|  |
| --- |
| **DATA PROTECTION POLICY** |
| **Date Approved:** |  **November 2016** |
| **Approved by:**  | **SMT** |
| **Review Date:** |  **November 2018** |
| **Responsible Manager:** | **Director Quality**  |
| **SMT Lead:** | **Vice Principal Funding, Data and Compliance** |
| **Accessible to Students:** | **Yes** |
| **Relevant to Sixth Form College:** | **Yes** |
| **Relevant to Employer Responsive:****Relevant to HE:** | **Yes****Yes**  |

# SCOPE AND PURPOSE

Barnsley College is committed to protecting the rights and privacy of individuals (including staff, students and others) in accordance with the Data Protection Act 1998. 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

## Purpose of Data Collection

Barnsley College needs to collect and use personal data about people including past, present and prospective staff, students and customers in order to carry out its business and meet its customers’ 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 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 Data Protection Act 1998. The college endorses and adheres to the eight principles of the Data Protection Act 1998. These principles state that data must be:

* Processed fairly and lawfully.
* Be obtained only for one or more specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose or those purposes.
* Be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
* Be accurate and where necessary, kept up to date.
* Not be kept any longer than is necessary for that purpose or those purposes.
* Be processed in accordance with the rights of the data subject under the Act.
* Be processed with the appropriate technical and organisational measures being taken against unauthorised or unlawful processing and against unauthorised or unlawful processing and against accidental loss, destruction or damage.
* Not to be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

## 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 Information 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>.

The college has identified the Director of Quality and Performance as the Data Controller.

## The College’s Obligations

In order to meet the requirements of the principles, the college will:

* Observe the conditions regarding the fair collection and use of personal data.
* Meet its obligations to specify the purposes for which personal data is used.
* Collect and process appropriate personal data only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement.
* Ensure quality of personal data used.
* Ensure that the rights of individuals about whom the personal data is held, can be fully exercised under the Act.
* Take appropriate security measures to safeguard personal data.
* Ensure that personal data is not transferred abroad without suitable safeguards.

## 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 will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

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 password protected and if possible 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 Data Controller 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 work 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

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.
* Sensitive data is appropriate encrypted.
* Sensitive data is not copied onto portable storage devices without first consulting 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 or Department Administrator.

## Access to Personal Information

Under the Data Protection Act, any staff or student, both present and past, may write to the college’s Information office at the address shown below and request a copy of the information which the college holds about them. The college reserves the right to charge a fee of £10 for providing this information and aims to produce it within 30 days. If the details are inaccurate a request can be made to have these details amended.

## 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 sign Consent to Process form, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can 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 Data Protection Act 1998, the college’s Data Protection Policy or any of the college’s Information Security Policies is considered 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

Data Controller

Barnsley College

PO Box 266

Church Street

Barnsley

S70 2YW

Tel: 01226 216565

Email: foi@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 relevant for this policy.

# LINKED POLICIES AND PROCEDURES

* Data Protection Procedures.
* Enrolment Terms & Conditions and procedures.
* Freedom of Information Policy.

# LOCATION AND ACCESS TO THIS POLICY

This policy is available on the college’s intranet.