



**BILBOROUGH**  
SIXTH FORM COLLEGE

# Data Protection Policy

Updated for GDPR May 2018

Reviewed March 2021

Next review due: March 2022

## Introduction

Bilborough College ("the College") needs to collect, store and use certain information about its employees, students and other users to allow it to monitor performance, achievements, health and safety, for example. It also needs to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government departments complied with. This policy describes how this data must be collected, processed and stored to meet the College's data protection standards and to comply with the law and in particular under Article 5 of GDPR.

Compliance with the Data Protection Act 2018 is the responsibility of all members of the College and any breach of the Data Protection policy may lead to disciplinary action being taken, access to the college being withdrawn, or a criminal prosecution. Any queries regarding the interpretation of the policy should be directed to the Data Protection Officer.

The College has implemented this Data Protection Policy to ensure all College Personnel are aware of what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in the College and will provide for a successful working and learning environment for all.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed unlawfully to any other person. To do this, the College must comply with the Data Protection Principles, which are set out in the Data Protection Act (1998).

In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- Be adequate, relevant and not excessive for those purposes
- Be accurate and kept up to date
- Not be kept for longer than is necessary for that purpose
- Be processed in accordance with the data subject's rights
- Be kept safe from unauthorised access, accidental loss or destruction
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data

The College and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the College has developed the Data Protection Policy.

Transparent Processing – Privacy notices

Where the College collects Personal Data directly from Individuals, the College will inform them about how the College uses their Personal Data. This is in a privacy notice. The College has adopted the following privacy notices:

- Student

- Staff
- Visitor
- Governor
- Homestay provider

If the College receives Personal Data about an Individual from other sources, the College 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 who will decide whether the intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

Copies of Privacy Notices (formerly called a Fair Processing Notice) are available on the Intranet and a copy of the student Privacy Notice is included in Appendix 1 as an example.

## **The designated Data Controller**

The College as a body corporate is the data controller under the Act, and the College Corporation is therefore ultimately responsible for implementation.

The designated Data Protection Officer on behalf of the College is:

Helen Dennis, Director of Marketing & Information

The Data Protection Officer is also responsible for:

- To inform and advise on GDPR and related obligations
- To monitor compliance with the GDPR and related obligations
- To provide advice regarding data protection impact assessment and to monitor its performance
- To act as a point of contact with the supervisory authority, if required
- Monitoring the application and compliance with the GDPR within the College
- Providing advice, guidance and direction on data protection issues within the College
- Maintaining the College's registration with the Information Commissioner's Office
- Notifying the ICO in the event of a data breach

The Data Protection Officer can be contacted by email on [dpo@bilborough.ac.uk](mailto:dpo@bilborough.ac.uk)

Or by phone: 0115 8515000

or at:

Bilborough College

College Way,

Nottingham,

NG8 4DQ

## **Scope**

The Data Protection Policy covers all computerised and manual data processing relating to identifiable individuals. It not only includes information about individuals, but also opinions and intentions towards an individual. It therefore includes, for example, personnel records about staff, student records, emails relating to identifiable individuals, team meeting minutes, student and staff references.

## **Status**

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the College from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

Any member of staff or student, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated data controller initially. If the matter is not resolved it should be raised as a formal grievance.

## **Responsibilities of Staff and Students**

All staff and students are responsible for:

- Checking that any information that they provide to the College in connection with their employment or learning is accurate and up to date
- Informing the College of any changes to or errors in information, which they have provided, i.e. changes of address. They must ensure that changes of address, etc. are notified to Human Resources (staff) and Student Services (students)

The College cannot be held responsible for any such errors unless the staff member or student has made the College aware.

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 Staff Guidelines in Appendix 2.

## **Data Security**

All staff are responsible for ensuring that:

- Any personal data stored (including personal images) are kept securely, for example in a locked room, locked filing cabinet or locked drawer
- All data that is stored electronically is password protected and that all passwords are regularly changed
  - The college operates a secure student tracking records system for collecting, storing and processing student data. It is expected that electronic student data should be collected, stored and processed within this system wherever possible.
  - Similarly, the college operates a secure system for collecting, processing and storing staff data and it is expected that electronic staff data should be collected, stored and processed within this system wherever possible.

- Data stored on hard-drives or other storage devices is removed before disposal
- Papers containing personal information are shredded before disposal
- Databases are closed and workstations securely locked when leaving the computer or device
- 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 will usually be a disciplinary matter and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual staff member. For the avoidance of doubt, staff are advised to refer to the Data Controller for advice before deciding to disclose any information.

Staff should not store data files containing personal information on portable storage such as CD or USB sticks for use off-site. This should not be necessary as staff can access this information securely via the remote-desktop server.

If in exceptional circumstances it is considered essential to store personal information on a portable storage device (for example emergency contact details for a trip), staff MUST ensure that the device is suitably encrypted first. Device encryption can be carried out by IT.

### **Rights to access information – Subject Access Requests**

Staff, students and other users of the College have the right to access any personal data that is being kept about them either on computer or in certain files. This is known as a Subject Access Request. Any person who wishes to exercise this right should contact the Data Protection Officer and state clearly what information is being requested.

The right of access to information is not an entitlement to access to documents as such (which may be accessible by means of the Freedom of Information Act, subject to any exemptions and the public interest), but the right to access personal data as contained within the document.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing to the Data Protection Officer. A fee may be payable for the administrative cost of complying with the request.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month.

The college may refuse a subject access request if the data includes information about another individual, except where the other individual has agreed to the disclosure, or where it is reasonable to provide the information without the consent of the other individual. In deciding this, the college will balance the rights of the data subject with the other individual's rights regarding their own information.

The college may also refuse any request which it considers manifestly unfounded or excessive, but in any case will explain and justify such a decision.

## **Subject Consent**

There may be instances where 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.

## **Processing Sensitive Information**

Processing means obtaining, recording, holding or carrying out any operation on the information or data.

Sensitive personal data is a special category. It may only be processed with the explicit consent of the data subjects. Sensitive personal data, including personal images, consists of information relating to:

the racial or ethnic heritage of the data subject

- political opinions
- religious or other beliefs of a similar nature
- trade union membership
- physical or mental health or condition
- sexual orientation
- the commission or alleged commission of any offence
- proceedings for any offence or alleged offence

Sometimes it is necessary to process information about a person's 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 Equality, Diversity & Inclusion Policy.

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 or disabilities. The College will only use the information for the protection of the health and safety of the individual, but will need consent to process this information, for example in the event of a medical emergency.

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 consent to this without good reason.

## **Examination Results**

Students will be entitled to information about their marks for both coursework and examinations. Examination results are normally notified directly to students. Lists of examination results identifying individual students are not posted on College notice boards. The College may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or books and equipment not returned to the College.

Examination results are made available to the Director of Education, Nottingham City Council, and Heads of partner schools.

Examination results may be made available for publication in the local newspapers. The College does not have to obtain specific consent to publish results but students have a right to object to publication. News stories focussing on individual students will only be made available with the consent of the student.

## **Retention of Data**

Personal data will be retained for no longer than is necessary for the purpose for which it was collected.

The College will keep some forms of information for longer than others to meet various contractual or legal requirements.

Appendix 3 indicates the length of time that certain records will be retained.

## **Data Protection breaches**

Where a Data Protection breach occurs, or is suspected to have occurred, this should be reported immediately in accordance with the Data Security Breach Management and Reporting Procedure.

## **Data Protection Audits**

Audits of computerised and manual record systems should be conducted annually.

## **Periodic review of Data Protection Policy**

The Data Protection Officer should review the Data Protection Policy annually.

## Appendix 1 - Privacy Notice for Students



### Privacy Notice (How we use student information)

This Privacy Notice describes how Bilborough Sixth Form College protects and makes use of the information you provide to us.

Colleges, schools, Local Authorities and the Department for Education, the government department which deals with education, all hold information on young people. This is to run the education system, and in doing so, they have to follow the Data Protection Act 2018, also known as the General Data Protection Act or GDPR. This means that the data held about young people must only be used for specific purposes allowed by law. This notice is to tell you about the types of data held, why that data is held, and with whom it may be shared under the law.

### Student information that we collect

We may collect a range of information including, but not limited to the following:

- Personal information (such as name, unique learner number or ULN and address)
- Contact information including phone, email and postal addresses
- Educational information including qualifications, predicted grades and learning support needs
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as lessons attended, absences and absence reasons)
- Contact details for your parent(s) or carers
- Other information (such as relevant medical information, Special Education Needs information, assessment information, reference information, well-being and progress information and CCTV imagery)

### Why we collect and use this information

Collecting your data helps us to manage and administer your education, support teaching and learning, monitor and report on your progress, provide appropriate pastoral care and to assess how well the college as a whole is doing. We use the student data:

- to meet our legal and statutory duties and responsibilities
- to process applications and enrolments
- to contact you about your application or enrolment, or to provide you with information about our courses which we think may be relevant to you
- to support student learning
- to monitor and report on student progress
- to provide appropriate pastoral care
- to assess the quality of our services

- to preserve the safety and security of all our students and staff

We will not use information that you provide to us for anything other than the reasons stated here. If you do not enrol at Bilborough College, we will retain your information in accordance with our retention policy and may use your information on an aggregated basis to guide and inform the college's recruitment strategies, (e.g. comparing numbers of students recruited from different schools/areas.)

## **The security of your information**

We will always hold your information securely.

To prevent unauthorised disclosure or access to your information, we have implemented strong organisational and technical security safeguards.

Where it is necessary and appropriate to share information with other organisations (see below) we will only do so with an appropriate Information Sharing Agreement in place.

We follow stringent procedures to ensure all our data processing meets the requirements of the Data Protection Act and the new GDPR.

## **Examination results and certificates**

Exam results and certificates may be collected in person on production of photo ID. Any third party collecting exam results or certificates on behalf of a student must bring a signed written authority from the student which names the student and the person collecting the information on their behalf. The person collecting will also be required to show photo ID confirming their identity.

## **Information Sharing and Disclosure**

We do not sell or otherwise distribute your personal information inappropriately.

Your information may when necessary, be disclosed to appropriate staff of Bilborough College and to government bodies (to fulfil our statutory duties) such as the Education Skills Funding Agency, Ofsted, the Department for Education and auditors or with local partners working on behalf of the Local Authority such as Nottinghamshire Futures.

Any personal information we hold about you is processed in accordance with the Data Protection Act and the new GDPR.

## **Using our website**

When you visit our website [www.bilborough.ac.uk](http://www.bilborough.ac.uk) we collect standard internet log information to help us understand how many visitors use different parts of the website. For more information about this please see our [Cookie policy](#) on the college website. Unless you have changed your browser settings to refuse cookies,

Our online applications portal uses session cookies. These are text files which are essential for you to use the online applications systems and view your information securely. No user-specific information is held within any of these cookies and they are deleted at the end of a user session.

## **Use of the college's computers**

We monitor how you use the college's equipment and computers and what websites you visit when browsing the internet at college. This is because we have legal obligations to protect you, and we also have a legitimate interest in making sure you are using our computer equipment correctly and that you are not looking at any inappropriate content. Please refer to the college's Acceptable Use Policy for computer equipment for more guidance on appropriate conduct when using college IT equipment.

## **The lawful basis on which we use this information**

To comply with GDPR articles 6 and 9, we are required to identify the legal basis on which we collect and use your personal information.

Generally, the information is processed as part of our public interest task of providing education to you. Where that information is special category personal information (e.g. medical information) we will process it because there is a substantial public interest for us to do so.

## **Collecting student information**

Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain student information to us or if you have a choice in this. Where information that is not mandatory, we will usually provide the option for you to respond "prefer not to say" or to leave your response blank.

## **Storing student data**

We store student data in line with data retention policy.

## **Who we share student information with**

We routinely share student information with:

- schools that the students attended prior to joining us
- local authorities
- the Department for Education (DfE)
- Education and Skills Funding Agency
- Ofsted
- Nottinghamshire Futures
- Parents and carers as detailed on your application

We also share mobile phone numbers with the company contracted to provide our college bus services in order that they can provide users of this service with travel

updates. We provide relevant mobile phone numbers and the route reference but no other details.

## **Why we share student information**

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.

We share student data with the Department for Education (DfE) on a statutory basis. This data sharing underpins education funding and educational attainment policy and monitoring.

## **Data collection requirements**

To find out more about the data collection requirements placed on us by the Education and Skills Funding Agency (part of the Department for Education) go to: <https://www.gov.uk/government/collections/individualised-learner-record-ilr>

## **Youth support services and data processing by 3<sup>rd</sup> parties**

We will also share certain information about students with local authorities and / or providers of youth support services to enable them to fulfil their statutory duties in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996; and to enhance their ability to support achievement, learning and welfare of all young people for whom they are responsible.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

We will only share information for processing by a third party where there is in place a 3<sup>rd</sup> party data sharing agreement which demonstrates that processing is carried out in a manner which meets all the requirements of the GDPR (for example to generate reports on value added and student progress to support us in assessing how well the college is performing).

## **Requesting access to your personal data**

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, contact the data protection officer detailed below.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means

- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>

## Contact

If you would like to discuss anything in this privacy notice, please contact the Data Protection Officer as follows:

The Data Protection Officer is: Helen Dennis, Director of Marketing & Information, and be contacted by email [DPO@bilborough.ac.uk](mailto:DPO@bilborough.ac.uk) phone 0115 8515000 or at the following address: College Way, Nottingham, NG8 4DQ

Bilborough College is registered with the Information Commissioner's Office as a Data Controller, as a public authority under the Freedom of Information Act 2000.

## Changes to our Privacy Notice

We keep our privacy Policy under regular review. Any changes we make to our privacy policy in the future and whilst you remain a student of Bilborough College will be notified to you by email.

This Privacy Notice has been prepared in accordance with the General Data Protection Regulation (EU) 2016/679 ("GDPR") and the Data Protection Act 2018.

Date of review:17/05/18 Reviewer: H Dennis

## **Appendix 2 – Data Protection staff guidelines**

All staff will process data about individuals when carrying out their role, for example when submitting attendance data or completing progress reports. Within its enrolment procedures, the college ensures that individuals give consent to such processing and are notified of the categories of processing and the reasons for doing so, as required by the Data Protection Act.

All staff have a duty to ensure that they comply with the data protection principles set out in the introduction to the Data Protection policy and in particular must ensure that records are:

- Up to date
- Accurate
- Fair
- Stored and disposed of securely and in accordance with college policy

Before processing any personal data, staff are advised to consider:

- Whether the information needs to be recorded
- Whether the information is sensitive
- If the information is sensitive, do you have the data subject's consent?
- Has the data subject been advised this type of data will be processed?
- Have you checked that the data is accurate?

The College will designate certain staff as authorised to access data that is sensitive or non-standard for example when dealing with matters relating to safe-guarding. Only these staff are authorised to access data in this category.

Authorised staff with access to sensitive data have a responsibility for maintaining the security of such data at all times by ensuring:

- IT equipment is not left unattended
- IT equipment is password-protected
- Any paper records are put away in lockable storage
- Paper records are securely destroyed when no longer required

Any person who discovers they have access to sensitive or non-standard data which they believe they are not authorised to access must report this to the designated safe-guarding lead person, their deputy or the Data Controller immediately.

### Appendix 3 - Data retention guidelines

<b>Data description</b>	<b>Retention period</b>
Student records including academic achievements, attendance and conduct	At least 10 years
Accident books and accident report forms	At least 3 years after the date of the last entry or in line with the requirements of RIDDOR 1985.
Examination certificates	Will be retained for a period of 4 years and thereafter destroyed
Staff application forms / interview notes	6 months from the date of the interview
Personnel files including records of disciplinary and grievance hearings	At least 6 years from the end of the period of employment
Personnel training and appraisal records	At least 6 years from the end of the period of employment
Financial records including sales invoices, purchase orders, financial statements.	At least 6 years from the end of the financial period to which they refer