POLICY/PROCEDURE: DATA PROTECTION POLICY

Approval required by:	Executive	Y	Governing Body	Y
Senior Lead:	Executive Director MIS			
Responsible Manager:	Executive Director MIS			
Date approved:	May 2025			
Date to be reviewed:	May 2028			

Significant changes to policy

Several sections have been added to the policy to refer to processes the College undertakes:

- DPIA section added
- Record of processing activity section added
- Privacy notices section added
- Training section added
- Data retention section added

Additional sections created that make existing paragraphs more visible:

- Lawful basis for processing personal details section added
- Individual rights section added
- Responsibilities

ITS has been included in the policy

Impact of changes

Although additional sections have been added, this does not impact on the College as they were already being undertaken.

SCOPE AND PURPOSE

Barnsley College or ITS ('the 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.

Data Protection Register
The ICO is the UK's data protection regulator (Supervisory Authority).

Barnsley College is the Data Controller for all personal data collected and is required to register with the ICO and submit an annual notification listing the purposes under which it processes personal information. The College must also notify the ICO within 28 days should any entry become inaccurate or incomplete. The ICO publishes a register of controllers on its website which is available to the public for inspection. Responsibility for maintaining these notifications rests with the Data Protection Officer.

The College's registrations are as follows:

- Barnsley College - Registration No: Z7019338
- Independent Training Services Limited – Registration No: Z6654163

Responsibilities
Board of Governors - The Board of Governors is responsible for ensuring the College has a Data Protection Policy.

Executive Director MIS - The Executive Director MIS is charged with ensuring that the College develops its control functions in accordance with the UK GDPR and adopting best practice, and is the College's nominated Data Protection Officer (DPO).

Information Governance Officer – The IGO is the initial point of contact for any Data Protection related enquiries and support staff to understand their responsibilities under the Act.

Both the DPO & IGO must be adequately trained and sufficiently well-resourced to perform the role and is given the required independence to perform their tasks.

Managers – All Managers are responsible for ensuring that staff within their department are fully aware of, and abide by, this policy and any specific requirements relating to their roles and that staff have completed any Data Protection training that the College implements to support Data Protection.

All Staff – All staff have a responsibility for ensuring that any personal data which they hold is kept securely, transported safely (where this has been approved by the DPO/IGO) and that personal information is not disclosed in any way to any unauthorised parties. Personal data can either be electronic or paper based. All staff have a duty to report any data breaches or near misses relating personal data as soon as they become aware of them.

For the purpose of this policy "aware" is defined as when a member of staff has a reasonable degree of certainty that an incident has occurred which has resulted in personal data being compromised.

All staff are under legal and contractual obligations to keep personal and other information confidential not only during their employment (or equivalent) but also after it has been terminated. Data breaches may lead to disciplinary action, gross misconduct and may constitute a criminal offence leading to a referral to the police and ICO.

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 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, this will be done through its privacy notices.

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**.

All college staff are responsible for ensuring that the above principles are observed at all times and at all stages of the data lifecycle including:

- Collection or capture of personal data
- Post collection processing of data e.g. storing, alteration, transmission, archiving, etc.
- Erasure or destruction of personal data

The College is required by law to be able to demonstrate compliance with the Data Protection Principles and has several policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that it can demonstrate its compliance.

Records of Processing Activities
"Processing" is the collection, recording, organisation structuring, storage, adoption or alteration, retrieval, consultation or use, disclosure, destruction or erasure of personal data.

The College will identify the legal basis for processing 'personal data' as defined by Article 6 and 'special categories of data' as defined by Article 9 and document this on a Record of Processing Activity (ROPA) through an Information Asset Register as required by Article 30.

The College will assess which lawful purpose applies to make each use of personal data lawful. If the use changes, then the assessment will need to be redone. The use of personal data will be reviewed periodically, and any initial data audits will be updated periodically too. If we are considering making changes, we will decide whether their intended use requires amendments to be made and any other controls which need to apply, and we may need to notify Individuals (Data Subjects) about the change.

Lawful Basis for Processing Personal Data
In order to process Personal Data lawfully, the College must meet one of the lawful basis for processing. The lawful basis must be established before processing begins.

The six lawful bases are:

Consent: The College should be able to demonstrate that the data subject has provided recent, clear, explicit and defined consent for their data to be processed for a specific purpose.

Contract: The processing is necessary for the performance of a contract to which the data subject is party to in order to take steps at the request of the data subject prior to entering into a contract.

Legal Obligation: The processing is necessary for compliance with a legal obligation to which the College is subject.

Vital Interest: The processing is necessary in order to protect the vital interests of the data subject or of another natural person. e.g. to protect an individual's life.

Public Interest: The processing is necessary for the College to perform a task in the public interest or for official functions and the task or function has a clear basis in law.

Legitimate Interest: The processing is necessary for the purpose of the legitimate interests of the College or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data. A legitimate interest assessment must be undertaken if using this lawful basis.

Lawful Basis for Processing Personal Data - 'Special Categories of Personal Data'
In addition, when the College collects and/or uses Special Categories of Personal Data, it must demonstrate that one of a number of additional conditions is met. These are set out in Article 9 and are as follows:

- Explicit consent
- Employment, social security and social protection (if authorised by law)
- Vital interests
- Not-for-profit bodies
- Made public by the data subject
- Legal claims or judicial acts
- Reasons of substantial public interest (with a basis in law)
- Health or social care (with a basis in law)

- Public health (with a basis in law)
- Archiving, research and statistics (with a basis in law)

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

Individual 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.

Individuals can request to exercise these rights verbally or in writing. When a request to exercise any of the following rights is received by a member of staff, they must inform the Data Protection Officer immediately.

The Right to be Informed
- Individuals have the right to be informed about the collection and use of their personal data.
- The College provides Privacy Notices to meet this requirement.

The Right of Access
- Individuals have the right to request access to their personal data.
- This is often called a Subject Access Request.

The Right to Rectification
- Individuals have the right to have inaccurate personal data rectified or completed if it is incomplete.

The Right to Erasure
- Also known as the right to be forgotten, this enables individuals to request their data be erased.
- This is not an absolute right and only applies in certain circumstances.

The Right to Restrict Processing
- Individuals have the right to request the restriction or suppression of processing of their personal data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, the College is permitted to store the personal data but not use it.

The Right to Data Portability
- The right to data portability allows individuals to obtain and reuse their personal data for

their own purposes across different services.
- The right only applies to information an individual has provided to a Controller (The College).
- It allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.

The Right to Object

- This gives individuals the right to object to the processing of their personal data in certain circumstances.
- Individuals have an absolute right to stop their data being used for direct marketing.
- In some cases, where the right to object applies the College may be able to continue processing if there is a compelling reason for doing so.

Rights in relation to Automated Decision Making and Profiling

- Automated decision making is using solely automated methods without any human involvement in order to make a decision about an individual.
- Profiling is any form of automated processing that uses personal data to analyse or evaluate certain personal aspects relating to an individual.

The College can only carry out this kind of processing if the decision is:

- Necessary for the entry into or performance of a contract.
- Authorised by domestic law applicable to the data controller.
- Based on the individual's explicit consent.

In order to process data in this manner, the College shall ensure that:

- Individuals receive information about the processing.
- There are simple ways for the individual to request human intervention or challenge a decision.
- Regular checks are carried out to make sure that the systems are working as intended.

College staff must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

The College does not carry out Automated Decision Making or Profiling in relation to its employees.

Subject Access Requests (SARs)

The most commonly exercised individual right is that of the right of access. The right of access allows an individual to know what information the College holds and processes about them. This is known as a subject access request, which also allows individuals to be given a copy of the information held, as well as supplementary information, such as where and with whom the information may have been shared. The right of access, like many of the individual rights, is not an absolute right and disclosure of the requested information is subject to exemptions.

Unless the information requested is provided as part of the normal course of business, the individual who is the subject of the data (the data subject) should be directed to the DPO/IGO who can be contacted at foi@barnsley.ac.uk for advice on how to make a Subject Access Request (SAR). The College must respond to these requests within one month of their receipt.

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.

Transparent Processing – Privacy Notices
Personal data must be processed 'in a transparent manner'. This is achieved by providing the data subject with information at the point of data capture, or if this is not possible, within a reasonable period after obtaining the data, but at least within one month. This information is known as a Privacy Notice.

If the College receives Personal Data about an Individual from other sources, it will provide the Individual with a privacy notice about how the College will use their Personal Data. This will be provided as soon as reasonably possible and in any event within one month.
If the College changes how it uses Personal Data, the College may need to notify Individuals about the change. If college staff therefore intend to change how they use Personal Data please notify the Data Protection Officer or Information Governance Officer who will decide whether the intended use can be permitted and requires amendments to be made to the privacy notices and any other controls which need to apply.

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.

Training
The College will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter in line with college expectations.

GDPR will be a mandatory training module for all staff and successful completion will be a requirement of their employment.

Individuals whose roles require regular access to special category data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

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 Executive Director 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 Protection Impact Assessments (DPIA)
The Data Protection Act 2018 introduces a new requirement to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment ("DPIA"). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

- describe the collection and use of Personal Data;
- assess its necessity and its proportionality in relation to the purposes;
- assess the risks to the rights and freedoms of individuals; and
- the measures to address the risks.

Where a DPIA reveals risks, which are not appropriately mitigated the ICO must be consulted.

When the College is launching or proposing to adopt a new process, product or service which involves Personal Data, the College needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The College needs to carry out DPIA at an early stage in the process i.e. prior to procurement of a new software system, so that the College can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

Situations where the College may have to carry out a DPIA include the following (please note that this list is not exhaustive):

- large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling where legal or similarly significant decisions are made;
- large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data; or
- systematic monitoring of public areas on a large scale e.g. CCTV cameras
- Introduction of an IT system which processes large amounts of personal data

All DPIAs must be reviewed and approved by the either the Data Protection Officer or the Information Governance Officer.

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.

Data Retention
The UK GDPR does not dictate how long the College should keep personal data however, one of the data protection principle states that *"data should be kept in a form which permits identification of a data subject for no longer than is necessary."* This means that the data must only be stored for as long as it is required. This might be stated for a specific timescale by external companies such as Awarding Organisations and funding bodies who will determine retention periods.

Where guidance does not exist, the College shall determine the suitable retention period for data being processed and ensure that once this data has reached this threshold, it is securely destroyed, anonymised or erased. The retention period of the data will be determined by the purpose for which it is processed and the lawful basis for processing it.

Where data is archived, it is the responsibility of the data owner to ensure this correctly labelled for storage and is disposed of after the date has expired. The exception might be if such as funding rule have changed. In these cases, the dates must be updated.

For data processed by the College, the retention period and any relevant justifications are recorded in the College's Document Retention Schedule. It is the responsibility of Managers to ensure that both paper and electronic records are retained or disposed of accordingly. Disposal of any paper documents must be done by using confidential waste disposal sacks provided by Estates.

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 Executive 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 Executive 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 Executive 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 Executive 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 Executive 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 Executive 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 Executive 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 Executive 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:**	