BRIDGWATER & TAUNTON COLLEGE

DATA PROTECTION POLICY AND PROCEDURE

Effective for all students and staff on or after 25 May 2018

Author:	Information Systems and Exams Manager
Approved by:	SMT
Date:	May 2018
Review date:	May 2020

Contents

1 Introduction

1.1 The General Data Protection Regulations (GDPR) regulates the processing of personal data by the College.

1.2 In relation to the GDPR, personal data relates to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. The definition covers a wide range of personal identifiers including name, identification number, location data or online identifier. It extends to all personal data held by the College electronically and in some manual records. The GDPR regulates the "processing" of personal data which has a very broad meaning and includes collection, recording, organisation, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, dissemination or otherwise making available, aligning or combining, restricting, erasing and destroying.

1.3 The GDPR seeks to balance the protection of individual privacy with the business needs of the College. In order to achieve this balance, the College must comply with the principles relating to the processing of personal data which are set out in the regulations. In summary these state that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes
- 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 they are processed, are erased or rectified without delay
- Kept in a form which permits identification of data subjects for no for longer than is necessary for the purposes for which the personal data are processed
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, ~~or~~ destruction or damage, using appropriate technical or organisational measures.

1.4 The College and all staff or others who process or use any personal data must ensure that these principles are followed at all times. In order to ensure that this happens, the College has developed this Data Protection Policy and Procedure.

2 Policy Statement

2.1 This policy does not form part of the formal contract for education or employment, but it is a condition of employment that employees will abide by the rules and policies made by the College. Any failure to follow the policy can therefore result in disciplinary proceedings.

2.2 Any data subject who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Data Controller initially. If the matter is not resolved it should be raised appropriate within the College's complaints procedure.

3 Notification of Data Held and Processed

3.1 All students and other users are entitled to:

- Know what personal data the College holds and processes about them and why
- Subject to any exemptions, gain access to it
- Know how to keep it up to date
- Know what the College is doing to comply with its obligations under the GDPR.

4 Purpose

4.1 The College needs to keep certain information about students for the purposes of discharging its contractual obligation to provide education and training, including monitoring performance and achievements and discipline. It is also necessary to process the information to comply with the College's statutory obligations (e.g. health & safety, child protection, safeguarding and disability discrimination legislation) and to discharge its obligations to its regulatory and funding bodies and government departments and agencies (e.g. the Education and Skills Funding Agency, OFSTED, Office for Students, Awarding Organisations, etc.).

4.2 The College may disclose personal data to the Education and Skills Funding Agency, OFSTED, Office for Students and such other statutory, regulatory and government bodies in accordance with the requirements referred to in the paragraph above.

4.3 The College may also disclose to a current or prospective employer or sponsor information relating to a data subject's attendance, performance, achievement and conduct.

4.4 An individual may take steps to prevent the College from processing information where to do so may cause the individual substantial damage or substantial distress (except where the processing is necessary to fulfil the College's contractual obligations to provide education and training or to comply with a statutory obligation or in order to protect the vital interests of the individual).

4.5 The College's entry on the Information Commissioner's Register of Data Controllers is No. Z4677243 and can be found at:

Data Protection Public Register

This entry sets out in detail the purposes for which the College processes personal data.

5 Data Security

5.1 Security of personal data is extremely important to the College. We are trusted to protect sensitive information that may be supplied while conducting business.

5.2 Special category data is regarded by the GDPR as more sensitive and requires additional protection and can only be processed where there is a lawful basis to do so.

5.3 Under Article 6 of the GDPR the College processes personal data relating to an individual's ethnic origin. Processing is carried out in the exercise of the College's official authority and in compliance with statutory obligations to which the College is subject.

5.4 Under Articles 6(1) and 10 of the GDPR the College processes information relating to criminal convictions and offences. Processing is carried out in the exercise of the College's official authority and in compliance with statutory obligations to which the College is subject.

5.5 All staff are responsible for ensuring that personal data is:

- kept securely
- not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party.

5.6 Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

5.7 Hard/physical copy personal data should be:

- kept in a locked filing cabinet or in a locked drawer
- not left unattended on desks/in offices/workrooms
- securely handled and distributed
- destroyed by shredding or disposed of as 'Confidential Waste at the end of its retention period or when no longer required.

5.8 Electronic personal data should be:

- stored on the College's central servers
- password protected
- securely encrypted if transferred to any other form of storage device e.g. USB stick, laptop, etc
- deleted at the end of its retention period or when no longer required.

5.9 Through regular training and awareness raising, the College will seek to minimise the amount of unstructured data in use and only where there are valid reasons to do so will this data be shared. The appropriate safeguards will be put in place to ensure this is not retained by either the College or recipient any longer that it is necessary to do so.

5.10 Under no circumstances should Personal data be stored at staff members' homes whether in manual or electronic form, on laptop computers or other personal portable device.

5.11 Staff working from home using the College's remote desktop facility must ensure the same level of data security is applied and not downloaded to personal devices.

6 Credit Card Information Handling

6.1 The College will destroy all cardholder information in a secure method when no longer needed.

6.2 Media containing card information must be destroyed by shredding or other means of physical destruction that would render the data irrecoverable.

6.3 It is prohibited to record the contents of the credit card magnetic stripe (track data) on any media whatsoever.

6.4 It is prohibited to record the card-validation code (3 or 4 digit value printed on the signature panel of the card) on any media whatsoever (including paper records).

6.5 All but the last 4 numbers of the credit card account number must be masked (i.e. x's or *'s) when the number is displayed electronically or on paper.

7 Responsibility of Staff

7.1 If and when, as part of their responsibilities, staff collect information about students, (e.g. about students' coursework, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff.

7.2 It is compulsory for all staff to complete the College's online e-learning Data Protection Briefing and undertake any additional training as appropriate.

8 Data Subject Rights

8.1 Students and other users of the College have the right to be informed about how the College collects and uses personal data. This information is available in the College's Privacy Policy:

Privacy Policy

8.2 Students and other users of the College have the right to access any personal data and supplementary information that is being held about them either on computer or in manual files. The College will provide a copy of the information free of charge in most cases, however a small fee may be charged where the request is deemed manifestly unfounded or excessive.

8.3 Students and other users of the College have the right to rectification of any inaccurate or incomplete data. It is the responsibility of the student to inform the College of any amendments to personal data previously provided. All amendments to be notified to the MIS & Exams Office/tutor as appropriate.

8.4 Students and other users of the College also have the following rights under the GDPR:

- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object
- Rights related to automated decision making (including profiling).

8.5 Any person who wishes to exercise any of these rights should apply in writing to:

Data Protection Officer
Bridgwater & Taunton College
Bath Road
Bridgwater
Somerset
TA6 4PZ

Or by email to dpo@btc.ac.uk

9 Requests for Information under the Freedom of Information Act

9.1 The Freedom of Information Act 2000 imposes a number of obligations on public authorities, which for these purposes includes the College, and provides the public with wide rights of access to the College's records. Any person who wishes to exercise this right should apply in writing to the Freedom of Information Act Officer:

Director of Finance

A charge may be made for this information in accordance with the legislation.

10 Subject Consent and Special Categories of Data

10.1 In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is regarded as special category data (as defined by the GDPR), **explicit consent** must be obtained. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course.

10.2 Some courses leading to a professional qualification require the College to assess the student as fit to practise the particular profession. Those courses often require practical placements with employers, which may bring the students into contact with children and vulnerable adults. The College is therefore required to conduct criminal records checks via the Disclosure & Barring Service on applicants for such courses and the fitness to practise requirements require successful applicants to report any convictions incurred while on the course. The DBS Disclosure will be conducted prior to course recruitment and the information will be processed by the College for the purposes of assessing the eligibility of the applicant for the particular course, his/her fitness to practise the particular profession or for the purposes of assessing risks to health and safety, and the information may be disclosed to those persons within the College who are responsible for making such assessments. It may also be disclosed to placement providers. Students will be required to complete relevant consent forms. Places on such courses are provided and maintained on the basis of satisfactory DBS Disclosures and continuing good character and failure to provide consent to processing this information may result in the offer of a place being withdrawn, failure to secure a necessary placement and/or removal from the course.

10.3 The College also has a duty to take reasonable steps to accommodate students with learning difficulties or disabilities. In order to discharge this duty the College will need to process information concerning students' learning difficulties/disabilities and will disclose such information only to those persons within the College who need to have access to it for the purposes of assessing what adjustments can reasonably be made to accommodate the learning difficulties/disabilities and/or to assess fitness to practise issues. The College may disclose information relating to learning

difficulties/disabilities to placement providers for similar purposes. While the College acknowledges the right of a student to require that information relating to their learning difficulties/disabilities remains confidential, failure to provide consent to processing this information may mean that the College may not be able to make reasonable adjustments to accommodate the individual's learning difficulties/disabilities.

11 The Data Controller and Designated Data Controller/s

11.1 The College as a body corporate is the Data Controller under the GDPR, and the board is therefore ultimately responsible for implementation. However, there are designated Data Controllers dealing with day to day matters. The first point of contact for enquirers is:

Data Protection Officer (dpo@btc.ac.uk**)**

who will deal with the enquiry or refer it to another designated data controller.

12 Examination Marks

12.1 Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide. The College may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all books and equipment returned to the College.

13 Retention and Disposal of Data

13.1 Dependent on statutory requirements, the College will keep some forms of personal data for longer than others. Due to storage restrictions, hard/physical copies of personal data about students cannot be kept indefinitely. Where possible, electronic copies of hard/physical data will be scanned and retained as appropriate.

13.2 For specific retention periods refer to the College's Document Retention Policy.

13.3 When personal data is no longer required, or has passed its retention date hard/physical copies of data must be shredded or disposed of as confidential waste in the case of a significant amount of material which cannot be dealt with by normal shredding machines. Electronic personal data will be deleted from the appropriate systems.

14 Confidentiality in Minutes

14.1 The College keeps records of information about the activities of students, staff and other people it engages with through written minutes.

14.2 Whilst it wishes to make minutes as widely available as possible, the College is concerned not to inhibit discussion at its meetings but seeks to protect the confidentiality of people who are referred to in discussions.

14.3 As such, staff responsible for taking and approving minutes must ensure that any matters that are discussed and minuted, where they are of a sensitive, personal and/or confidential nature must not have names recorded against them. This may mean that some minutes have a restricted section where the distribution is limited, as

in particular cases it may be necessary to discuss and record names in specific terms.

14.4 More generally however minutes should not include names but instead could refer to the person by a reference that only a restricted number people will be aware of.

15 Conclusion

15.1 Compliance with data protection legislation is the responsibility of all members of the College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution.

15.2 Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated College Data Controller.

16 Review of Policy

16.1 The Data Protection Policy and Procedure will be reviewed in line with future legislative changes, case law or at no later than 3 years after the issue date.

16.2 The planned review date for the Data Protection Policy and Procedure is May 2020.