General Data Protection Regulation policy

This policy is annually reviewed to ensure compliance with current regulations

Approved/reviewed by	
Data Protection Officer	
Date of next review	July 2023

Data Protection Policy

1 Purpose and scope

1.1 The purpose of this policy is to ensure compliance with the General Data Protection Regulation and related EU and national legislation ('data protection law').[1] Data protection law applies to the storing or handling ('processing') of information ('personal data') about living identifiable individuals ('data subjects').

1.2 This policy applies to all parts of Boston College ('the College'), as a single organisation ('data controller'). It does not apply to associated Trusts or subsidiary companies, which are separate legal entities and data controllers.

1.3 This policy applies to all staff except when acting in a private or non-College capacity. In this policy, the term 'staff' means anyone working in any context within the College at whatever level or grade and whether permanent, fixed term or temporary, including but not limited to employees, retired but active research staff, other visiting research or teaching staff, workers, trainees, interns, seconded staff, agency staff, agents, volunteers, and external members of committees.

1.4 This policy applies to all students when processing personal data on behalf of the College, but not in any other situation including when acting in a private or non- College capacity.

1.5 This policy is not, and should not be confused with, a privacy notice (a statement informing data subjects how their personal data is used by the College).

1.6 This policy should be read in conjunction with the obligations in the following documents, which supplement this policy where applicable:

1.6.1 staff employment contracts and comparable documents (e.g. worker agreements), which impose confidentiality obligations in respect of information held by the College;

1.6.2 information security policies, procedures and terms and conditions, which concern the confidentiality, integrity and availability of College information, and which include rules about acceptable use, breach reporting, IT monitoring, and the use of personal mobile devices;

1.6.3 records management policies and guidance, which govern the appropriate retention and destruction of College information; and

1.6.4 any other contractual obligations on the College or individual staff which impose confidentiality or data management obligations in respect of information held by the College, which may at times exceed the obligations of this and/or other policies in specific ways (e.g. in relation to storage or security requirements for funded research).

2 Policy statement

2.1 The College is committed to complying with data protection law as part of everyday working practices.

2.2 Complying with data protection law may be summarised as but is not limited to:

2.2.1 understanding, and applying as necessary, the data protection principles when processing personal data[1];

2.2.2 understanding, and fulfilling as necessary, the rights given to data subjects under data protection law [2]; and

2.2.3 understanding, and implementing as necessary, the College's accountability obligations under data protection law.[3]

3 Roles and responsibilities

3.1 The College has a corporate responsibility as a data controller (or when acting as a joint data controller or a data processor) for:

3.1.1 complying with data protection law and holding records demonstrating this;

3.1.2 cooperating with the Information Commissioner's Office (ICO) as the UK regulator of data protection law; and

---

[1] The principles in relation to personal data are: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality.

[2] The data subject rights are: to be informed; access; rectification; erasure; restriction; data portability; and objection (including in relation to automated decision-making).

[3] The accountability obligations include: implementing appropriate data protection policies; implementing data protection by design and default in projects, procurement and systems; using appropriate contracts with third party data controllers and data processors; holding relevant records about personal data processing; implementing appropriate technical and organisational security measures to protect personal data; reporting certain personal data breaches to the Information Commissioner's Office; conducting Data Protection Impact Assessments where required; and ensuring adequate levels of protection when transferring personal data outside the European Economic Area.

3.1.3 responding to regulatory/court action and paying administrative levies and fines issued by the ICO.

3.2 The College is responsible for:

3.2.1 reviewing (at least once every five years) and approving this policy; and

3.2.2 assessing the overall risk profile and ensuring appropriate resources and processes are in place and implemented to enable compliance with data protection law.

3.3 The independent Data Protection Officer is responsible for:

3.3.1 monitoring and auditing the College's compliance with data protection law, especially its overall risk profile, and reporting annually to the College Council;

3.3.2 advising the College on all aspects of its compliance with data protection law (including its use of Data Protection Impact Assessments);

3.3.3 acting as the College's standard point of contact with the ICO with regard to data protection law, including in the case of personal data breaches; and

3.3.4 acting as an available point of contact for complaints from data subjects.

3.3.5 Inform the ESFA of any request to rectify, block or erase any Personal Data

3.3.6 Inform the ESFA if they become aware of a data loss event

3.4 The Compliance Office, in collaboration with other relevant offices, is responsible for:

3.4.1 providing advice, guidance, training and tools/methods, in accordance with the College's overall risk profile and having taken into account the advice of the independent Data Protection Officer, relevant case law and ICO/other regulatory guidance, to help College Institutions and staff comply with this policy;

3.4.2 publishing and maintaining core privacy notices and other College-wide data protection documents;

3.4.3 handling data subject rights requests; and

3.4.4 as advised by the College Data Protection Officer, managing and/or handling Data Protection Impact Assessments, data subject complaints and personal data breaches.

3.5 Heads of Institutions are responsible for:

3.5.1 making all staff within their Institution aware of this policy as necessary;

3.5.2 ensuring that appropriate processes and training are implemented within their Institution to enable compliance with data protection law; and

3.5.3 ensuring that appropriate processes are implemented within their Institution to enable information assets containing personal data within their Institution to be included in the College's Information Asset Register.

3.6 Individual staff, as appropriate for their role and in order to enable the College to comply with data protection law, are responsible for:

3.6.1 completing relevant data protection training;

3.6.2 following relevant advice, guidance and tools/methods provided by the Information Compliance Office (and other relevant offices) depending on their role, regardless of whether access to and processing of personal data is through College-owned and managed systems, or through their own or a third party's systems and devices;

3.6.3 when processing personal data on behalf of the College, only using it as necessary for their contractual duties and/or other College roles and not disclosing it unnecessarily or inappropriately;

3.6.4 recognising, reporting internally, and cooperating with any remedial work arising from personal data breaches;

3.6.5 recognising, reporting internally, and cooperating with the fulfilment of data subject rights requests;

3.6.6 when engaging with students who are using personal data in their studies and research, advising those students of relevant advice, guidance and tools/methods to enable them to handle such personal data in accordance with this policy; and

3.6.7 only deleting, copying or removing personal data when leaving the College as agreed with their Head of Institution and as appropriate.

3.7 The responsibilities in paragraph 3.6 apply to individual students when processing personal data on behalf of the College.

3.8 Non-observance of the responsibilities in paragraph 3.6 may result in disciplinary action.

3.9 The roles and responsibilities in paragraphs 3.1 to 3.8 do not waive any personal liability for individual criminal offences for the wilful misuse of personal data under data protection law.[11]

4 Contact and date of last revision

4.1 This policy was last revised and approved by the College in July 2021.

4.2 The DPO can be contacted on dataprotection@boston.ac.uk

[11] These criminal offences include: unlawfully obtaining, disclosing or retaining personal data; recklessly re-identifying de-identified personal data without the data controller's consent; deliberately altering or deleting personal data to prevent disclosure in accordance with data subject access rights; forcing a data subject to exercise their access rights; and knowingly giving false statements to the ICO.

[12] See https://www.information-compliance.admin.cam.ac.uk/contact-us.

Boston College Equality Impact Assessment Template: Policies

1. What is the name of the policy

General Data Protection

2. What is the aim of the policy?

To ensure full compliance with the General Data Protection Act 2016 and to protect the confidentiality of personal data by ensuring all staff are given clear guidance on data protection and are aware of their responsibilities.

3. Who does the policy impact on? (Staff, learners, partners etc.)

To provide guidance to staff and sub-contractors on the correct process surrounding the collection and storage of learner and customer data by the College

4. Who implements the policy?

The Director of Planning & Performance is responsible for the policy along with the two Data Protection Officers, however, all staff involved in handling data are responsible for implementing the policy

5. What information is currently available on the impact of this policy?
(This could include data that is routinely collected for this policy and/or minutes from management or team meetings. It could also include conversations with students and/or staff who have used this policy in their day to day role).

The policy has been written to comply with the requirements of the General Data Protection Act 2016 which provides the same level of protection to all data subjects, and the guidelines require a consistent approach to the handling and sharing of data from all data subjects.

A record of all data protection requests is maintained by the Data Protection Officer and any breaches of data protection are reported directly to the Principal.

6. Do you need more information before you can make an assessment about this policy?
(If yes, please put down what information you need and identify in the action plan, how you intend to collect it)

No. The nature of a Data Protection request does not allow us to request or collect E&D or protected characteristic data.

7. Do you have any examples that show this policy is having a positive impact on any of the equality characteristics shown in Table.1?

The rules are the same for all user and data subjects. There are no differential impacts with respect to persons with protected characteristics

Boston College Equality Impact Assessment Template: Policies

8. Are there any concerns that this policy could have a negative impact on any of the equality characteristics shown in Table.1?

The rules are the same for all user and data subjects. There are no differential impacts with respect to persons with protected characteristics

Table. 1

Category	No	Yes	Please supply any additional comments
Race	√		
Disability		√	We have a number of learners with complex needs so need to consider communication of this policy.
Gender	√		
Gender re-assignment	√		
Age	√		
Sexual orientation	√		
Religion/belief	√		
Pregnancy/maternity	√		
Marriage/Civil Partnership	√		
Socio-economic	√		
Rurality	√		

Actions are to be taken as a result of the Equality Impact Assessment

Action Required *(clearly state where within existing management structures these actions will be performance monitored)*	Person responsible	Comp date	Review details - impact and outcome

Signed: Fiona Wrisberg	**Position: Data Protection Officer**	**Date: July 2021**

Boston College Equality Impact Assessment Template: Policies