contextual explanation where requested.

84. BSB will protect the rights of other individuals when responding to Subject Access Requests and will apply appropriate redactions or exemptions where necessary.

Privacy notices and transparency

85. BSB will maintain a clear and accessible Privacy Notice explaining how it collects, uses and shares personal data and the rights available to individuals.

86. The BSB Privacy Notice states that it is BSB's core privacy notice and applies across academic, professional, governance and operational activities.

87. Where BSB introduces new processing that materially changes how personal data is used, BSB will update the Privacy Notice and, where appropriate, provide targeted notices at the point of collection or use.

88. Staff must ensure that privacy information is provided before or at the time personal data is collected, unless an exception applies.

89. Where personal data is obtained from another source, BSB will provide privacy information within the required timeframe unless an exemption applies.

Internal access to personal data

90. Access to personal data will be limited to those who need it for a legitimate academic, professional, operational, welfare, safeguarding, employment, governance, legal, contractual, security or regulatory reason.

91. The BSB Privacy Notice states that BSB will limit access to personal data to employees, managers, academic staff, HR staff, finance staff, line managers, agents and contractors who need access for a legitimate operational reason.

92. Staff must not access personal data out of curiosity, for personal reasons, or for any purpose outside their role.

93. Line managers and system owners must ensure that access rights are appropriate, reviewed periodically and removed promptly when staff change role or leave BSB.

Data sharing

94. BSB may share personal data under a lawful basis, and if necessary and proportionate.

95. BSB may share personal data with organisations such as awarding bodies, validating partners, regulators, HESA, the Office for Students, the Home Office where immigration compliance applies, placement providers, sponsors, student support providers, IT providers, library providers, survey contractors, tuition-fee-related providers, HR and payroll providers, HMRC, pension administrators, occupational health providers, police or enforcement bodies, auditors, data hosting providers, maintenance and facilities providers, and other third parties involved in BSB operations where lawful and necessary. The BSB Privacy Notice identifies these categories of sharing.

96. BSB does not sell personal data and does not permit third parties to use personal data for their own marketing or unrelated purposes. This reflects the position set out in BSB's Privacy Notice.

97. Before sharing personal data, staff must ensure that:

    97.1. The sharing has a lawful basis;

    97.2. The purpose is clear;

    97.3. Only necessary data is shared;

    97.4. The recipient is appropriate;

    97.5. Individuals have been given privacy information where required;

    97.6. Security arrangements are suitable;

    97.7. Retention and deletion responsibilities are clear;

    97.8. A data sharing agreement, controller-to-controller arrangement, joint controller arrangement or processor contract is in place where required; and

    97.9. The sharing is recorded in BSB's ROPA or other approved compliance record where appropriate.

98. New or high-risk sharing arrangements must be reviewed by the DPO before they begin.

Processors and suppliers

99. Where BSB appoints a processor to process personal data on its behalf, BSB will carry out appropriate due diligence and put in place a written contract containing the required data protection terms.

100. Processor contracts must require the processor to process personal data only on BSB's documented instructions, maintain confidentiality, implement appropriate security, support rights requests, assist with breach management, manage sub-processors

appropriately, return or delete data at the end of the service, and make information available to demonstrate compliance.

101. ICO guidance identifies written contracts with organisations that process personal data on an organisation's behalf as an accountability measure.

102. Staff responsible for procuring or managing suppliers must consult the DPO where a supplier will access, host, store, analyse, transmit, support or otherwise process personal data.

International transfers

103. BSB will transfer personal data outside the UK only where permitted by data protection law.

104. Where personal data is transferred outside the UK, BSB will ensure that an appropriate transfer mechanism is in place, such as adequacy regulations, International Data Transfer Agreements (IDTA), approved transfer clauses or another lawful transfer route.

105. The BSB Privacy Notice states that some personal data may be transferred to, and stored at, a destination outside the UK, for example where processed by overseas staff or suppliers or where a supplier uses overseas storage facilities, and that BSB will only transfer personal data where a lawful transfer mechanism applies.

106. Staff must consult the DPO before entering into any new international transfer arrangement.

Automated decision-making, AI and analytics

107. BSB may use technology, algorithms, analytics or AI-enabled tools to support administrative efficiency, service delivery, institutional management, student support and staff decision-making.
108. BSB will not make solely automated decisions that have legal or similarly significant effects on individuals unless permitted by law and subject to appropriate safeguards.

109. The BSB Privacy Notice states that applicant automated tools are limited to clearly defined scenarios, that decisions involving professional judgement or significant effects are reviewed by trained staff, and that learner analytics, risk scoring and attendance alerts are decision-support tools only.

110. The Data Governance and Integrity Policy states that automated analyses may flag patterns, but human judgement is required before action, and that AI should augment rather than replace human support.

111. Where analytics, profiling or AI-enabled processing may affect individuals, BSB will ensure appropriate transparency, human oversight, bias assessment, data quality checks, DPIA review, routes for challenge and proportionate safeguards.

112. Staff must not introduce AI-enabled tools, profiling, learner analytics, risk scoring or automated decision-support processes involving personal data without consulting the DPO and following the DPIA process where required.

CCTV, body-worn cameras and monitoring

113. BSB may use CCTV, body-worn cameras and other monitoring technologies for legitimate operational, safety, security, crime prevention, safeguarding, estates, regulatory or incident-management purposes.

114. The BSB Privacy Notice states that BSB may use CCTV across campuses and body-worn cameras worn by security staff during work hours across campuses, and that this may involve personal data of students, staff, contractors, visitors and others on BSB premises or using BSB facilities.

115. Monitoring must be necessary, proportionate, transparent and subject to appropriate retention, access and security controls.

116. New or materially changed monitoring arrangements must be assessed for data protection risk and may require a DPIA.

Personal data breaches

117. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

118. Examples may include:

    118.1. Emails sent to the wrong recipient;

    118.2. Loss or theft of devices, files or papers;

    118.3. Unauthorised access to systems;

    118.4. Disclosure of personal data to an unauthorised person;

    118.5. Cyber incidents affecting personal data;

    118.6. Ransomware or malware affecting personal data;

    118.7. Accidental deletion or alteration of records;

    118.8. Failure of access controls;

    118.9. Lost exam, student, HR or finance records; or

    118.10. Inappropriate publication of personal data.

119. All staff, contractors and suppliers must report actual or suspected personal data breaches immediately to the DPO and IT as appropriate.

120. BSB will maintain a Data Breach Register recording the facts, effects, assessment, remedial action and notification decisions for personal data breaches.

121. Where legally required, BSB will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

122. Where legally required, BSB will inform affected individuals without undue delay.

123. The DPO will advise on breach assessment, containment, investigation, notification, communication, remediation and lessons learned.

124. Staff must preserve evidence, follow instructions from the DPO and IT, and must not attempt to conceal or independently resolve a breach without reporting it.

Training and awareness

125. BSB will provide data protection and information security training to staff at induction and at appropriate intervals thereafter.

126. Staff whose roles involve higher-risk processing, special category data, criminal offence data, statutory returns, safeguarding, student records, HR, finance, IT administration, analytics, research, marketing, procurement or system ownership may be required to complete additional training.

127. The Data Governance and Integrity Policy states that all staff receive training on data protection and security at induction and that staff in key data-handling roles undergo specialised training.

128. Staff must complete required training and apply it in their day-to-day work.

129. Managers must ensure that staff understand the data protection requirements relevant to their role.

Governance, roles and responsibilities

Board of Directors and committees

130. The Board of Directors has overarching responsibility for ensuring that BSB has appropriate arrangements for data protection, data governance, risk management and compliance. The Data Governance and Integrity Policy states that the Board has overarching accountability for adequate and effective data management arrangements, with oversight delegated through the Finance and Audit Committee, which approves this policy.

Academic Board

131. The Academic Board ensures that academic policies and practices involving personal data are consistent with this policy.

Senior Information Risk Owner / Data Protection Officer (DPO)

132. The DPO provides senior oversight of information risk, data governance and related institutional controls, and works with IT, data owners and the Data Assurance Group to ensure appropriate risk management.

133. The DPO provides independent advice and oversight on data protection compliance, monitors compliance, advises on DPIAs, supports breach response, advises on individual rights, acts as a contact point for the ICO and may report directly to senior leadership or the Board on data protection matters.

134. The Data Governance and Integrity Policy states that the DPO has authority to act independently and report directly to the Board of Directors on data protection matters, in line with regulatory requirements.

135. Where the DPO holds additional senior roles, BSB documents and retains a role-compatibility assessment to ensure compliance with Article 38(6) UK GDPR and avoid conflicts of interest.

Data Assurance Group

136. The Data Assurance Group supports implementation of data protection and data governance standards, reviews data-related risks and proposals, monitors controls, supports DPIAs and escalates significant matters as appropriate.

137. The Data Governance and Integrity Policy describes the Data Assurance Group as a cross-functional group that coordinates data governance activities, reviews procedures, monitors data quality indicators, discusses new data proposals and ensures DPIAs are conducted for major initiatives in consultation with the DPO.

Data owners and system owners

138. Data owners and system owners are responsible for ensuring that personal data within their area is accurate, secure, appropriately accessed, lawfully used, retained correctly, and covered by appropriate procedures, training and records.

Managers

139. Managers must ensure that staff follow this policy, complete training, use approved systems, report incidents, maintain records, and consult the DPO where required.

Staff and associates

140. All staff and associates must:

    140.1. Process personal data lawfully, fairly and securely;

    140.2. Follow this policy and related procedures;

    140.3. Complete required training;

    140.4. Use approved systems and secure methods;

    140.5. Respect confidentiality;

    140.6. Report breaches and risks immediately;

140.7. Support rights requests;

140.8. Keep records accurate and up to date;

140.9. Avoid unnecessary collection or retention of personal data;

140.10. Consult the DPO where unsure; and

140.11. Challenge and report inappropriate use of personal data.

Students

141. Students are data subjects in relation to their own personal data. Where students handle personal data as part of employment, placements, research, projects, representation, volunteering or other BSB activities, they must follow relevant data protection requirements and supervision arrangements.

Data protection and research

142. Research involving identifiable personal data must comply with this policy, ethical approval requirements, data protection law, research governance requirements and any funder or partner conditions.

143. Research projects involving special category data, vulnerable participants, large-scale data, data linkage, profiling, AI-enabled analysis or intrusive methods must be reviewed for DPIA requirements and ethical approval requirements.

144. Personal data used for research should be anonymised or pseudonymised wherever reasonably practicable.

145. Research participants must receive appropriate privacy information unless an exemption applies.

Marketing and communications

146. BSB will ensure that direct marketing and electronic communications comply with data protection law and (Privacy and Electronic Communications Regulations) PECR where applicable, and cookie transparency.

147. Marketing preferences must be recorded, respected and kept up to date.

148. Consent must be obtained where required, and individuals must be given a clear and simple way to opt out of marketing communications.

149. Alumni engagement, fundraising and promotional communications must be carried out in accordance with the lawful basis and preference arrangements described in the relevant privacy information.

Complaints and concerns

150. Individuals may raise concerns about BSB's processing of personal data using the contact details in the BSB Privacy Notice.

151. The BSB Privacy Notice states that individuals also have the right to complain to the Information Commissioner's Office, and provides the ICO complaints link.

152. Staff who become aware of a data protection concern, complaint or regulatory enquiry must notify the DPO promptly.

153. BSB will handle complaints fairly, promptly and transparently, and will use complaints to improve practice where appropriate.

154. Concerns about compliance with this policy or BSB's handling of personal data may be raised directly with the Data Protection Officer, independently of any formal complaint process. Raising a concern will not result in detriment or retaliation.

Non-compliance

155. Non-compliance with this policy may expose individuals and BSB to legal, regulatory, financial, operational and reputational risk.

156. Staff who fail to comply with this policy may be subject to disciplinary action, up to and including dismissal, depending on the seriousness of the matter.

157. Contractors, suppliers or other third parties who fail to comply may be subject to contractual action, termination, access withdrawal, reporting to regulators or other appropriate action.

158. Students who misuse personal data may be subject to action under the relevant student conduct or disciplinary procedure.

159. BSB will distinguish between deliberate or reckless misconduct and honest mistakes that are reported promptly. Early reporting is encouraged so that risks can be contained and lessons learned.

Monitoring, audit and assurance

160. BSB will monitor compliance with this policy through training records, internal audits, spot checks, breach reviews, DPIA monitoring, information governance reporting, supplier reviews, data quality checks and periodic review of processing records.

161. The Data Governance and Integrity Policy states that BSB will monitor adherence to data governance requirements through routine line management oversight, spot checks, internal audits, feedback and reporting to the Finance and Audit Committee.

162. Significant data protection risks, breaches, audit findings or compliance concerns must be escalated to the DPO, SIRO, Data Assurance Group, senior management, Academic Board, Finance and Audit Committee or Board of Directors as appropriate.

163. The DPO may provide periodic reports on data protection compliance, risk, incidents, training, DPIAs, individual rights, policy compliance and regulatory developments.

Policy review

164. This policy will be reviewed at least annually, or sooner where required by changes in law, ICO guidance, institutional structure, systems, processing activities, risk profile or regulatory expectations.

165. This policy must include a completed approval date and maintained change log prior to publication. Changes must be version-controlled and recorded to support audit, accountability and regulatory assurance.

166. The Data Governance and Integrity Policy is reviewed at least annually and may be updated more frequently where needed because the data landscape and regulatory requirements are continually evolving.

167. The DPO will advise on required updates and will ensure that the policy remains aligned with the BSB Privacy Notice, Data Governance and Integrity Policy, Records Retention Schedule and other related policies.

168. Updates must be communicated to staff and, where appropriate, to students, contractors, suppliers or other relevant groups.

Related policies, procedures and records

169. This policy should be read alongside the following documents and records:

    169.1. BSB Privacy Notice;

    169.2. BSB Data Governance and Integrity Policy;

    169.3. Records Retention Schedule;

    169.4. Information Security Policy;

    169.5. Acceptable Use Policy;

    169.6. Data Breach Procedure;

    169.7. Subject Access Request Procedure;

    169.8. Data Sharing Procedure;

    169.9. DPIA Procedure;

    169.10. Records of Processing Activities;

    169.11. Data Sharing Agreements;

169.12. Processor Contracts;

169.13. Supplier Due Diligence Records;

169.14. Training Records;

169.15. Data Breach Register;

169.16. Risk Register;

169.17. Whistleblowing Policy;

169.18. Fraud Prevention Policy; and

169.19. Relevant student, staff, academic, research, safeguarding, complaints and disciplinary procedures.

170. The Data Governance and Integrity Policy identifies the Data Protection Policy, Privacy Notice, Records Retention Schedule, Information Security Policy, Whistleblowing Policy, Fraud Prevention Policy and Risk Management Policy as part of BSB's broader compliance and governance framework.

Contact details

171. Questions about this policy, data protection compliance, personal data processing, individual rights, DPIAs, data sharing, breaches or privacy notices should be referred to:

Data Protection Officer
Bridge School of Business
Email: DPO@bsblondon.co.uk

Change Log			
Date	Version Updated	Resulting Version	Details