

Process for: G&M 1h	Data Protection Policy
Process owner:	Data Protection Officer
To ensure that:	The College complies with relevant data protection regulation - UK GDPR & UK Data Protection Act 2018
Which applies to:	All staff and students
Monitoring and evaluation:	Deputy Principal Finance & Resources

<p>Introduction</p> <p>The College needs to keep certain information about its employees, students and other users to allow it to monitor, for example, performance, achievements and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, BCoT must comply with the Data Protection Principles (Article 5) in UK GDPR & the Data Protection Act 2018. In summary these state that personal data shall:</p> <ul style="list-style-type: none"> • Be processed¹ lawfully, fairly, and in a transparent manner in relation to individuals • Be obtained for a specified, explicit and lawful purpose and not be processed in any manner incompatible with that purpose. • Be adequate, relevant and not excessive for that purpose. • Be accurate and, where necessary, kept up to date. • Not be kept for longer than is necessary for that purpose. • Be processed in accordance with the data subject's rights. • Be kept safe from unauthorised access, accidental loss, destruction or damage. • Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data. <p>Article 5(2) of GDPR also states</p> <ul style="list-style-type: none"> • The controller shall be responsible for, and be able to <i>demonstrate</i>, compliance with these principles <p>The College and all staff or others, who process or use any personal information, must ensure that they follow these principles at all times. In order to ensure that this happens, BCoT has developed this Data Protection Policy.</p> <p>Information that is already in the public domain is exempt from the 2018 Act & GDPR. It is BCoT's policy to make as much information public as possible, as detailed in 'Policy on Access to College Information' [G&M 1f)]. Documents detailed in appendices 1 and 2 of G&M 1f are public documents; any individual who has good reason for wishing details in these appendices to remain confidential should contact the designated data controller.</p>
<p>2 Status of the Process</p> <p>This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by BCoT from time to time. Any failures to follow the policy will be treated seriously by the College and will result in disciplinary proceedings.</p>

¹ Processed is defined as accessing, altering, adding to, changing, disclosing or merging any data.

Date Reviewed: Feb 25	Date Impact Assessed: Apr 19	Date Review Due: Feb 27
-----------------------	------------------------------	-------------------------

Compliance with the GDPR is the responsibility of everyone associated with the College. Any deliberate breach of the Data Protection Policy will lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated data controllers.

3 Scope

The policy applies to all employees and students of the college.

4 Rights of Staff and Students

All staff, students and other users are entitled to:

- Know what information BCoT holds and processes about them and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what BCoT is doing to comply with its obligations under GDPR.

Any person who wishes to gain access to the information held on them should complete the college "Access to Information" form and give it to the relevant data controller.

The first request is free. BCoT may make a charge of £10 however where a request is "manifestly unfounded or excessive", or for each further copy of their data after the first. A Data Controller will usually have discretion to waive this charge.

BCoT aims to comply with requests for access to personal information as quickly as possible, and will ensure that it is provided within a calendar month unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request with no undue delay.

Current students will be entitled to information about their marks for both coursework and examinations at no cost. 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 have not been returned to the College.

5 Responsibilities of Staff

Staff have responsibility for:

- Checking that any information that they provide to the College in connection with their employment is accurate and up to date.
- Informing the College of any changes to information which they have provided, eg changes of address, change in qualifications
- Checking the accuracy of the information that the College sends out from time to time. BCoT cannot be held responsible for any errors unless the staff member has informed the College of them.
- Complying with guidelines for staff when collecting information about other people.
- Ensuring any personal data which they hold is kept securely and in line with college policy
- Ensuring personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.
- Ensuring that they report any breaches to the DPO as soon as they become aware of it, as per the breach policy (G&M 1r)

Personal information should be:

- Kept in a locked filing cabinet, or
- In a locked drawer, or

- In a room which is kept locked unless an authorised person is present
 - If it is computerised, password protected, or
 - Kept only on disk which is itself kept securely and encrypted.
- Keys, combinations and passwords should themselves be kept securely.

6 Responsibilities of Students

Current students must ensure that:

- All personal data provided to BCoT is accurate and up to date.
- Any relevant changes are notified to the Student Records Office.

BCoT cannot be held responsible for any errors unless the student has informed the college.

Current students may, from time to time, process (see page 1) personal data. If they do they must notify the relevant data controller. Any student who requires further clarification about this should contact their Assistant Principal.

7 Sensitive Information / Special Category

In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive as in the examples below, **express consent** must be obtained (this includes information about previous criminal convictions).

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. The College has a duty under the Children Act and other enactments to ensure that staff are suitable for the job, and students for the courses offered. The College also has a duty of care to all staff and students and must therefore make sure that employees and those who use BCoT's facilities do not pose a threat or danger to other users (see Appendix 3).

BCoT will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The College will only use the information in the protection of the health and safety of the individual, but will usually need consent to process in the event of a medical emergency, for example. In matters of "life or death", we will use Vital Interests as a lawful basis to share information, usually with health professionals to protect a person's life.

Sometimes it is necessary to process information about a person's immigration status, race and gender and family details. This may be to monitor the operation of College policies, such as the Attendance Management Policy (HR2f) or Equality & Diversity Policy (EDS 1a), or for fulfilment of our contractual obligations with the ESFA.

Therefore, all prospective staff and students will be asked to sign a Consent to Process statement, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a statement can result in the offer being withdrawn. However a student may decline to answer any questions about religion and sexuality if they choose to do so. This information is collected to ensure that all students' experience equal opportunities during their time at BCoT, or the data may influence changes to policies and procedures in future years.

8 The Data Controller, Data Protection Officer and the Designated Data Controllers

The College as a body corporate is the Data Controller under the Act, and the Board is therefore ultimately responsible for implementation. However, the Data Protection Officer, assisted by the designated Data Controllers, will deal with day to day matters to ensure the requirements of the Act are met.

3

Date Reviewed: Feb 25	Date Impact Assessed: Apr 19	Date Review Due: Feb 27
-----------------------	------------------------------	-------------------------

This College has designated five posts as Data Controllers. They are:

- Clerk to the Board of Corporation – Simon Burrell
- Deputy Principal (Finance & Resources) – David Moir
- HR Manager – Sammy Dibbern
- Head of Information Services – Greg Devereux-Cooke
- Transition Manager – Helen Key

9 The Retention of Data

The College will keep some forms of information for longer than others. Due to storage problems, information about students cannot be kept indefinitely, unless there are specific requests to do so. Records will be kept for periods as stated in the Records Management Policy (G&M 1m). This will include:

- name and address,
- academic achievements, and
- copies of any reference written.

In general, all information about staff will be kept for six years after a member of staff leaves the college. Some information however will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment. A full list of information with retention times is available from the Human Resources Department. If data needs to be held for a different length of time the Data Controller should be informed.

Date Reviewed: Feb 25	Date Impact Assessed: Apr 19	Date Review Due: Feb 27
-----------------------	------------------------------	-------------------------

STAFF GUIDELINES FOR DATA PROTECTION

- 1 All staff will process data about students on a regular basis, when marking registers, or College work, writing reports or references, or as part of a pastoral or academic supervisory role. The College will ensure, through enrolment procedures, that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the GDPR. The information that staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:
- General personal details such as name and address,
 - Details about class attendance, coursework marks and grades and associated comments
 - Notes of personal supervision, including matters about behaviour and discipline.
- 2 Information about a student's physical or mental health; sexual life, political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the student's consent. If staff need to record this information, they should contact a designated Data Controller for further guidance, eg, recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of pastoral duties.
- 3 All staff have a duty to make sure that they comply with the data protection principles, which are set out in the staff handbook and the College Data Protection Policy. In particular, staff must ensure that records are:
- Accurate;
 - up-to-date;
 - fair;
 - kept and disposed of safely, and in accordance with the College policy
- 4 The College will designate certain staff to be authorised to hold or process sensitive data. Authorised staff will be responsible for ensuring that all data is kept securely. These will include the College nurse, HR and Student Records staff.
- The only exception to this will be if a non-authorised staff member is satisfied that the processing of the data is necessary:
- in the best interests of the student or staff member, or a third person, or the College; AND
 - he or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances.
- The legal basis for doing so is when it is in the "vital interests" of the subject. This should only happen in very limited circumstances. For example, a student is injured and unconscious, but in need of medical attention, and a staff tutor tells the hospital that the student is pregnant or a Jehovah's witness.
- 5 Staff must not disclose personal data about any other student, without authorisation or agreement from the data controller or the data subject themselves.

- 6 Staff must not disclose personal data about any other staff member except with the authorisation or agreement of the designated data controller, or the data subject.
- 7 Before processing any personal data, all staff should consider the checklist.

Staff Checklist for Recording Data

- Do you really need to record this information or is it already available elsewhere?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive do you have the data subject's express consent?
- Has the student been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- Are you sure the data is accurate?
- Are you sure that the data is secure?
- If you are recording information not already available, have you taken advice from the Data Controller?
- If you are looking at purchasing/using new software, have you follow the 3-Tick sign off process: Digital, IT, DPO?

Date Reviewed: Feb 25	Date Impact Assessed: Apr 19	Date Review Due: Feb 27
-----------------------	------------------------------	-------------------------

STANDARD REQUEST FORM FOR ACCESS TO DATA

I, [insert name], wish to have access to either [delete as appropriate]

1 All the data that the College currently has about me, either as part of an automated system or part of a relevant filing system; or

2 Data that the College has about me in the following categories:

- Academic marks or coursework details for the year.
- Academic or employment references
- Disciplinary records
- Health and medical matters
- Political, religious or trade union information
- Any statements of opinion about my abilities or performance
- Personal details including name, address, date of birth etc

Other information

Signed Date

To ensure that we identify you accurately please complete the following details

Full name Date of Birth

Address

.....

..... Post code

Are you staff/student/other Date of leaving the college

Student/staff reference number (if known)

You should receive a reply to this request within 1 calendar month.

Date of receipt: Response date:

DISCLOSURE AND BARRING SERVICE PRIVACY STATEMENT

The following statement is provided for staff information.

The Disclosure and Barring Service is fully committed to compliance with the Data Protection Act 2018 and the GDPR. The following principles will apply when we handle your personal information:

- only information that we actually need is collected and processed
- your personal information is only seen by those who need it to do their jobs
- personal information is retained only for as long as it is required
- decisions affecting you are made on the basis of reliable and up to date information
- your information is protected from unauthorised or accidental disclosure
- you will be provided with a copy of the information we hold on you, on request
- any information found to be inaccurate will be investigated and corrected/amended where applicable
- your personal information with regard to the disclosure service is only processed with your knowledge

These principles apply whether we hold your information on paper or in electronic form.

Note: the college destroys completed Disclosure and Barring Service forms six months after they are returned by the Service.

Supporting Documentation:

Appendix 1 Staff Guidelines for Data Protection Appendix 2 Standard Request form for Access to Data Appendix 3 Disclosure and Barring Service Privacy Statement	
Data Protection Act 2018 (the 2018 Act)	
UK/EU regulation 2016/679 (GDPR)	
G&M 1f Access to College Information	
HR Staff Attendance Management Procedure	
EDS 1a Equality & Diversity Policy	
G&M 1m Records Management Policy	

Date Reviewed: Feb 25	Date Impact Assessed: Apr 19	Date Review Due: Feb 27
-----------------------	------------------------------	-------------------------