POLICY/PROCEDURE: DATA PROTECTION POLICY

Approval required by:	SMT	Y	Governing Body	Y	
SMT Lead:	Director MIS				
Responsible Manager:	Director MIS				
Date approved:	May 2023				
Date to be reviewed:	May 2025				

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

No changes

Impact of changes

None

SCOPE AND PURPOSE
Barnsley College is committed to protecting the rights and privacy of individuals (including staff, students and others) in accordance with UK 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 Director of MIS is charged with ensuring that the College develops its control functions in accordance with the UK GDPR and is the Data Protection Officer for Barnsley College.

~~and is charged with carrying out Data Protection Impact Assessments. They may be contacted as follows:~~

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

The Director MIS is responsible for authorising and requesting action in relation to data protection processes and procedures, risk, and privacy assessments and to ensure the appropriate level of staff training is implemented.

In addition, the Information Governance 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.

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 UK GDPR. The College endorses and adheres to the data protection principles specified in Article 5 of the UK 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 Articles 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 Notices.
- **Kept safe and secure**.

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 Governance Officer or a copy may be obtained from the Information Commissioner's Office or website (type **BARNSLEY COLLEGE** in the 'Name' field) - https://ico.org.uk/ESDWebPages/search/

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 must report the breach to the Director of MIS or the Information Governance 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 role restricted and/or 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.

Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, for example 'deliberate, unauthorised and unintentional' incidents. Whilst most Personal data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

There are three main types of personal data breach which are as follows:

1.Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, personal data e.g. hacking, accessing internal systems to which you are not authorised to access, accessing personal data stored on a lost laptop, phone or other device, people "blagging" access to personal data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong member of staff or student, or disclosing information over the phone to the wrong person

2. **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, personal data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting personal data in error, loss of access to personal data stored on systems, inability to restore access to personal data from back up, or loss of an encryption key

3. **Integrity breach** - where there is an unauthorised or accidental alteration of personal data.

Notifying breaches to the ICO
As an organisation we have to report breaches to the Information Commissioner's Office within 72 hours of detection where the breach is likely to result in a risk to the rights and freedoms of Individuals (Data Subjects). Failure to report a breach when required to do so may result in penalties and fines of up to €10 million, or 2% of an organisations global turnover.

Notifying breaches to Individuals (Data Subjects) affected
We will notify the Individuals (Data Subjects) affected by the Data Breach as soon as possible where the breach is likely to result in a high risk to their rights and freedoms, for example identity theft or fraud or where the breach may give rise to discrimination.

Whilst we are still required to notify the ICO, we are not obliged to notify the Individuals (Data Subjects) affected where:

- There are technological and organisational protection measures in place (e.g. encryption)
- We have taken action to eliminate the high risk
- It would involve disproportionate effort

Reporting a breach or concern
- Data breach and data concerns within the College will be notified to the Head of Department and Information Governance Officer immediately as per the Data Breach Management Procedure - see flowchart at Appendix 1.
- Data breach and data concerns from those outside the College should be made to the Information Governance Officer.
- We will follow guidance from the ICO where necessary to determine if the breach is reportable.
- We will maintain a register of Data Breach incidents and concerns.

Data Subject Rights
The College will make sure that all policies and procedures relating to data processing are clear, unambiguous and easily accessible. Privacy notices 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.

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

Subject Access Requests (SARs)

Individuals have a right to access any personal data relating to them which are held by the College.

If you wish to request information we hold about you, we would prefer you to complete a Data Subject Access Request form (Appendix 2) and email it to foi@barnsley.ac.uk. However, any request in writing or email from the Individual (Data Subject) will be considered as a valid request, as long as it contains the relevant information to enable us to deal with your request.

If you are not known to the relevant Department or Business area, you will be asked to provide proof of your identity. The following forms of identity will be accepted as proof of identity (please note, we will require sight of the original):

A copy of your passport
A copy of your driving licence
A copy of your Bank, Building Society or credit card statement in the Data Subject's name for the last quarter
A copy of your Council Tax bill

If you are requesting information on behalf of someone else you must complete the Data Subject Access Request form and provide written evidence that you have the Data Subject's authority to ask for the information on their behalf, e.g. signature on the Data Subject Access form, a letter written by them, evidence of Power of Attorney, etc.

If your Data Subject Access Request is approved, you will be provided with either a printout or a photocopy of paper records. Where information is requested to be provided by email, we will only agree to this if it can be sent via an approved secure method.

We will respond to your request within 30 days, where we are unable to approve your request for information or are unable to provide the information within 30 days, we will notify you. Verification of identity of the person/organisation making the request will be required.

Information will normally be provided free of charge. However, there may be certain circumstances when a charge can be made: for example, where the request is manifestly unfounded or excessive, we may charge a 'reasonable fee' for the administrative costs of complying with the request. We can also charge a reasonable fee if an Individual (Data Subject) requests further copies of their data following a request. We will follow guidance from the ICO to determine if a charge applies and advise you prior to collating the information.

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 Information Governance Officer.

All requests will be handled in regard to Articles 16 – 19 of the UK GDPR.

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 14 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 UK GDPR, 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.

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.

Contact Details

For further information please contact:
Information Governance Officer
Barnsley College
PO Box 266
Church Street
Barnsley
S70 2YW

Email: foi@barnsley.ac.uk

EQUALITY AND DIVERSITY
An EqIA is not required for this policy.

LINKED POLICIES AND PROCEDURES

- Data Retention Policy
- External Hosting Policy
- Freedom of Information Policy
- Privacy Notices
- Removable Media Policy
- Information Security Incident Policy
- Record of Processing Activities (ROPA)

LOCATION AND ACCESS TO THIS POLICY
This policy is available on the College's intranet and website.

Appendix 1 - Data Breach Notification Procedure

IDENTIFYING AND REPORTING A DATA BREACH
If you discover a data breach, you must report this to our **Information Governance Officer** immediately by emailing foi@barnsley.ac.uk. All breaches big or small, regardless of the harm or potential harm, should be identified and reported. False alarms or even breaches that do not cause any harm to individuals or to the College should nevertheless be reported as it will enable the College to learn lessons in how to respond and the remedial action that we put in place. We have a legal obligation to keep a register of all data breaches. Please ensure that you report any breach, even if you are unsure whether or not it is a breach.

BECOMING AWARE OF A DATA BREACH – INVESTIGATING
We become aware of a data breach when we have a reasonable degree of certainty that a security incident has occurred that has led to personal data or security being compromised. From this point, our time limit for notification to the **Information Commissioner's Office (ICO)** will commence. When you report a data breach to the Information Governance Officer (IGO), they will liaise with the Director of MIS to ensure an investigation into the breach to ascertain whether we are fully aware that a breach has occurred leading to personal data being compromised for our data subjects. The investigation will be done within 48 hours of a breach being reported to the College, so that it can ensure it complies with the 72-hour deadline to report any data subject or serious security breaches in a timely way to the ICO data breach may result in disciplinary action.

ASSESSING A DATA BREACH
Once you have reported a breach and the IGO has investigated it and has decided that we are aware that a breach has occurred, the IGO will log the breach in the Data Breach Register and will carry out an initial assessment of the breach to evaluate its severity. Once the level of severity is known, the Director of MIS will notify the Senior Leadership Team (SLT). If necessary, SLT will appoint a response team which may involve for example our HR and IT teams and we will assign responsibility for particular tasks as necessary across the response team. We will then investigate the breach and consider any on-going risks to the College and any individuals affected. If it is considered that the breach is very serious, they will consider the impact on our reputation and the effect it may have on the trust placed in us.

FORMULATING A RECOVERY PLAN

The Director of MIS in consultation with senior management will investigate the breach and consider a recovery plan, if required, to minimise the risk to individuals. As part of the recovery plan, our investigating officer and senior management may interview any key individuals involved in the breach to determine how the breach occurred and what actions have been taken.

NOTIFYING A DATA BREACH TO THE INFORMATION COMMISSIONER'S OFFICE (ICO)

Unless the breach is unlikely to impact on data subjects or result in a risk to the rights and freedoms of individuals, the ICO must be notified of the breach within 72 hours of the College becoming aware of the breach.

Individuals concerned (Data Subjects) must be notified as soon as possible where the breach is likely to result in a high risk to their rights and freedoms.

The content of the notification will be drafted the IGO, and any notification to the ICO must only be made by the Director of MIS.

NOTIFYING A DATA BREACH TO INDIVIDUALS

Individuals concerned (Data Subjects) must be notified as soon as possible where the breach is likely to result in a high risk to their rights and freedoms.

The content of the notification will be drafted by the IGO in line with procedures and in conjunction with consulting the ICO if considered necessary. Individuals will be notified in clear and plain language and in a transparent manner (for example by email, SMS or letter). Please be aware that **under no circumstances must you try and deal with a data breach yourself.**

In some circumstances, we may not need to notify the affect individuals (Data Subjects). The Director of MIS will decide whether this is the case.

This will be carried out as soon as possible after we become aware of the breach.

NOTIFYING A DATA BREACH TO OTHER RELEVANT THIRD PARTIES

It may also be necessary to notify other third parties about the data breach depending on the nature of the breach. This could include:

- Insurers
- Parents/Guardians
- Banks
- Police
- Sponsors
- Contract counterparties
- Employees

The decision as to whether any third parties need to be notified will be made by the Director of MIS and SLT. They will decide on the content of such notifications and act within 5 days of becoming aware of the data breach.

UPDATING NOTIFICATIONS
We need to keep the ICO up to date about the data breach. If anything changes from the time we send the initial notification to the ICO, the Director of MIS will consider whether we need to update the ICO about the data breach.

EVALUATION AND RESPONSE
The key to preventing further incidents is to ensure that the College learns from previous incidents. It is extremely important to identify the actions that the College needs to take to prevent a recurrence of the incident. The Director of MIS and the IGO will carry out an evaluation as to the effectiveness of our response to the data breach and document this in the Data Breach Register. SLT may then make changes to College procedures to minimise the likelihood of incidents occurring again.

Appendix 2 - Data Subject Access Request Form

We will respond to your request within one month, where we are unable to approve your request for information or are unable to provide the information within one month, we will notify you.

Information will normally be provided free of charge, however, there may be certain circumstances when a charge can be made, we will follow guidance from the ICO to determine if a charge applies and advise you prior to collating the information.

If you require assistance in completing a request, please contact the Information Governance Officer.

- If you are making the request for yourself, please complete the form below.
- If you are completing the request on behalf of someone else, please ensure that you provide written authority. We will expect you to verify your identity.
- Requests for Disclosure by the Police and Enforcing Bodies should be made via an official request or the Police/Enforcing Bodies Request Form. We will expect you to verify your identity.

Full Name	
Organisation/Relationship to Data Subject	
Address	
Telephone Number	
Email Address	

1. Are you requesting information about yourself?	**Yes**	**No**

If Yes, you are the data subject and documentary evidence may be required if you are not known to the relevant Department or Business area, we may ask to see proof of your identity. The following will be accepted as proof of identity.
-A copy of your passport
-A copy of your driving license
-A copy of your Bank, building society or credit card statement in the Data Subject's name for the last quarter
-A copy of your Council Tax Bill

If No, please supply the written consent of the data subject and supply their details as follows:

Full Name			
Address			
Telephone Number			
Email Address			
Signature		**Date**	

2. Please briefly explain why you are requesting this information rather than the data subject.
3. **Please describe the information you seek together with any other relevant information to help us identify the information you require. It would be helpful if you could advise the reason for the request.** (please continue on a separate sheet if necessary)
ALL APPLICANTS MUST COMPLETE THIS SECTION (Please note that any attempt to mislead may result in prosecution).
I confirm that the information given on this application is true and I understand that Barnsley College may need more information to confirm my identity or the identity of the data subject and to locate the information that I am requesting.

Full Name			
Signature		Date	

Please return the completed form to the:

Information Governance Officer
Barnsley College
Church Street
Barnsley
S70 2YW
Email: foi@barnsley.ac.uk

FOR COLLEGE USE ONLY			
Request Approved	Yes/No	**Reason for refusal**	
Request approved by			
Signed:		**Date:**	