INFORMATION SECURITY AND DATA PROTECTION:

DATA PROTECTION POLICY

This policy is annually reviewed to ensure compliance with current regulations

Approved/reviewed by	
Approved by: **ISMS Committee / Chief Operating Officer** Reviewed by: **Director of ICT**	
Date of next review	**September 2024**

This policy and procedure is subject to The Equality Act 2010 which recognises the following Protected Characteristics: Age, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex, Sexual orientation and Disability

1. Document Control

1.1. Document Details

Title	Data Protection Policy
Author	Debbie Holland / Robbie Wallis
Version	1.2
Date	October 2023
Status	Published

1.2. Revision History

Version	Date	Author	Comments
1.0	May 2023	R Wallis	Definitive Release
1.1	September 2023	D Holland	Amendments – Definitive Release
1.2	October 2023	R Wallis	Amendment – Change of DPO

1.3. Distribution

Name	Email	Organisation
All Staff	Uploaded to SharePoint	Boston College
Everyone	Website	General Public

1. Introduction

This Policy sets out the obligations of Boston College regarding data protection and the rights of, inter alia, learners, parents, staff and visitors ("data subjects") in respect of their personal data under the Data Protection Act 2018 and the associated UK GDPR including any subsequent amendments.

The UK GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets out the college's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the college, its employees, agents, contractors, or other parties working on behalf of the college.

The college is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and College of all individuals with whom it deals.

2. The Data Protection Principles

This Policy aims to ensure compliance with the UK GDPR. The UK GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

2.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation

of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of the data subject.

2.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3. The Rights of Data Subjects

The Data Protection Act 2018 and the UK GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

3.1 The right to be informed (Part 12).

3.2 The right of access (Part 13).

3.3 The right to rectification (Part 14).

3.4 The right to erasure (also known as the 'right to be forgotten') (Part 15).

3.5 The right to restrict processing (Part 16).

3.6 The right to data portability (Part 17).

3.7 The right to object (Part 18); and

3.8 Rights with respect to automated decision-making and profiling (Parts 19 and 20).

4. Lawful, Fair, and Transparent Data Processing

4.1 The UK GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The UK GDPR states that processing of personal data shall be lawful if at least one of the following applies:

4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes.

4.1.2 The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them.

4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject.

4.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person.

4.1.5 The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

4.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such

interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4.2 If the personal data in question is "special category data" (also known as "sensitive personal data") (for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

4.2.1 The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless UK law prohibits them from doing so).

4.2.2 The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by UK law which provides for appropriate safeguards for the fundamental rights and interests of the data subject).

4.2.3 The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

4.2.4 The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;

4.2.5 The processing relates to personal data which is clearly made public by the data subject.

4.2.6 The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity.

4.2.7 The processing is necessary for substantial public interest reasons, on the basis of UK law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

4.2.8 The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of UK law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR.

4.2.9 The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of

health care and of medicinal products or medical devices, on the basis of UK law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

4.2.10 The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR based on UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5. Specified, Explicit, and Legitimate Purposes

5.1 The college collects and processes the personal data set out in Part 21 of this Policy. This includes:

5.1.1 Personal data collected directly from data subjects; and

5.1.2 Personal data obtained from third parties.

5.2 The college only collects, processes, and holds personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the UK GDPR).

5.3 Data subjects are kept informed at all times of the purpose or purposes for which the college uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

6. Adequate, Relevant, and Limited Data Processing

6.1 The college will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 21, below.

7. Accuracy of Data and Keeping Data Up to Date

7.1 The college shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.

7.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or outof-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Data Retention

8.1 The college shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

8.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

8.3 For full details of the college's approach to data retention, including retention periods for specific personal data types held by the us, please refer to our Data Retention Policy which is available on request.

9. Secure Processing

9.1 The college shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 22 to 27 of this Policy.

10. Accountability and Record-Keeping

10.1 The College's Data Protection Officer is Bivika, 8 Chesterford Road, London E12 6LB, dataprotection@boston.ac.uk

10.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the College's other data protection-related policies, and with the UK GDPR and other applicable data protection legislation.

10.3 The college shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

10.3.1 The name and details of The College, its Data Protection Officer, and any applicable third-party data processors;

10.3.2 The purposes for which The College collects, holds, and processes personal data;

10.3.3 Details of the categories of personal data collected, held, and processed by The College, and the categories of data subject to which that personal data relates;

10.3.4 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

10.3.5 Details of how long personal data will be retained by the college (please refer to our Data Retention Policy); and

10.3.6 Detailed descriptions of all technical and organisational measures taken by the college to ensure the security of personal data.

11. Data Protection Impact Assessments

11.1 The college shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the UK GDPR.

11.2 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

11.2.1 The type(s) of personal data that will be collected, held, and processed.

11.2.2 The purpose(s) for which personal data is to be used;

11.2.3 The College's objectives;

11.2.4 How personal data is to be used;

11.2.5 The parties (internal and/or external) who are to be consulted;

11.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

11.2.7 Risks posed to data subjects;

11.2.8 Risks posed both within and to the college; and

11.2.9 Proposed measures to minimise and handle identified risks.

12. Keeping Data Subjects Informed

12.1 The College shall provide the information set out in Part 12.2 to every data subject:

12.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

12.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

a) if the personal data is used to communicate with the data subject, when the first communication is made; or

b) if the personal data is to be transferred to another party, before that transfer is made; or

c) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

12.2 The following information shall be provided:

12.2.1 Details of the College including, but not limited to, the identity of its Data Protection Officer;

12.2.2 The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;

12.2.3 Where applicable, the legitimate interests upon which the college is justifying its collection and processing of the personal data;

12.2.4 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

12.2.5 Where the personal data is to be transferred to one or more third parties, details of those parties;

12.2.6 Where the personal data is to be transferred to a third party that is located in a territory without an adequacy agreement as approved by the UK Government, details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details);

12.2.7 Details of data retention;

12.2.8 Details of the data subject's rights under the UK GDPR;

12.2.9 Details of the data subject's right to withdraw their consent to the college's processing of their personal data at any time;

12.2.10 Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the UK GDPR);

12.2.11 Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

12.2.12 Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13. Data Subject Access

13.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the college holds about them, what it is doing with that personal data, and why.

13.2 Employees wishing to make a SAR should contact dataprotection@boston.ac.uk

13.3 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

13.4 Responses to SARs shall be dependent upon the terms of the UK GDPR, the Data Protection Act (2018) and associated ICO guidance.

13.5 The College will make reasonable efforts to find and retrieve the requested information, however, if the searches are unreasonable or disproportionate to the importance of providing access to the information the request will be declined.

13.6 The college does not charge a fee for the handling of normal SARs. The college reserves the right to charge reasonable fees for additional copies of information

that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

14.1 Data subjects may have the right to require the college to rectify any of their personal data that is inaccurate or incomplete.

14.2 Where such rectification is possible, The College shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the college of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

14.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15. Erasure of Personal Data

15.1 Data subjects have the right to request that the college erases the personal data it holds about them in the following circumstances:

15.1.1 It is no longer necessary for The College to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

15.1.2 The data subject wishes to withdraw their consent to The College holding and processing their personal data;

15.1.3 The data subject objects to The College holding and processing their personal data (and there is no overriding legitimate interest to allow the college to continue doing so) (see Part 18 of this Policy for further details concerning the right to object);

15.1.4 The personal data has been processed unlawfully;

15.1.5 The personal data needs to be erased in order for The College to comply with a particular legal obligation; or

15.1.6 The personal data is being held and processed for the purpose of providing information society services to a child.

15.2 Unless the College has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

15.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing

16.1 Data subjects may request that the college restricts processing the personal data it holds about them. If a data subject makes such a request, The College shall in so far as is possible ensure that the personal data is only stored and not processed in any other fashion.

16.2 If the College is required to process the data for statutory purposes or for reasons of legal compliance, then the college shall inform the Data Subject that this processing is expected to take place. If possible, this notice will be provided prior to processing.

16.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Data Portability

17.1 The college processes personal data using automated means. Such processing is carried out by, inter alia, our management information system (Integris), our human resources systems and our catering management system.

17.2 Where data subjects have given their consent to the college to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the college and the data subject, data subjects have the right, under the UK GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

17.3 Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

17.4 All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

18. Objections to Personal Data Processing

18.1 Data subjects have the right to object to the college processing their personal data based on performing a task in the public interest. Its' legitimate interests, or direct marketing (including profiling)

18.2 Where a data subject objects to the college processing their personal data, the college shall cease such processing immediately, unless it can be demonstrated that the college's grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

18.3 Where a data subject objects to the college processing their personal data for direct marketing purposes, the college shall cease such processing immediately.

18.4 Where a data subject objects to the college processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the UK GDPR, "demonstrate grounds relating to his or her particular situation". The college is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19. Automated Decision-Making

19.1 The college is not currently using personal data in automated decision-making processes. In the event that that this situation changes, the college shall notify data subjects of its' intentions to commence such processing.

19.2 Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge to such decisions under the UK GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the college.

19.3 The right described in Part 19.2 does not apply in the following circumstances:

19.3.1 The decision is necessary for the entry into, or performance of, a contract between the college and the data subject;

19.3.2 The decision is authorised by law; or

19.3.3 The data subject has given their explicit consent.

20. Profiling

20.1 The college uses personal data for profiling purposes. These purposes relate to helping student maximise achievement and monitor staff performance.

20.2 When personal data is used for profiling purposes, the following shall apply:

20.2.1 Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;

20.2.2 Appropriate mathematical or statistical procedures shall be used;

20.2.3 Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and

20.2.4 All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 to 26 of this Policy for more details on data security).

21. Personal Data Collected, Held, and Processed

21.1 The college uses a wide range of personal data across many processes. More detail can be found in our privacy notices. If you wish to view the complete lists of categories of personal data we process please contact our Data Protection Officer.

22. Data Security - Transferring Personal Data and Communications

The college shall ensure that the appropriate measures are taken with respect to all communications and other transfers involving personal data:

22.1 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

22.2 The college will ensure that where special category personal data or other sensitive information is sent in the post that it shall be possible to demonstrate that it was delivered.

22.3 Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

22.4 Where special category personal data or other sensitive information is to be sent by e-mail the email will either be sent using a suitable encryption method or the data will be sent in an attached, encrypted document and not in the body of the e-mail.

22.5 Where personal data is to be transferred in removal storage devices, these devices shall be encrypted. The use of unencrypted removable storage devices is prohibited by The College.

23. Data Security - Storage

The college shall ensure that the following measures are taken with respect to the storage of personal data:

23.1 All electronic copies of personal data should be stored securely using passwords, user access rights and where appropriate data encryption;

23.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

23.3 All personal data relating to the operations of The College, stored electronically, should be backed up on a regular basis

23.4 Where any member of staff stores personal data on a mobile device (whether that be computer, tablet, phone or any other device) then that member of staff must abide by the Acceptable Use policy of the college. The member of staff shall also ensure that they can provide a secure environment for that device to be used to minimise any risk to the confidentiality or integrity of the information.

24. Data Security - Disposal

24.1 When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the College's Data Retention Policy.

25. Data Security - Use of Personal Data

The college shall ensure that the following measures are taken with respect to the use of personal data:

25.1 No personal data may be shared informally and if an employee, agent, subcontractor, or other party working on behalf of The College requires access to any personal data that they do not already have access to, such access should be formally requested from

25.2 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of The College or not, without the initial authorisation of the data protection team (dataprotection@boston.ac.uk).

25.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

25.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and

25.5 Where personal data held by the college is used for marketing purposes, it shall be the responsibility of the Head of Marketing to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

26. Data Security - IT Security

The college shall ensure that the following measures are taken with respect to IT and information security and also adhere to all other Information Security Policies:

26.1 The college requires that any passwords used to access personal data shall have a minimum of 12 characters, composed of a mixture of upper and lower case characters, numbers and symbols. Passwords are not expected to be changed upon a regular basis but users will be expected to change their password if instructed by The College.

26.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of The College, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

26.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The College's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and

26.4 No software may be installed on any Company-owned computer or device without the prior approval of the Director of IT.

26.5 Where members of staff or other user use applications that require the use of personal data, the use of that application must be signed off by the Director of ICT.

26.6 All employees, agents and contractors who process college data will follow the Data Classification Policy.

26.7 Under no circumstances must college data be held on personal devices.

26.8 The use of removable media(USB, SD Cards, CD Rom's) is prohibited unless a specific exception has been granted by the Director of IT.

27. Organisational Measures

The college shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

27.1 All employees, agents, contractors, or other parties working on behalf of The College shall be made fully aware of both their individual responsibilities and our responsibilities under the UK GDPR and under this Policy, and shall have free access to a copy of this Policy;

27.2 Only employees, agents, sub-contractors, or other parties working on behalf of the college that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the college;

27.3 All employees, agents, contractors, or other parties working on behalf of the college handling personal data will be appropriately trained to do so;

27.4 All employees, agents, contractors, or other parties working on behalf of the college handling personal data will be appropriately supervised;

27.5 All employees, agents, contractors, or other parties working on behalf of the college handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

27.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

27.7 All personal data held by the college shall be reviewed periodically, as set out in the College's Data Retention Policy;

27.8 The performance of those employees, agents, contractors, or other parties working on behalf of the college handling personal data shall be regularly evaluated and reviewed;

27.9 The contravention of these rules will be treated as a disciplinary matter.

27.10 All employees, agents, contractors, or other parties working on behalf of the college handling personal data will be bound to do so in accordance with the principles of the UK GDPR and this Policy by contract;

27.11 All agents, contractors, or other parties working on behalf of the college handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as

those relevant employees of the college arising out of this Policy and the UK GDPR; and

27.12 Where any agent, contractor or other party working on behalf of the college handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the college against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

28. Transferring Personal Data to a Country without an adequacy decision

28.1 The college may from time to tie transfer ('transfer' includes making available remotely) personal data to countries without a suitable adequacy decision from the UK Government.

28.2 The transfer of personal data to a country without an adequacy decision shall take place only if one or more of the following applies:

28.2.1 The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the UK Government has determined ensures an adequate level of protection for personal data;

28.2.2 The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the UK Government compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the UK GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

28.2.3 The transfer is made with the informed consent of the relevant data subject(s);

28.2.4 The transfer is necessary for the performance of a contract between the data subject and the college (or for pre-contractual steps taken at the request of the data subject);

28.2.5 The transfer is necessary for important public interest reasons;

28.2.6 The transfer is necessary for the conduct of legal claims;

28.2.7 The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

28.2.8 The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

29. Data Breach Notification

29.1 All personal data breaches must be reported immediately to the college DPO, Bivika using dataprotection@boston.ac.uk

29.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

29.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 29.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

29.4 Data breach notifications shall include the following information:

29.4.1 The categories and approximate number of data subjects concerned;

29.4.2 The categories and approximate number of personal data records concerned;

29.4.3 The name and contact details of the college's data protection officer (or other contact point where more information can be obtained);

29.4.4 The likely consequences of the breach;

29.4.5 Details of the measures taken, or proposed to be taken, by the college to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

30. Implementation of Policy

This Policy shall be deemed effective on 16th October 2023. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.