# POLICY/PROCEDURE: DATA PROTECTION POLICY

Approval required by: SMT Y Governing Body Y

SMT Lead: Vice Principal Funding, Data and Compliance

Responsible Manager: Director Quality and Performance

Date approved: May 2018

Date to be reviewed: May 2019

Relevant to: Students Y Staff Y

 Visitors Y

Relevant to: All students Y

 16-18 Vocational Y Sixth Form Y

 Higher Education Y Adults Y

Apprenticeships Y 14-16 Y

Other Y …………………………..

Relevant to: All staff Y

 Board Y SPH Y

Managers Y

 Teaching staff Y Support staff Y

Accessible to Students Y Staff Y

Friendly version Students N Staff Y

EQIA required N

Significant changes to policy

* Policy changed to reflect GDPR requirements.
* Charge removed for processing access requests.
* Failure to report a breach, may be grounds for disciplinary action.
* Identifies the Data Controller.

Impact of changes

To ensure the college is compliant with GDPR.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# SCOPE AND PURPOSE

Barnsley College is committed to protecting the rights and privacy of individuals (including staff, students and others) in accordance with General Data Protection Regulation (GDPR) and the Data Protection Act 2018. The college needs to keep and process certain information about its staff, students and other individuals with whom it has dealings for administrative purposes, e.g. to recruit and pay staff, to administer programmes of study, to record progress, to agree awards, to collect fees and to comply with legal obligations to funding bodies and government as indicated in its notification to the Information Commissioner.

This document sets out the college’s policy in relation to data protection.

# BACKGROUND

Any data held is processed in an appropriate manner to ensure security. Training will be given to all staff to ensure secure processes.

Data Protection Impact Assessments will be carried out when new systems and processes are introduced.

## Role Definition

Barnsley College is the Data Controller for all personal data held in college systems.

The Vice Principal Funding, Data and Compliance is charged with ensuring that the college develops its control functions in accordance with the GDPR and is charged with carrying out Data Protection Impact Assessments. He may be contacted as follows:

Vince Dalton

Vice Principal Funding Data and Compliance

Barnsley College

PO Box 266

Church Street

Barnsley

S70 2YW

Tel: 01226 216547

Email: v.dalton@barnsley.ac.uk

The Director Quality and Performance is the Data Protection Office for Barnsley College. He may be contacted as follows:

Kurt Taylor

Director Quality and Performance

Data Protection Officer

Barnsley College

PO Box 266

Church Street

Barnsley

S70 2YW

Tel: 01226 216565

Email: k.taylor@barnsley.ac.uk

## Responsibility

Barnsley College Board of Governors is responsible for ensuring the college has a Data Protection Policy.

The Vice Principal Funding, Data and Compliance is responsible for authorising and requesting action in relation to data protection processes and procedures, risk and privacy assessments.

The Data Protection Officer is also responsible for the provision of staff training.

In addition the Data Protection Officer will:

* Be visible and contactable by staff, governors and learners.
* Have direct access to the Board through the nominated link Governor.
* Be advised of any data breaches or relevant disclosure.
* Report breaches and information disclosure to the Information Commissioners Office.
* Provide staff training.

## Purpose of Data Collection

Barnsley College needs to collect and use personal data about people including past, present and prospective staff, students, Governors and customers in order to carry out its business and meet its stakeholders’ requirements effectively. The college recognises that the lawful and correct treatment of personal data is very important to successful operations and to maintaining its customers’ confidence.

When the college collects any personal data, it will inform the individual/organisation how long it proposes to retain the data, why it is collecting their data and what it intends to use it for.

## Personal Sensitive Data

Where the college collects any sensitive data, it will take appropriate steps to ensure that it has explicit consent to hold, use and retain the information. Sensitive data is personal data regarding an individual’s race or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sex life, details of the commission or alleged commission of any offence and any court proceedings relating to the commission of an offence.

## Principles of Data Processing

Any personal data which it collects, records or uses in any way whether it is held on paper, on computer or other media will have appropriate safeguards applied to it to ensure compliance with the General Data Protection Regulation. The college endorses and adheres to the data protection principles specified in Article 5 of the GDPR:

* **Processed lawfully, fairly and transparently** - To ensure that personal data is obtained and processed lawfully the college will only process data when one of the conditions of processing in Article 7 and 8 are met.
* **Collected for specific purposes** - The college will ensure that all processing of personal data is undertaken for explicit and legitimate purposes. The college will not sell or rent data to third parties. In addition college does not use automated processes for decision making.
* **Adequate, relevant and limited –** The College will ensure that personal data processed is adequate, relevant and limited to what is necessary in relation to the purpose.
* **Accurate and kept up to date** – The college will ensure that there are mechanisms in place to ensure personal data remains accurate and up to date.
* **Retained for as long as required** – The college will ensure that personal data is held for no longer than necessary. Retention records are specified in the college Data Retention Policy and Privacy Note.

## Data Protection Register

The college’s purpose for holding personal data and a general description of the categories of people and organisations to which this may be disclosed are listed in the college’s Data Protection Register. This may be inspected by contacting the college’s Data Protection Officer or a copy may be obtained from the Information Commissioner’s Office or website (type Barnsley College in the ‘Name’ field):

<http://www.ico.gov.uk/ESDWebPages/search.asp>.

## Responsibilities of Staff

All staff are responsible 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 i.e. changes of address.
* Checking the information that the college will send out from time to time, giving details of information kept and processed about staff.
* Informing the college of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed the college of them.

If and when, as part of their responsibilities, staff collect information about other people (i.e. about students course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the data protection principles.

## Data Security

All staff are responsible for ensuring that:

* Any personal data which they hold is kept securely.
* Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Staff should note that unauthorised disclosure and/or failure to adhere to the requirements set below may, depending on the circumstance, be a disciplinary matter.

If staff become aware of a data protection breach they have caused, they must report the breach to the Data Protection Officer. Failure to do so may result in disciplinary action.

Personal information should be:

* kept in a locked filing cabinet; or
* in a locked drawer; or
* if it is computerised, be password protected; or
* when kept or in transit on portable media the files themselves must be encrypted.

Personal data relating to either staff or learners should never be stored at staff members’ homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites, unless encrypted and only used for college approved work.

Ordinarily, personal data should not be processed at staff members’ homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the relevant Head of Department must be obtained, and all the security guidelines given in this document must still be followed.

Staff should refrain from keeping local copies of learners’ information and should not duplicate anything that is held centrally.

If marking work at home staff can identify learners by student number, name and course as this information is available publicly. Any other data such as marks awarded should be stored on One Drive or encrypted on a laptop.

Data stored on portable electronic devices or removable media is the responsibility of the individual member of staff who operates the equipment. It is the responsibility of this individual to ensure that:

* Suitable backups of the data exist.
* The data is appropriately encrypted.
* Data is not copied onto portable storage devices without first deploying appropriate encryption and protection measures.
* Electronic devices such as laptops, mobile devices and computer media (USB devices, CDs, etc.) that contain sensitive data are not left unattended when offsite and are encrypted.

Staff who are using their home computers, laptops or tablets to access the college servers remotely need take no further action provided that personal/sensitive data is not subsequently stored locally.

## Student Obligations

Students must ensure that all personal data provided to the college is accurate and up to date. They must ensure that changes of address, etc. are notified to the course tutor, TTL or department administrator.

## Data Subject Rights

The college will make sure that all policies and procedures relating to data processing are clear, unambiguous and easily accessible. A privacy notice will be provided to cover all instances of processing and will provide enough information to ensure compliance with Article 13 of the General Data Protection Regulation.

Requests for access to personal data should be made to the Director Quality and Performance (K.taylor@barnsley.ac.uk).

The college will not charge for this and will aim to respond within a month.

By following this process the college is complying with Article 15 of the General Data Protection Regulation.

## Correction and Erasure

The college recognises the right of users to request that incorrect data be corrected and that data be erased in specific circumstances.

Routine amendments requests should be managed by the relevant college department.

Requests to erase data should be referred to the Data Protection Officer.

All requests will be handled in regard to Articles 16 – 19 of the General Data Protection Regulation.

## Data Sharing

In many cases, the college can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express 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, and a condition of employment for staff. 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 legislation 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 the college facilities do not pose a threat or danger to other users.

The college 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 need consent to process in the event of a medical emergency, for example.

Therefore, all prospective staff and students will be asked to consent to processing data, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form will result in the offer being withdrawn.

The college has a responsible marketing policy and does not give details of its customers or related individuals to any other organisation without their explicit authorisation.

The policy applies to all staff, students and governors of the college. Any breach of the General Data Protection Regulation, the college’s Data Protection Policy or any of the college’s information security policies may be an offence and in that event the college disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with the college who have access to personal information will be expected to have read and comply with this policy. It is expected that departments who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy (*See Data Sharing Protocol*).

For further information please contact:

Director Quality and Performance

Data Protection Officer

Barnsley College

PO Box 266

Church Street

Barnsley

S70 2YW

Tel: 01226 216565

Email: k.taylor@barnsley.ac.uk

## Processing Sensitive Information

Sometimes it is necessary to process information about a person’s health, criminal convictions, race and gender and family details. This may be to ensure the college is a safe place for everyone, or to operate other college policies, such as the Sick Pay Policy or Equal Opportunities Policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for the college to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason.

# EQUALITY AND DIVERSITY

An EqIA is not required for this policy.

# LINKED POLICIES AND PROCEDURES

* Data Protection Procedures.
* Enrolment Terms & Conditions and procedures.
* Freedom of Information Policy.
* Privacy Notice.
* Removable Media Policy.
* Information Security Incident Policy.
* Data Hosting Policy.

# LOCATION AND ACCESS TO THIS POLICY

This policy is available on the college’s intranet.